MINISTRY OF EDUCATION AND SCIENCE OF UKRAINE
ZAPORIZHZHIA NATIONAL UNIVERSITY

O. H. CHEREP
S. V. MARKOVA
Yu. V. KALYUZHNA

KEY DIRECTIONS OF DEVELOPMENT OF INTELLECTUAL TECHNOLOGIES IN COUNTERING DISINFORMATION AND POST-WAR RECOVERY

Monograph

IZDEVNIECĪBA
BALTIJA
PUBLISHING
2025

UDC 33(082)
Ke970

Reviewers:

Maria Bondarchuk – Doctor of Economic Sciences, Professor, Head of the Department of Finance, Lviv Polytechnic National University;

Olga Honchar – Doctor of Economic Sciences, Professor, Department of Economic Theory, Entrepreneurship and Trade, Khmelnytskyi National University;

Nila Khrushch – Doctor of Economic Sciences, Professor, Head of the Department of Finance, Banking, Insurance and the Stock Market, Khmelnytskyi National University;

Ihor Vinichenko – Doctor of Economic Sciences, Professor, Head of the Department of Economics, Dnipro State Agrarian and Economic University

Recommended by the decision of the Academic Council of Zaporizhzhia National University (protocol № 11 of 27.05.2025)

Ke970 **Key** Directions of Development of Intellectual Technologies in Countering Disinformation and Post-War Recovery : monograph / O. H. Cherep, S. V. Markova, Yu. V. Kalyuzhna. Riga, Latvia : Baltija Publishing, 2025. 226 p.

ISBN 978-9934-26-682-9

DOI https://doi.org/10.30525/978-9934-26-682-9

The study considers the theoretical foundations of the use of intelligent technologies to counter disinformation, with the definition of a key concept and the classification of such technologies. Theoretical approaches to the analysis of disinformation in the context of military conflict are highlighted, as well as the role of intelligent technologies in guaranteeing national information security and supporting economic recovery is emphasized. The current state of development of these technologies is analyzed and their effectiveness in the world and in Ukraine is assessed. The main directions for the development of intellectual technologies during the war and for the post-war economic recovery of the country have been identified. Models for the use of intelligent solutions to combat disinformation are proposed, as well as practical cases of their use both during the war and in the process of post-war reconstruction of the Ukrainian economy are presented.

The research materials are intended for students and teachers of economic faculties of higher education institutions of higher education institutions of III and IV levels of accreditation, as well as for managers, financiers, marketers and specialists in the field of management decisions.

UDC 33(082)

ISBN 978-9934-26-682-9

МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

О. Г. ЧЕРЕП
С. В. МАРКОВА
Ю. В. КАЛЮЖНА

КЛЮЧОВІ НАПРЯМИ РОЗВИТКУ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ У ПРОТИДІЇ ДЕЗІНФОРМАЦІЇ ТА ПІСЛЯВОЄННОМУ ВІДНОВЛЕННІ

Монографія

IZDEVNIECĪBA
BALTIJA
PUBLISHING
2025

УДК 004.8-043.86:316.776.23-048.66:341.38
Ч-46

Рецензенти:

Марія Бондарчук – доктор економічних наук, професор, завідувач кафедри фінансів, Львівський політехнічний національний університет;

Ольга Гончар – доктор економічних наук, професор кафедри економічної теорії, підприємництва та торгівлі, Хмельницький національний університет;

Ніла Хрущ – доктор економічних наук, професор, керівник Департаменту фінансів, банківської справи, страхування та фондового ринку, Хмельницький національний університет;

Ігор Вініченко – доктор економічних наук, професор, завідувач кафедри економіки, Дніпровський державний аграрно-економічний університет

Рекомендовано до друку рішенням Наукової ради
Запорізького національного університету
(протокол № 11 від 27.05.2025 р.)

Череп О. Г.

Ч-46 Ключові напрями розвитку інтелектуальних технологій у протидії дезінформації та післявоєнному відновленні : монографія / О. Г. Череп, С. В. Маркова, Ю. В. Калюжна. Рига, Латвія : Baltija Publishing, 2025. 226 с.

ISBN 978-9934-26-682-9

DOI https://doi.org/10.30525/978-9934-26-682-9

У дослідженні розглянуто теоретичні основи використання інтелектуальних технологій для протидії дезінформації, із визначенням ключового поняття та наведенням класифікації таких технологій. Висвітлено теоретичні підходи до аналізу дезінформації в умовах воєнного конфлікту, а також підкреслено роль інтелектуальних технологій у гарантуванні національної інформаційної безпеки та підтримці економічного відновлення. Проаналізовано сучасний стан розвитку цих технологій і оцінено їх ефективність у світі та в Україні. Визначено основні напрями розвитку інтелектуальних технологій у період війни й для післявоєнного економічного відновлення країни. Запропоновано моделі застосування інтелектуальних рішень для боротьби з дезінформацією, а також представлено практичні кейси їх використання як під час війни, так і в процесі післявоєнної реконструкції економіки України.

Матеріали дослідження призначаються для студентів і викладачів економічних факультетів закладів вищої освіти III та IV рівнів акредитації, а також для менеджерів, фінансистів, маркетологів і спеціалістів у сфері управлінських рішень.

УДК 004.8-043.86:316.776.23-048.66:341.38

ISBN 978-9934-26-682-9

CONTENT

ЗМІСТ

PREFACE

In the modern world, the rapid development of digital technologies is driving fundamental changes in all spheres of social life. Artificial intelligence, as one of the most powerful technologies of the 21st century, plays a crucial role in transforming the global environment, influencing not only scientific and technological progress but also economic stability, social security, and the information space. In the context of wartime challenges and hybrid threats, the relevance of studying the role of intelligent technologies in countering disinformation is significantly increasing, as information security has become an integral component of national resilience and state policy.

Contemporary Ukraine is compelled to fight simultaneously on the battlefield and in the information domain. Massive campaigns of disinformation, fake news, and manipulative technologies have become one of the key instruments of hybrid warfare, aimed at undermining public trust in state institutions, weakening international support, and destabilizing society. Under such conditions, the use of intelligent technologies – artificial intelligence, machine learning, neural networks, and big data analytics – opens new opportunities for building effective mechanisms of monitoring, detection, and neutralization of destructive information content.

The monograph "Key Guidelines for the Development of Intelligent Technologies in Countering Disinformation and Post-War Recovery" is devoted to a comprehensive study of theoretical, methodological, and practical aspects of applying intelligent technologies within the national information security system. Its purpose is to outline strategic directions for the development of digital solutions that enhance the efficiency of public administration, strengthen information sovereignty, and stimulate economic growth during the post-war recovery period.

The first chapter of the monograph examines the theoretical foundations of intelligent technologies in countering disinformation,

including the essence and classification of intelligent systems, the evolution of approaches to analyzing disinformation processes during armed conflicts, and the role of artificial intelligence technologies in strengthening national information security.

The second chapter focuses on assessing the current state of development of intelligent technologies in the world and in Ukraine, analyzing trends in their implementation, evaluating their effectiveness in combating disinformation during wartime, and identifying promising vectors for the development of digital tools to support economic recovery.

The third chapter presents practical aspects of the application of intelligent technologies, including the modeling of innovative approaches to countering disinformation, the analysis of real cases of using intelligent systems during the war, and recommendations for their implementation in the post-war period. It emphasizes that the development of intelligent technologies is not only a technical task but also a social process that requires the enhancement of digital culture, the formation of ethical and legal frameworks for the use of AI, and the strengthening of international cooperation.

The monograph has both scientific-theoretical and practical significance. It aims to support government institutions, educational and research organizations, business entities, and civil society institutions in developing digital transformation strategies and enhancing Ukraine's information resilience.

This collective work presents theoretical generalizations, conclusions, and practical recommendations that will be useful for researchers, educators, graduate and doctoral students, policymakers, business representatives, and members of civil society.

The monograph is based on the results of research conducted within the framework of the project of fundamental and applied scientific studies, as well as scientific and technical (experimental) developments on the topic No. 2/25 "Artificial Intelligence as a Tool for Countering Disinformation During the War and Post-War Economic Recovery in Ukraine" (state registration number 0125U000996) (01.01.2025–31.12.2027).

CHAPTER 1.
THEORETICAL FOUNDATIONS OF INTELLIGENT TECHNOLOGIES IN COUNTERING DISINFORMATION

1.1. THE CONCEPT, ESSENCE, AND CLASSIFICATION OF INTELLIGENT TECHNOLOGIES

Intelligent technologies are the result of the development of information and communication systems and represent one of the key directions of the digital transformation of modern society. They combine the achievements of artificial intelligence, machine learning, neural networks, natural language processing, big data analytics, and expert systems. The main goal of using intelligent technologies is to create systems capable of self-learning, adaptation, and decision-making based on data analysis, which makes it possible to increase management efficiency, optimize business processes, and ensure high-quality managerial decision support.

Intelligent technologies are the result of the evolution of information and communication systems that integrate knowledge, algorithms, models of reasoning, and elements of artificial intelligence to solve complex tasks that previously could only be performed by humans. Their essence lies in the ability to self-learn, analyze, predict, and make decisions based on large volumes of data.

Unlike traditional digital tools that operate according to predefined algorithms, intelligent technologies imitate human thinking processes. They analyze not only statistical information but also patterns, contexts, and causal relationships, which allows them to adapt to environmental changes and make optimal decisions in real time [1].

A key feature of intelligent technologies is the presence of a cognitive component – the system's ability to "understand" the task, form hypotheses, and improve its own behavioral models through machine learning. That is why such technologies form the foundation for creating intelligent systems of management, analytics, marketing, and production.

The essence of intelligent technologies also lies in the integration of analytical, predictive, and communicative functions. They not only collect and process data but also generate new knowledge, identify trends, help forecast risks, and interact with users in natural language.

From an economic perspective, intelligent technologies act as a driving force of digital business transformation. Their implementation ensures process automation, increased labor productivity, cost reduction, and the creation of new competitive advantages. As a result, not only the structure of the enterprise changes, but also the approach to managerial decision-making itself.

Moreover, the essence of intelligent technologies encompasses synergy between humans and machines. They do not replace humans but complement human intelligence, enhancing the ability to analyze, model situations, and find optimal business development paths. This approach forms the foundation of a knowledge economy, where data, information, and intelligent decisions become the main resources.

The modern stage of economic and managerial development is marked by the integration of humans and technologies into a single cognitive system. Intelligent technologies have become the instrument that ensures synergy between human reasoning and artificial intelligence, combining the analytical power of machines with the creative and ethical potential of humans. The essence of this synergy is that computer systems not only execute commands but also interact with users, learn from them, and jointly form new knowledge, behavioral models, and managerial decisions.

Intelligent technologies create conditions for redistributing functions between humans and machines. Machines take on routine,

analytical, and computational operations, while humans focus on strategic, creative, and ethical aspects of management. This approach does not diminish the human role – on the contrary, it enhances human intellectual potential, opening a new level of interaction – cognitive partnership. Such partnership ensures greater speed and accuracy of decision-making and reduces the risk of human error in complex economic systems [12–20].

The synergy between humans and machines is realized through machine learning, natural language processing, neural networks, intelligent data analysis, and expert systems. Thanks to these tools, computers not only follow instructions but can independently draw conclusions, learn from experience, and predict trends. Humans, in turn, set strategic goals, evaluate results, and establish ethical boundaries for the use of such systems. This results in mutual reinforcement of cognitive abilities, where human intelligence provides context and artificial intelligence provides analytical depth [2].

The importance of human-machine synergy is particularly evident in enterprise management, marketing analytics, finance, and production. Intelligent technologies help collect, systematize, and analyze data from various sources, while humans determine their value and make decisions that align with the organization's strategic goals. This interaction creates an intelligent business environment where decisions are made not intuitively but based on precise analysis and forecasting. The key outcome of this synergy is the formation of a new type of managerial culture – a culture of cooperation with technology. Humans no longer perceive machines as threats but as intellectual partners that help unlock potential, reduce information analysis time, and ensure effective functioning of organizations in a digital economy. This requires the development of digital literacy, ethical understanding of AI's limits, and the ability to –25 build balanced "human – machine" systems [21].

Thus, the essence of intelligent technologies lies not only in creating smart systems but also in forming harmonious interaction

between human and machine intelligence. This interaction gives rise to a new quality of management based on data, adaptability, analytics, and moral responsibility. Such synergy ensures the transition from digitalization to the intellectualization of the economy, where partnership – not competition – between humans and machines plays the leading role [3, p. 143].

Therefore, intelligent technologies represent an integrative concept of the modern digital world, the essence of which lies in creating systems capable of thinking, learning, and making decisions. This ensures a new level of efficiency in management, competitiveness, and sustainable development of enterprises and the economy as a whole.

The essence of intelligent technologies lies in modeling human cognitive functions – thinking, learning, analysis, forecasting, and decision-making – through algorithms and software systems. They enable the automation of complex intellectual processes, create conditions for developing intelligent management, marketing, finance, education, and security systems. The use of such technologies enhances enterprises' digital maturity, develops innovation potential, and strengthens economic competitiveness.

Intelligent technologies can be classified according to various criteria – by the level of autonomy, learning method, field of application, or type of algorithmic base. In particular, we distinguish between weak (narrow) and strong artificial intelligence technologies; systems trained with supervision, without supervision, or through reinforcement; as well as applied solutions oriented toward specific industries (marketing, medicine, transport, finance, etc.). Such classification allows for a clearer understanding of the place and role of each technology within the structure of modern digital solutions.

Intelligent technologies, or artificial intelligence (AI) technologies, are becoming an integral part of the modern business environment. They encompass a wide range of tools – from big data analytics to automated management systems, chatbots, and predictive models. In Ukraine, their implementation began relatively recently,

but development rates are increasing due to businesses' growing need to improve efficiency and competitiveness [4].

The emergence of intelligent technologies in Ukrainian business is driven by several factors: enterprise digitalization, the increasing volume of data, and global competition. Companies are realizing that using AI helps reduce costs, accelerate production and management processes, and improve decision-making quality.

At the initial stage, Ukrainian companies used intelligent technologies to automate routine processes such as accounting, warehouse management, logistics, and customer service. Chatbots for customer support and demand forecasting systems became the first AI tools in business [26–29].

The financial sector, retail, logistics, agribusiness, and manufacturing hold the greatest potential for AI implementation in Ukraine. Banks use AI for fraud detection and credit scoring, while agricultural companies apply it for crop yield forecasting and resource optimization.

Despite active adoption, Ukrainian businesses face a number of challenges – a shortage of qualified specialists, high technology costs, low levels of digital culture in enterprises, and an underdeveloped legal framework for AI usage. These factors slow down the large-scale and effective implementation of intelligent technologies.

Government initiatives, such as business digitalization programs and the creation of innovation hubs, support the development of intelligent technologies. AI development centers, startup accelerators, and training programs preparing specialists for the Ukrainian market are emerging in major cities.

The introduction of intelligent technologies enables Ukrainian companies to increase productivity, optimize processes, and make strategic decisions based on accurate data. This is particularly important in the context of economic instability and international competition, where the speed and accuracy of managerial decisions determine business success. In the long term, intelligent technologies

will become a key factor of competitiveness for Ukrainian enterprises. Their mass adoption will contribute to production automation, the development of personalized services, more accurate market forecasting, and Ukraine's integration into the global digital economy.

Table 1.1 – Types of Intelligent Technologies [30; 34]

Business Sector	Types of Intelligent Technologies	Main Functions	Business Effect
Finance and Banking	AI systems for credit scoring, fraud detection, big data analytics	Assessment of clients' creditworthiness, automatic detection of fraudulent transactions, forecasting financial risks	Reduction of financial losses, enhanced security, more effective risk management
Retail	Recommendation systems, customer behavior analytics, chatbots	Personalization of offers, demand forecasting, automation of customer service	Increased sales, improved customer experience, inventory optimization
Logistics	AI for route optimization, warehouse management, demand forecasting	Delivery route planning, inventory management, warehouse automation	Reduced logistics costs, faster delivery, more efficient use of resources
Agribusiness	Yield prediction, soil monitoring, automated equipment management	Assessment of soil and crop conditions, yield forecasting, optimization of fertilizer application	Increased productivity, resource savings, reduced risk of losses
Manufacturing	Robotics, AI quality control, predictive maintenance	Automation of production processes, quality monitoring, failure prediction	Cost reduction, increased productivity, minimized downtime
Startups and IT	Machine learning, chatbots, data analytics	Product development, service automation, market analysis	Accelerated product development, improved competitiveness, attraction of investments

Intelligent technologies, particularly artificial intelligence, have become a key factor in the development of modern business in Ukraine. They enable companies to adapt more rapidly to market changes, enhance management efficiency, and create new competitive advantages.

Different sectors of the economy demonstrate varying rates of AI implementation. Finance, retail, and agribusiness actively use these technologies for analytics, forecasting, and automation of routine processes, while some manufacturing companies are only beginning to integrate intelligent systems.

In the current context of digital transformation, various economic sectors show uneven rates of intelligent technology adoption. This is determined by industry specifics, the level of digital maturity of enterprises, financial capacity, and access to skilled professionals. The most active implementation occurs in areas with large data volumes, where the speed of decision-making determines competitive advantage.

The leaders in adoption are the financial sector, IT industry, telecommunications, logistics, and e-commerce. These industries respond quickly to innovation, possess flexible business models, and focus on customer centricity. For them, intelligent technologies mean improved forecasting accuracy, cost reduction, better service personalization, and lower risks.

In manufacturing and energy, intelligent technologies are used to optimize production processes, automate quality control, improve energy efficiency, and predict equipment failures. Although the pace of implementation is slower, the effect of intellectualization is significant – particularly in the context of Industry 4.0.

In healthcare, education, and public administration, progress is gradual. Major barriers include high solution costs, shortage of specialists, and the need for personal data protection. However, these sectors possess the greatest social potential for intelligent technologies – they can enhance diagnostic accuracy, ensure personalized learning, and improve public service efficiency [38].

The agricultural sector is implementing intelligent technologies through precision farming systems, yield monitoring, weather forecasting, and market analytics. Although adoption remains limited, agribusiness is becoming one of the most promising areas for intelligent technology development in the medium term [40–46].

Thus, different branches of the economy exhibit asynchronous digital development; however, the general trend is clear – intelligent technologies are becoming a universal tool for increasing efficiency, transforming business models, the labor market, and the competitive environment (see Table 1.2, p. 11).

The implementation of intelligent technologies allows enterprises to optimize internal processes such as warehouse management, logistics, customer service automation, and demand forecasting. As a result, companies reduce costs and improve productivity.

The concept of intelligent technologies (ITech) has evolved significantly over the past decades, reflecting the interdisciplinary convergence of computer science, cognitive studies, and management theory. Although there is no single universally accepted definition, most scholars agree that intelligent technologies combine elements of artificial intelligence, data analytics, and adaptive systems to support decision-making and problem-solving in dynamic environments.

According to O. Kosenko, I. Dolyna, and P. Pererva (2023), intelligent technologies represent an integrated approach that unites intellect, innovation, and technology. They define them as technological systems capable of combining human-like reasoning, adaptive learning, and analytical functionality to enhance management efficiency and respond flexibly to environmental changes. This definition emphasizes the hybrid nature of intelligent technologies – combining technical algorithms with human cognitive models.

O. Bilotserkivskyi and I. Sosnov (2022) interpret intelligent technologies as intelligent information systems that integrate data processing, machine learning, and expert knowledge for supporting managerial and strategic decisions. Their focus lies on the functional

Table 1.2 – Pace of Implementation of Intelligent Technologies in Economic Sectors [48]

Economic Sector	Examples of Intelligent Technology Applications	Implementation Level	Expected Effect	Main Barriers
Financial Sector	Client data analytics, credit scoring, chatbots, fraud detection systems	High	Risk reduction, service personalization, cost savings	Cyber threats, regulatory constraints
IT and Telecommunications	Service automation, intelligent networks, user behavior analytics	Very high	Improved service quality, network optimization	High competition, need for constant innovation
Industry (Industry 4.0)	Robotics, predictive analytics, quality control, digital twins	Medium-high	Production optimization, cost reduction	High implementation cost, shortage of personnel
Agricultural Sector	Precision farming, drones, yield forecasting, market analytics	Medium	Higher productivity, resource efficiency	High technology cost, weak infrastructure
Healthcare	Medical diagnostic systems, image analysis, epidemic forecasting	Medium	Better treatment quality, fewer errors	Data protection, ethical issues
Education	Personalized learning, adaptive platforms, knowledge assessment	Medium	Individualized educational process	Insufficient funding, low digital literacy
Public Administration	E-services, data analytics, social process forecasting	Low – medium	Greater efficiency and transparency	Bureaucracy, limited resources

dimension – how such systems perform analysis, forecasting, and decision-making within complex business or administrative contexts.

From a more philosophical standpoint, A. Yarovyi (2020) considers intelligent technologies as a part of the broader evolution of human cognition, linking them to the interaction between rational and imaginative thinking. In his view, intelligent systems are not merely computational tools but extensions of human intelligence that reshape cognitive paradigms and transform modes of reasoning.

In the context of digital transformation, international organizations such as UNESCO (2023) and the OECD (2021) define intelligent technologies as a *set of* digital solutions capable of perceiving, analyzing, learning, and acting autonomously, thereby supporting innovation, governance, and social progress. This definition broadens the interpretation from a purely technical domain to one that includes ethical, social, and economic implications.

In practical terms, intelligent technologies encompass a range of digital tools and methodologies, including:

– Artificial Intelligence (AI) – systems that simulate cognitive functions such as learning, reasoning, and problem-solving;

– Machine Learning (ML) – algorithms that enable systems to improve performance through experience and data analysis;

– Neural Networks – computational models inspired by the structure of the human brain, capable of recognizing complex patterns;

– Natural Language Processing (NLP) – tools for understanding, generating, and analyzing human language;

– Big Data Analytics – technologies for processing and interpreting massive datasets to extract actionable insights;

– Robotic Process Automation (RPA) – systems that automate repetitive tasks, enhancing efficiency and accuracy.

Relevance of Intelligent Technologies

The relevance of intelligent technologies in the 21st century is determined by the rapid digitalization of all spheres of life, the growing complexity of global systems, and the need for timely

and evidence-based decision-making. Modern economies, governance structures, and societies increasingly rely on data-driven intelligence to function effectively in uncertain and volatile environments.

Firstly, intelligent technologies have become a core driver of digital transformation in both the public and private sectors. They enable the automation of administrative processes, predictive analytics, and real-time monitoring of economic and social trends. This leads to increased efficiency, transparency, and accountability – essential elements of good governance.

Secondly, in the context of national information security, intelligent technologies play a vital role in identifying and countering cyber threats and disinformation campaigns. AI systems can analyze vast information streams, detect fake content, and prevent the spread of harmful narratives that threaten social stability and trust. This function has become especially relevant during hybrid wars and information conflicts, where technological superiority often determines strategic success.

Thirdly, intelligent technologies are essential for economic recovery and innovation-led growth. In post-crisis or post-war conditions, they support the optimization of production and logistics, enhance financial risk management, and improve market forecasting. Through machine learning and predictive analytics, enterprises can adapt to rapidly changing conditions, ensuring resilience and competitiveness in the global economy.

Fourthly, intelligent technologies have profound implications for human capital development. They foster the creation of digital education systems, personalized learning environments, and skill-training platforms based on AI. This contributes to building a knowledge-based society capable of continuous learning and adaptation – a critical requirement in an age of automation and global competition.

Moreover, the ethical and legal dimensions of intelligent technologies underscore their societal relevance. As automation expands, questions of transparency, accountability, and human oversight become central

to sustainable innovation. International institutions such as the European Commission (2022) and UNESCO (2023) stress the importance of ensuring that AI and related technologies are aligned with democratic values, privacy rights, and social responsibility.

In summary, intelligent technologies represent a multidimensional phenomenon that integrates technical, cognitive, and social components. Their relevance extends beyond technological advancement – they shape how societies communicate, govern, produce, and learn. For Ukraine and other nations undergoing transformation, the adoption of intelligent technologies is not merely a matter of modernization but a strategic imperative for ensuring national security, economic resilience, and global competitiveness.

Thus, intelligent technologies stand at the intersection of innovation and security, defining the trajectory of sustainable development in the digital era. Their integration into state governance, industry, and education creates the foundation for a resilient, adaptive, and future-oriented society capable of thriving in the conditions of uncertainty and rapid technological change.

AI technologies help Ukrainian companies strengthen competitiveness in domestic and international markets. Through big data analysis and market trend forecasting, businesses can respond faster to changes, offer personalized products, and reduce the risk of poor decisions.

However, alongside advantages, there are notable challenges. A shortage of qualified professionals, high implementation costs, and low levels of digital culture within enterprises slow down widespread adoption of intelligent technologies. Overcoming these barriers requires a comprehensive approach and state support.

Government programs for digitalization and the development of innovation centers contribute to the acceleration of intelligent technology adoption. Accelerators, educational programs, and startup hubs provide businesses with qualified talent and new technological solutions, fostering innovative growth.

Thus, intelligent technologies in Ukrainian business are already shaping new standards of efficiency and competitiveness. They enable process optimization, enhance decision-making quality, and open prospects for enterprise development within the global economy. Continued investment in AI and human capital development will become the key drivers of sustainable growth for Ukrainian business.

In both scientific and practical dimensions, intelligent technologies are regarded not merely as a set of tools but as a strategic resource for organizational development. Their implementation requires the integration of technical, organizational, and cognitive approaches that enable the creation of next-generation intelligent systems. These form the foundation for transitioning toward an intelligent economy – one in which knowledge is the primary resource, and the key success factor is the ability of systems to learn and adapt to dynamic environmental changes.

Table 1.3 – Classification of Intelligent Technologies by Key Characteristics

Classification Criterion	Types of Intelligent Technologies	Description
By Level of Intelligence	Weak AI, Strong AI	Weak AI performs specific tasks (image recognition, forecasting), while strong AI is capable of independent reasoning and generalizing knowledge
By Learning Method	Supervised, Unsupervised, Reinforcement Learning	Differ in the degree of human involvement in the algorithm's training process
By Field of Application	Business analytics, marketing, medicine, education, security, etc.	Used for automation, analytics, and decision support across various industries
By Algorithm Type	Neural networks, expert systems, genetic algorithms, fuzzy logic	Define the technical foundation of intelligent technologies and methods of data processing
By Degree of Autonomy	Automated, semi-autonomous, autonomous systems	Differ in their level of independence in decision-making and interaction with the environment

As shown in Table 1.1, intelligent technologies have a multidimensional structure that reflects various approaches to their classification. Depending on the level of intelligence, they may perform narrowly specialized functions (weak artificial intelligence) or comprehensively replicate human cognitive processes (strong artificial intelligence).

According to the learning method, technologies are divided into those that are trained under human supervision, self-trained, or trained through reinforcement, which determines their adaptability to environmental changes. The field of application is an important criterion, as intelligent solutions are widely used in business, medicine, education, transportation, marketing, and public administration.

From an algorithmic perspective, such technologies are based on various methods – from neural networks and expert systems to genetic algorithms and fuzzy logic. Finally, by the degree of autonomy, systems can operate under operator supervision, semi-autonomously, or fully autonomously [22].

This classification allows for a comprehensive assessment of the potential of intelligent technologies and helps justify the selection of their optimal type for specific managerial tasks.

As illustrated in Table 1.1, intelligent technologies form a multi-level system that integrates different approaches to information processing, interpretation, and utilization. According to the level of intelligence, technologies can be weak, performing a specific function (e.g., speech recognition, data analysis, demand forecasting), or strong, capable of modeling complex cognitive processes and making decisions under uncertainty.

By learning method, intelligent technologies encompass a wide range of approaches – from supervised learning, where the system uses predefined data samples, to unsupervised learning or reinforcement learning, which is based on receiving rewards for correct actions. This allows models to adapt to new conditions and optimize decisions based on accumulated experience.

The scope of intelligent technologies spans almost all areas of human activity. In marketing management, they are used to analyze consumer behavior, forecast demand, detect fake information, and manage reputational risks. In medicine, they support disease diagnostics and clinical decision-making; in education, they enable personalized learning; and in business, they drive analytics and process optimization.

Depending on the algorithmic foundation, intelligent technologies are based on neural networks, genetic algorithms, fuzzy logic methods, expert systems, or hybrid models that combine multiple approaches. Each has its advantages – for instance, neural networks are effective in pattern recognition, while expert systems excel in modeling decision-making logic.

Table 1.4 – Dynamics of Intelligent Technology Implementation in Economic Sectors of Ukraine (2023–2024) [33–40]

Economic Sector	2023	2024
Financial Sector	75%	85%
IT and Telecommunications	70%	80%
Industry and Energy	60%	75%
Agricultural Sector	55%	70%
Healthcare	50%	65%
Education	45%	60%

The dynamics of intelligent technology implementation in various sectors of Ukraine's economy from 2023 to 2024 demonstrate a gradual increase in the level of digitalization and integration of innovative solutions. The overall trend indicates that nearly all industries are beginning to use intelligent technologies to optimize processes, improve productivity, and reduce risks.

The financial sector in 2023 already showed a high level of AI use for data analytics, credit scoring, and fraud detection (75%). In 2024, this figure rose to 85%, driven by the need for greater accuracy in managerial decisions and more personalized financial services.

The IT and telecommunications sector increased from 70% to 80%, linked to the development of cloud platforms, network infrastructure, and the integration of AI into customer service systems to improve service quality.

In industry and energy, the adoption level grew from 60% to 75%, reflecting active use of digital twins, automated production lines, and predictive analytics systems that optimize production, reduce costs, and improve efficiency.

The agricultural sector showed growth from 55% to 70% due to the use of drones, precision farming systems, and AI analytics for yield forecasting and resource management.

Overall, this upward trend highlights the acceleration of intelligent technology adoption as a key driver of Ukraine's economic digital transformation and competitiveness on global markets.

In the healthcare sector, the implementation of intelligent technologies increased from 50% to 65%. This growth is associated with the use of AI for diagnostics, personalized treatment, medical image analysis, and process optimization in medical institutions. Education and public administration demonstrate lower but steady growth rates – from 45% to 60% and from 40% to 55%, respectively. The main barriers in these sectors include limited funding, low levels of digital literacy, and the need for regulatory frameworks.

Overall, the analysis demonstrates an asynchronous implementation of intelligent technologies across various sectors; however, the general trend toward digitalization and intellectualization is evident. The leading sectors set standards for others, which gradually adopt innovative practices, creating a systemic effect on the transformation of Ukraine's economy. Thus, the dynamics of intelligent technology adoption indicate that the intellectualization of the economy is becoming a key factor in improving the competitiveness and efficiency of Ukrainian enterprises. Continued investment in digital technologies and workforce training will ensure sustainable development across all economic sectors.

The dynamics of intelligent technology implementation in various sectors of the Ukrainian economy during 2023–2024 demonstrate a steady increase in the level of digitalization and the integration of innovative solutions. This trend reflects a broader global shift toward data-driven decision-making, automation, and artificial intelligence (AI)-assisted management. Almost all industries in Ukraine have begun to recognize the strategic importance of intelligent technologies in improving efficiency, optimizing processes, and mitigating operational and economic risks.

In 2023, the financial sector already exhibited one of the highest levels of AI adoption among Ukrainian industries. Approximately 75% of financial institutions were actively using intelligent technologies for data analytics, credit scoring, fraud detection, and customer behavior modeling. By 2024, this figure rose to 85%, driven by the growing need for precise decision-making, personalization of financial services, and protection against cyber and fraud risks. The rapid development of fintech solutions and AI-based risk management systems has significantly transformed the competitiveness and transparency of Ukraine's financial ecosystem.

The information technology (IT) and telecommunications sector also showed impressive growth, with the level of intelligent technology integration rising from 70% in 2023 to 80% in 2024. This increase is attributed to the expansion of cloud platforms, network infrastructure modernization, and the integration of AI into customer service systems and digital communication tools. The sector's progress has been largely supported by private investment, the development of IT clusters, and the active participation of Ukrainian specialists in international AI projects.

The industrial and energy sectors experienced a notable technological acceleration during this period. The implementation level of intelligent technologies grew from 60% to 75%, reflecting active adoption of digital twins, predictive analytics, and automated production systems. These innovations have allowed enterprises to reduce production costs,

enhance resource efficiency, and improve energy management. AI-based predictive maintenance has been particularly effective in preventing equipment failures and minimizing downtime in critical industries such as metallurgy and energy production.

The agricultural sector demonstrated an equally remarkable digital transformation, with the integration of intelligent systems increasing from 55% to 70%. This growth has been driven by the adoption of drones, precision farming technologies, and AI analytics for crop forecasting and resource management. The use of intelligent solutions in agriculture has improved productivity, reduced resource waste, and increased the resilience of Ukraine's agri-food sector amid climate change and post-war recovery challenges.

In the healthcare sector, the implementation of intelligent technologies rose from 50% in 2023 to 65% in 2024. AI tools are increasingly applied for medical diagnostics, personalized treatment planning, and the analysis of medical imaging. Intelligent hospital management systems have also been introduced to optimize administrative workflows, manage patient data, and forecast demand for medical services. These changes contribute not only to the quality of healthcare but also to the efficiency and sustainability of Ukraine's health infrastructure.

The education sector is also gradually embracing intelligent technologies, though at a slower pace. Between 2023 and 2024, AI adoption in education increased from 45% to 60%. This progress is mainly due to the introduction of AI-driven learning platforms, virtual classrooms, and adaptive learning systems. Such tools have transformed traditional pedagogical models by enabling personalized education and improving students' digital literacy – crucial for preparing the workforce of the future.

The public administration sector lags slightly behind other industries but still shows a positive trend, growing from 40% in 2023 to 55% in 2024. The main drivers of this growth include the automation of government services through RPA (Robotic Process

Automation), the introduction of AI chatbots for citizen interaction, and the development of e-governance systems. These initiatives have improved service delivery efficiency, transparency, and public trust in government institutions.

Despite these positive trends, several barriers still hinder the widespread implementation of intelligent technologies across Ukraine's economy. Among the most significant challenges are limited access to financing, insufficient digital infrastructure in rural areas, and the shortage of qualified specialists in AI, data science, and cybersecurity. Furthermore, many organizations face difficulties in integrating AI into existing business models due to outdated management structures and a lack of long-term innovation strategies.

Another key obstacle is the regulatory framework. The rapid development of AI technologies requires timely adaptation of national legislation to ensure data privacy, ethical use of algorithms, and cybersecurity compliance. In Ukraine, regulatory initiatives are still evolving, which slows down large-scale adoption in sectors such as healthcare, education, and public administration. The creation of comprehensive AI governance standards remains one of the priority tasks for policymakers.

However, despite these constraints, the overall dynamics indicate a clear upward trajectory. The continuous integration of intelligent technologies contributes to Ukraine's transition toward a digital economy, enhances productivity, and fosters innovation-driven growth. By combining domestic expertise with international partnerships, Ukraine is gradually building a sustainable AI ecosystem that can compete on the global stage.

The increasing role of intelligent technologies in different sectors has also created new opportunities for cross-sectoral synergy. For example, AI systems developed for finance can be adapted to healthcare analytics, while predictive models from the energy industry can be applied to logistics and agriculture. This convergence enhances innovation diffusion, reduces costs, and stimulates

the creation of integrated digital platforms that serve both private and public interests.

From a macroeconomic perspective, the rising adoption of intelligent technologies strengthens Ukraine's competitiveness and economic resilience. AI-supported decision-making enables more efficient use of national resources, better crisis management, and improved investment planning. These technologies also attract foreign investors who view Ukraine as a promising hub for technological innovation and digital entrepreneurship.

At the same time, intelligent technologies have significant social implications. They promote transparency, reduce corruption risks, and improve access to services in healthcare, education, and public administration. By fostering digital inclusion and technological awareness, they contribute to the development of a knowledge-based society. In post-war conditions, these processes are especially crucial for rebuilding public trust, restoring institutions, and shaping a new model of governance based on data and accountability.

In conclusion, the dynamics of intelligent technology implementation in Ukraine during 2023–2024 illustrate a critical stage in the country's digital transformation. Every major sector – from finance and industry to agriculture, healthcare, and education – is integrating AI and related tools to improve efficiency and resilience. Although challenges remain, the trend is irreversible: intelligent technologies have become not just instruments of modernization but key drivers of national recovery, security, and sustainable growth. Their continued expansion promises to reinforce Ukraine's global competitiveness, strengthen its information security, and accelerate the creation of an innovation-oriented economy capable of thriving in the digital age.

The criterion of autonomy determines the degree of system independence – from simple automated solutions that assist users to autonomous systems capable of independently analyzing situations, making decisions, and executing them. This level of autonomy is critical for ensuring safety, reliability, and ethical responsibility in the use of AI.

Hence, the classification of intelligent technologies allows for systematization by key characteristics, determination of application opportunities in different industries, and assessment of their maturity level. Comprehensive use of these technologies contributes to the creation of intelligent management systems that improve organizational efficiency, reduce disinformation risks, and ensure a qualitatively new level of analytics in decision-making processes.

Intelligent technologies have become an integral component of the modern knowledge economy. Their implementation provides enterprises with new opportunities for development, enabling more efficient resource use and the creation of innovative business models. In the context of global digital transformation, intelligent systems are becoming the foundation of enterprises' competitive advantages.

One of the main advantages of intelligent technologies is the optimization of management processes. The use of artificial intelligence algorithms enables the analysis of large data volumes, identification of hidden patterns, and the formulation of management decisions based on accurate information. This shortens decision-making time and improves precision.

Intelligent systems allow the automation of typical and repetitive tasks – from accounting to order processing and customer inquiries. This frees employees from routine work, allowing them to focus on strategic objectives that enhance business value.

The use of intelligent technologies helps reduce operating costs. AI systems optimize logistics chains, energy use, raw material consumption, and labor resources. Companies can increase productivity without significant cost growth, positively impacting financial performance.

Intelligent technologies ensure a personalized approach to clients. Data analytics systems and chatbots make it possible to create individualized offers, respond quickly to requests, and enhance customer experience, fostering satisfaction and loyalty.

AI technologies can predict consumer behavior, demand fluctuations, currency changes, or market trends. Such analytical tools help businesses develop effective marketing strategies, mitigate risks, and respond faster to environmental changes.

Intelligent technologies also facilitate the creation of new products and services. They enable companies to analyze consumer needs, model market behavior scenarios, and test concepts before implementation, significantly reducing the time-to-market and improving product quality.

AI solutions are actively used for cybersecurity monitoring, fraud detection, and risk management. Through machine learning, systems can recognize suspicious activities in real time, reducing data leakage and financial loss risks. Intelligent technologies contribute not only to operational management but also to strategic planning, allowing modeling of enterprise development scenarios, analysis of external and internal factors, and justification of long-term decisions.

Thus, intelligent technologies are a powerful tool for increasing the efficiency, flexibility, and competitiveness of Ukrainian business. Their application enables resource optimization, improved management quality, innovation development, and sustainable enterprise growth in the digital era. In the future, their influence will only increase, shaping a new economic reality where knowledge, analytics, and automation become the main drivers of success.

Intelligent technologies represent a set of methods, algorithms, and software tools that enable computer systems to identify, analyze, and interpret data similarly to human thinking. They are aimed at automating decision-making, learning, and performance forecasting based on large volumes of data. These technologies rely on artificial intelligence, machine learning, neural networks, expert systems, natural language processing, computer vision, and other tools that allow systems to acquire new knowledge through interaction with their environment. Their application covers management, education, healthcare, economics, defense, and social communications. The key

feature of intelligent technologies is their ability to self-learn and adapt, distinguishing them from traditional information technologies. They not only perform programmed actions but also improve their algorithms, optimizing analysis, forecasting, and management processes depending on environmental changes. The use of intelligent technologies enhances the efficiency of managerial, production, and marketing processes, contributes to digital transformation, and fosters the formation of intellectual capital within organizations. They form the foundation for developing smart systems, digital governance, and an innovative knowledge economy.

Table 1.5 – Definitions of Intelligent Technologies [50–51]

Author	Definition of Intelligent Technologies
Voronkova V. H.	Intelligent technologies are viewed as a set of artificial intelligence methods and tools that provide information systems with the ability to perceive, analyze, and make decisions based on knowledge. According to the researcher, they form the foundation of the current stage of scientific and technological progress focused on the creation of intelligent systems for managing socio-economic processes
Cherep A. V.	The scholar defines intelligent technologies as a set of software and algorithmic tools that simulate human cognitive functions – thinking, learning, recognition, analysis, and forecasting. They contribute to the development of managerial innovations, optimization of business processes, and improvement of decision-making quality
Gorwa R. & Ash T.	The authors interpret intelligent technologies as integrated data-processing systems that apply artificial intelligence methods to automate information analysis, identify patterns, and forecast the behavior of socio-economic systems. They emphasize the role of intelligent technologies in combating disinformation and fostering digital trust
Canale N. & Messina M.	The authors define intelligent technologies as a complex of interrelated AI methods implementing analytical thinking, data-driven learning, and adaptive management in uncertain environments. They consider such technologies a key factor in the digital transformation of the economy and society

Additional Definitions:

– Intelligent technologies are a set of methods, algorithms, and software tools aimed at modeling human thought processes to solve complex tasks requiring analysis, forecasting, learning, and decision-making [25].

– Intelligent technologies represent a combination of hardware and software tools that enable big data processing, self-analysis, and self-learning to improve management, production, and communication efficiency [26].

– Intelligent technologies in business are innovative digital solutions that use artificial intelligence, machine learning, neural networks, and data analytics to optimize resources, automate processes, and support managerial decisions [27].

– Intelligent technologies are instruments of intellectual management support that ensure systemic analysis, result forecasting, and selection of optimal solutions under complex economic conditions [28].

– Intelligent technologies are an element of the information society that contributes to forming a new quality of labor, digital human-machine interaction, and the creation of a knowledge-based economy [29].

– Intelligent technologies are the practical application of AI tools capable of analyzing data, forecasting market trends, and making management decisions without direct human intervention.

– Intelligent technologies are innovative digital systems capable of self-learning, analytics, and adaptation that support managerial decision-making, enhance business process efficiency, and develop competitive advantages for enterprises in the context of digital economic transformation.

1.2. THEORETICAL APPROACHES TO THE STUDY OF DISINFORMATION IN WARTIME CONDITIONS

Disinformation is the deliberate dissemination of false or distorted information with the purpose of manipulating public opinion, undermining trust in institutions, or achieving strategic objectives. It differs from propaganda in that it is usually disguised as truthful messages, combines elements of factuality and fabrication, and employs psychological mechanisms of audience influence.

Disinformation in wartime aims to demoralize the population, disorganize the enemy, and construct controlled narratives to achieve strategic results. Modern conflicts-especially hybrid and information wars – demonstrate the high effectiveness of disinformation campaigns. The spread of fake news through social networks, messengers, and other digital platforms poses a threat to national security, influences economic stability, and weakens social cohesion [65–69].

Under wartime conditions, information counteraction becomes as important as military action, since control over the information space determines the moral state of society and the effectiveness of governmental decision-making.

Disinformation is a multidimensional phenomenon that combines psychological, social, technological, and legal aspects. Its study involves several scientific approaches: information-psychological, social-constructivist, political-communicative, digital-technological, and normative-legal. Each of these approaches highlights a specific dimension of the problem and enables the development of comprehensive strategies for counteraction [66].

Disinformation is the deliberate dissemination of false or distorted information intended to manipulate public opinion, undermine trust in institutions, or achieve specific political, military, or strategic goals. Unlike simple misinformation, which may result from misunderstanding or error, disinformation is intentionally

designed and systematically implemented to deceive and influence target audiences. It often blends factual elements with fabricated or selectively edited content, creating an illusion of credibility that makes it more persuasive and difficult to detect.

Disinformation differs from propaganda in its methods and appearance. While propaganda is typically open in its intent to persuade or mobilize, disinformation conceals its manipulative purpose under the guise of authenticity. It frequently employs techniques such as emotional framing, partial truths, and false equivalencies to erode rational judgment and foster confusion. Through this hybrid structure – part truth, part fabrication – disinformation effectively exploits the cognitive biases and emotional vulnerabilities of individuals, making it one of the most powerful tools in modern psychological and informational warfare.

In wartime conditions, disinformation acquires heightened strategic significance. It is not only a weapon of information warfare but also an instrument of psychological and moral influence. Its primary objectives include the demoralization of the civilian population, disorganization of the adversary's command structures, and the formation of controlled narratives that legitimize certain actions or conceal strategic failures. By shaping perceptions of reality, disinformation helps to weaken resistance, disrupt communication channels, and influence both domestic and international audiences.

The mechanisms of disinformation are multidimensional. At the psychological level, it manipulates fear, uncertainty, and social identity. At the technological level, it utilizes digital platforms, social networks, bots, and artificial intelligence to amplify content and target specific audience groups with tailored messages. At the political level, it seeks to erode democratic governance by undermining confidence in media, government, and expert institutions. The combination of these mechanisms creates an environment of cognitive overload, where individuals struggle to distinguish between verified facts and constructed fictions.

Modern disinformation campaigns often exploit the logic of information virality – the faster and more emotionally charged the content, the more likely it is to spread uncontrollably. Digital ecosystems, characterized by algorithmic personalization and echo chambers, enhance this effect by isolating users within ideologically homogeneous groups. This structural feature of online communication makes societies more susceptible to manipulation, polarization, and social fragmentation.

In the context of hybrid and information wars, disinformation becomes a strategic component of non-kinetic operations. It complements military, economic, and diplomatic efforts by influencing perceptions, weakening morale, and sowing distrust. For example, in modern conflicts, state and non-state actors employ coordinated disinformation campaigns to distort international narratives, justify aggression, or delegitimize opposing governments. Thus, control over the information space becomes as vital as control over physical territory.

The targets of disinformation are diverse – from individual citizens and social groups to media institutions, governmental agencies, and international organizations. Its impact extends beyond the immediate battlefield, shaping long-term attitudes, social cohesion, and the credibility of democratic systems. Moreover, disinformation's ability to adapt and evolve through technology – including deepfakes, AI-generated content, and microtargeting – has dramatically increased its efficiency and global reach.

Scholars emphasize that disinformation represents not only a communication challenge but also a systemic societal threat. It corrodes the epistemic foundations of public discourse, undermines trust in expertise, and destabilizes democratic deliberation. By spreading cynicism and relativism, it weakens the collective capacity to respond rationally to crises – whether political, economic, or military.

Consequently, the fight against disinformation requires a multidisciplinary approach combining technological tools, media

education, psychological resilience, and legal regulation. Artificial intelligence plays an increasingly important role in identifying disinformation patterns, verifying content authenticity, and monitoring the spread of fake narratives. However, technological solutions must be complemented by societal efforts to foster critical thinking, media literacy, and institutional transparency.

In the case of Ukraine, the confrontation with disinformation has become a central element of national information security. During wartime, Russian disinformation campaigns target both the domestic population and the international community, seeking to distort perceptions of the conflict and weaken global support. Ukraine's response – through fact-checking initiatives, strategic communication, and AI-based monitoring systems – demonstrates the growing integration of intelligent technologies in countering information warfare.

In summary, disinformation is a complex hybrid phenomenon that combines psychological manipulation, technological amplification, and strategic intent. Its ultimate goal is not merely to misinform but to control narratives, shape realities, and influence decisions at both individual and institutional levels. Understanding its mechanisms and developing effective countermeasures are essential not only for safeguarding national security but also for preserving the integrity of democratic discourse in the digital era.

Table 1.6 – Theoretical Approaches to the Study of Disinformation in Wartime Conditions [70–73]

Approach	Key Features	Research Focus
1	2	3
Information-Psychological	Considers disinformation as a tool for psychological influence and manipulation of collective consciousness. Emphasizes emotional triggers, cognitive biases, and mechanisms of persuasion	Analysis of information attacks, emotional contagion, and audience susceptibility

End of Table 1.6

1	2	3
Social-Constructivist	Views disinformation as a product of social interaction and narrative construction within specific communities	Study of the formation of collective meanings, identity manipulation, and trust erosion in information sources
Political-Communicative	Examines disinformation as an instrument of political struggle and hybrid warfare, aimed at controlling public discourse and legitimizing power	Research on political narratives, media framing, and communication strategies during conflict
Digital-Technological	Focuses on the technological means of creating and disseminating false information, including AI-generated content, bots, and algorithms	Development of AI-based detection systems, analysis of digital platforms, and data verification technologies
Normative-Legal	Interprets disinformation as a violation of information security and public order; studies legal frameworks and international mechanisms of regulation	Formation of legal norms, international standards, and mechanisms for countering information aggression

The information-psychological and social-constructivist approaches allow for a deeper understanding of the mechanisms of audience influence, yet they pay less attention to the technological aspect.

The digital-technological approach is effective for practical counteraction in the digital environment but requires integration with legal and psychological strategies.

The multidisciplinary approach demonstrates the most comprehensive understanding of disinformation, combining various levels of influence and counteraction tools.

Disinformation is the deliberate dissemination of false or partially distorted information aimed at manipulating public opinion,

demoralizing the opponent, or achieving strategic objectives. Although disinformation is generally perceived as a negative phenomenon, theoretical and applied research also considers it from the standpoint of strategic advantages for those who employ it.

Advantages of disinformation: a tool of psychological influence, a means of gaining strategic advantage, and a way to shape the behavior of target groups. Disadvantages of disinformation: moral and ethical risks, loss of trust, unpredictable consequences, technological and legal limitations.

Table 1.7 – Theoretical Approaches to the Study of Disinformation

Approach	Essence	Key Authors	Examples of Application
Information and Communication	Distortion of the communicative process; manipulation of information flows	H. Lasswell, M. Castells, J. McNair	Dissemination of fake news, manipulative messages
Information-Psychological	Influence on consciousness and behavior through emotions and cognitive biases	D. Kahneman, O. Ovsiienko	Panic, fear, demoralization of the population
Social-Constructivist	Disinformation as a social construct and a struggle for the "interpretation of reality"	P. Berger, T. Luckmann, M. Foucault	Formation of alternative war narratives
Political-Communicative	Instrument of political influence and propaganda	J. Ellul, E. Noelle-Neumann	Propaganda media, symbols, slogans
Digital-Technological	Use of algorithms, bots, and artificial intelligence for dissemination or detection	R. Gorwa, N. Canale	Deepfakes, bot networks, automated monitoring
Normative-Legal	Institutional and legal mechanisms of counteraction	V. Petrenko, European Commission	Media regulation, blocking of harmful sources
Multidisciplinary	Integration of psychological, social, technological, and legal aspects	UNESCO, J. Wardle	Comprehensive information security strategies

Disinformation in wartime conditions is not a random phenomenon but a deliberate and systematic strategy that aims to influence perceptions, destabilize societies, and achieve political or military objectives without direct confrontation. The academic study of disinformation encompasses several theoretical and methodological approaches, each of which reveals different dimensions of this complex phenomenon – communicative, psychological, social, political, technological, legal, and systemic.

The information-communication approach views disinformation primarily as a distortion of the communicative process and manipulation of information flows in the media and digital environment. Drawing on the classical models of communication developed by Harold Lasswell, Manuel Castells, John McNair, and Heorhii Pocheptsov, this approach emphasizes that the sender of information in wartime deliberately alters or falsifies messages to influence the audience's interpretation. The main manifestations include organized information campaigns, fake news dissemination through social networks, and the substitution or fabrication of information sources to achieve control over public perception.

This approach helps explain how communication models, originally designed for peaceful social exchange, are transformed into tools of informational aggression. In modern conflicts, disinformation functions as a kind of "information weapon," where the message itself becomes a form of attack. Information-communication analysis therefore focuses on the study of narrative structures, framing, and message propagation

The information-psychological approach examines disinformation through the prism of human perception, emotions, and cognitive biases. Scholars such as Daniel Kahneman, Paul Slovic, O. Ovsiienko, and N. Kopylova highlight that human cognition is inherently prone to errors in judgment, emotional overreactions, and selective attention. Disinformation exploits these vulnerabilities to provoke fear, panic, apathy, or aggression. Typical examples include the spread

of panic-inducing messages during crises or the manipulation of social emotions to create a sense of threat or despair.

This approach allows researchers to identify how psychological mechanisms – such as confirmation bias, cognitive dissonance, and emotional contagion – amplify the effect of disinformation. In wartime, these mechanisms are weaponized to lower morale, break trust in institutions, and create a sense of helplessness among the population. Thus, the psychological study of disinformation is crucial for understanding its devastating social and emotional impact.

The social-constructivist approach, developed by theorists like Peter Berger, Thomas Luckmann, Michel Foucault, and Neil Postman, interprets disinformation as a social construct created through communication between power, media, and society. From this perspective, the concept of "truth" itself becomes contested, as different actors compete to impose their interpretation of reality. In wartime, this struggle manifests in the formation of alternative historical narratives, reinterpretation of events, and manipulation of memory.

Social constructivism demonstrates that disinformation is not merely false information – it is a mechanism of social reality construction. Competing narratives aim to legitimize one side's actions while delegitimizing the other. This approach is particularly relevant in hybrid warfare, where controlling the "information battlefield" is as important as controlling physical territory.

The political-communicative (propaganda) approach focuses on disinformation as a tool of political influence and ideological manipulation. Classical theorists such as Lasswell, Jacques Ellul, Elisabeth Noelle-Neumann, and Sergey Kara-Murza describe propaganda as a system of persuasive communication designed to shape mass consciousness and mobilize populations. In wartime, disinformation functions as an element of political strategy – mobilizing one's own citizens, demoralizing the enemy, and maintaining public support for military actions.

This approach highlights the interplay between propaganda and power. Disinformation becomes a political resource used to maintain legitimacy, justify aggression, or create an illusion of control. Through slogans, symbols, and emotionally charged media messages, governments and political actors can manipulate national sentiment and international opinion. Understanding this dynamic is key to analyzing information operations at the geopolitical level.

The digital-technological approach brings a modern dimension to the study of disinformation by focusing on the role of algorithms, bots, social media platforms, and artificial intelligence. Researchers such as Robert Gorwa, Tobias Ash, Nicola Canale, and Marco Messina emphasize that digital infrastructure now enables the automation and amplification of false narratives. Disinformation campaigns operate through algorithmic recommendation systems, bot networks, and AI-generated content (including deepfakes), creating self-reinforcing cycles of deception.

This approach is particularly relevant to the current era of information warfare, where technology allows both the production and detection of disinformation at unprecedented scales. AI-based monitoring systems can identify coordinated campaigns and analyze large data sets, while adversaries use the same technologies to generate sophisticated forgeries. The digital-technological perspective thus reveals disinformation as a technological as well as sociopolitical phenomenon.

The normative-legal approach addresses the institutional and legal mechanisms of countering disinformation, especially during states of emergency or armed conflict. Scholars such as V. Petrenko, along with organizations like the European Commission and OSCE, emphasize the need to balance freedom of speech with the protection of national security. In wartime, this balance is particularly delicate, as governments must regulate media activity, block hostile propaganda resources, and establish strategic communication centers while avoiding excessive censorship.

This legal perspective is vital for developing state-level strategies of information security. It provides the framework for legislative initiatives, media accountability, and international cooperation against disinformation. Moreover, it underscores that countering disinformation must respect human rights and democratic principles, ensuring transparency and proportionality in government actions.

The multidisciplinary or systemic approach integrates all previous perspectives, combining psychological, social, political, technological, and legal dimensions. Institutions such as UNESCO, as well as researchers Claire Wardle and Hossein Derakhshan, advocate for a holistic model of combating disinformation that includes education, technology, regulation, and civic engagement. This systemic view regards disinformation as a multifaceted ecosystem that must be addressed through coordinated national and international strategies.

In conclusion, the study of disinformation in wartime requires an interdisciplinary synthesis that bridges communication theory, psychology, sociology, political science, technology studies, and law. Each approach reveals a different aspect of the phenomenon, but only together can they explain how disinformation operates as a mechanism of influence and control. Understanding these approaches not only deepens theoretical comprehension but also guides the practical development of intelligent technologies and information security policies aimed at protecting societies from manipulation, ensuring democratic resilience, and strengthening national stability in the digital age.

Analytical Summary

1. The information-psychological and social-constructivist approaches provide a deeper understanding of audience influence mechanisms but give less attention to technological aspects.

2. The digital-technological approach is effective for practical counteraction in the digital environment but requires combination with legal and psychological strategies.

3. The multidisciplinary approach demonstrates the most comprehensive understanding of disinformation by integrating different levels of influence and counteraction tools.

Disinformation is the deliberate dissemination of false or partially distorted information aimed at manipulating public opinion, demoralizing the opponent, or achieving strategic goals. Although typically perceived as negative, theoretical and applied studies also consider it from the perspective of strategic advantages for actors who use it.

Table 1.8 – Advantages and Disadvantages of Disinformation

Indicator	Advantages	Disadvantages
Impact on the Audience	Ability to shape emotions and behavior of target groups	Increased tendency toward panic and fear; disruption of social stability
Strategic Utility	Can be used as an element of information warfare or competitive struggle	Risk of backfire; demoralization of one's own population
Technological Aspects	Use of digital platforms, bots, and algorithms for rapid dissemination	Vulnerability to fact-checking, exposure, and cyberattacks
Legal and Ethical Aspects	May create advantages in crisis or wartime conditions	Violation of laws, ethical conflicts, sanctions
Control and Adaptability	Allows testing of audience reactions and message adjustments	Difficult to control consequences; risk of losing trust and legitimacy

Interpretative Commentary

1. Audience influence: Disinformation can quickly alter public perception and behavior but may provoke panic or social conflict.

2. Strategic benefit: Used in military, political, or economic campaigns; however, it can backfire due to unpredictable outcomes.

3. Technological aspects: Digital tools accelerate dissemination but make disinformation vulnerable to exposure and blocking.

4. Legal and ethical aspects: Disinformation can bring short-term gains but entails risks of legal violations and ethical breaches.

5. Control and adaptability: Testing and adjusting messages enhance efficiency but make overall outcomes hard to predict [80–90].

Disinformation is therefore a dual phenomenon – capable of providing strategic advantages while simultaneously posing serious risks for its creators and society.

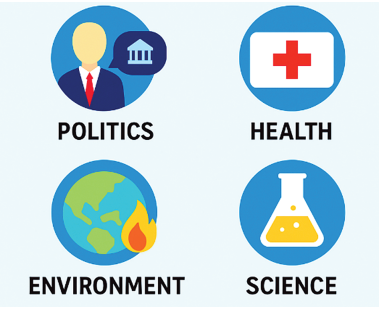

Figure 1.1 – Key Spheres of Information Influence: Politics, Health, Environment, and Science

Effective use or counteraction of disinformation is possible only through the integration of psychological, technological, and legal control mechanisms. Given its destructive consequences, counter-disinformation measures and media literacy are becoming crucial components of information security [74].

Theoretical Approaches to the Analysis of Disinformation

Information and Communication Approach

The earliest and most traditional is the information and communication approach, which interprets disinformation as a distortion of the communicative process, disrupting the balance between truthfulness, objectivity, and the intended influence of information. Within this framework, disinformation is viewed as a purposeful distortion of information flows to achieve political, military, or economic objectives [90–93]

According to the models of H. Lasswell and C. Shannon – W. Weaver, disinformation functions as noise or signal distortion that

disrupts the transmission of meaning between the sender and receiver. In wartime, this approach explains how information influence can be used as an element of hybrid warfare, shaping perceptions and reactions of the adversary

Information-Psychological Approach

Developed in the works of O. Ovsiienko, N. Kopylova, A. Maslow, G. Gerbner, and D. Kahneman, this approach emphasizes the psychological mechanisms of perception and interpretation of false information that activate cognitive biases and emotional reactions.

Disinformation, from this perspective, acts as a tool of psychological influence, provoking fear, panic, helplessness, or, conversely, aggression. It operates through three core mechanisms:

– emotional contagion;
– cognitive dissonance;
– social imitation.

In wartime, these mechanisms are used to reduce morale, undermine trust in institutions, and disrupt national unity.

Social-Constructivist Approach

Within the social-constructivist framework, disinformation is understood as a social construct emerging through the interaction between authority, media, and audiences. Reality, especially during wartime, is not seen as objective but rather constructed through information narratives, symbols, and discourses.

Military disinformation becomes part of the struggle for the interpretation of events, where opposing sides seek to impose their worldview. This approach is particularly relevant for analyzing information operations aimed at shaping alternative historical memories or delegitimizing state authority.

Political-Communicative (Propagandist) Approach

This approach views disinformation as an instrument of political influence and propaganda. Classical works by H. Lasswell, J. Ellul, E. Noelle-Neumann, and S. Kara-Murza emphasize that propaganda is not limited to spreading falsehoods but represents

a system of value-laden messages designed to manipulate mass consciousness.

In wartime contexts, disinformation serves to mobilize domestic audiences, demoralize the enemy, and create illusions of control or superiority. Hence, this approach links disinformation with political technologies, strategic communication, and media influence on both national and international levels.

Digital-Technological Approach

In the twenty-first century, the digital-technological approach has become increasingly widespread. It studies disinformation in the context of the algorithmization of information flows and digital communication platforms. According to Gorwa & Ash (2022), modern disinformation campaigns function as automated ecosystems in which bots, trolls, recommendation algorithms, and social media platforms create a self-reinforcing environment for the circulation of false information. Here, disinformation is viewed not only as content but as a technological process of information circulation supported by digital infrastructures.

In wartime, this is manifested in the creation of so-called "information explosions," manipulative videos (deepfakes), and the use of artificial intelligence for both the detection of and resistance to fake content.

Normative-Legal Approach

This approach examines institutional and legal mechanisms for countering disinformation, particularly under martial law. Scholars emphasize that states must seek a balance between freedom of expression and the protection of the information space from destructive content.

During wartime, this approach takes on a practical dimension through the establishment of government communication centers, fact-checking units, cybersecurity agencies, and legislative initiatives aimed at blocking information attacks and ensuring information sovereignty [93–95].

Synthesis of Approaches and the Modern Paradigm

Modern scholarship tends toward an integrative or systemic approach that combines information-psychological, socio-communicative, digital-technological, and legal dimensions of disinformation. Within this framework, disinformation is viewed as a multilevel system of influence, in which content, dissemination technology, and the context of perception form a unified field of manipulative impact [96].

Table 1.9 – Theoretical Approaches to the Study of Disinformation under Wartime Conditions [99–103]

Approach	Essence	Research Focus
Information-Psychological	Considers disinformation as a tool of psychological influence that manipulates emotions, cognition, and behavior	Study of cognitive biases, emotional contagion, and audience susceptibility
Social-Constructivist	Views disinformation as a social construct arising from the struggle for the interpretation of reality	Analysis of narrative formation, symbolic meaning, and trust in media
Political-Communicative	Examines disinformation as an instrument of political influence and propaganda	Study of strategic communication, framing, and media control
Digital-Technological	Focuses on algorithmic processes and the role of digital ecosystems in spreading or countering disinformation	Development of AI-based detection systems, monitoring of bot networks, analysis of digital platforms
Normative-Legal	Investigates legal and institutional frameworks for countering disinformation during crises and wartime	Creation of legislation, regulation of media, and strengthening of cybersecurity mechanisms
Multidisciplinary / Integrative	Combines psychological, technological, communicative, and legal aspects into a unified system	Formation of comprehensive strategies for information security and resilience

A special role in this context is played by intelligent technologies – AI systems used for monitoring, identification, and forecasting of information threats. Therefore, a theoretical understanding

of disinformation under wartime conditions requires an interdisciplinary approach that unites philosophical, psychological, communicative, technological, and legal dimensions. This vision makes it possible to move from passive responses to information attacks toward active strategies of information security and trust management in society.

Fake news are deliberately fabricated messages presented as credible news. They are disseminated through mass media, social networks, or messengers to manipulate public opinion, discredit political opponents, or gain financial profit.

1. Manipulative content. This type of disinformation includes changes to the context or headlines of real news and the use of emotionally charged images and quotations that distort the actual situation. The goal is to influence people's emotions and push them to draw certain conclusions without fact-checking.

2. Conspiracy theories. These spread unrealistic scenarios of events attributed to secret groups or governments. They cultivate a sense of threat and distrust toward official sources and contribute to political or social destabilization.

3. Viral rumors. Viral rumors spread very quickly, especially on social networks, and often take the form of tips, predictions, or stories about the private lives of public figures or social events. Their danger lies in their mass influence on people's behavior and opinions.

4. Propaganda and information wars. This type of disinformation is an organized form of influence by states or groups on public opinion to achieve political or economic goals. It uses all mass-communication channels to construct a desired narrative (see Table 1.10, p. 43).

Disinformation is one of the most dangerous threats in today's information environment. It is characterized by the deliberate dissemination of false or distorted information to influence public opinion, political processes, the economy, or state security. A key feature of disinformation is its systemic and mass nature, which makes it an effective tool of manipulation in social, political, and economic spheres [105–110].

Table 1.10 – Analysis of Types of Disinformation [103–105]

Type of Disinformation	Sources	Objective	Methods of Dissemination	Consequences
Fake news	Social networks, websites	Manipulation, financial gain	Fabricated stories, clickbait	Disorientation, decreased trust in the media
Manipulative content	News portals, social networks	Eliciting an emotional reaction	Distortion of headlines and quotations	Manipulation of behavior and decision-making
Conspiracy theories	Blogs, forums, video channels	Destabilization, fostering distrust	Conspiracy narratives, pseudo-scientific explanations	Political and social disorientation
Viral rumors	Social networks, messengers	Rapid spread of information	Reposts, memes, short videos	Panic, misguided actions, spread of fear
Propaganda and information wars	Mass media, state channels	Political control, influence	Mass advertising, media campaigns	Formation of a desired narrative, manipulation of public opinion

Disinformation can be classified by various criteria: channels of dissemination, motives, form of presentation, and level of impact on the audience. For example, in social networks, digital disinformation predominates and spreads rapidly through recommendation algorithms and bot accounts. Traditional media may at times become sources of deliberate distortion of facts, while political actors can employ disinformation to influence voters and shape public opinion.

By form, disinformation may take the shape of completely fabricated information, distorted or de-contextualized truths, satellite or fake news, as well as manipulative graphics, video, or audio. Each type uses its own tactics and dissemination mechanisms. For instance, distorted information is often used to amplify specific emotions

in the audience, while entirely fake content serves to generate panic or chaos [111–123].

By motive, disinformation may be political, economic, social, or military. Political disinformation targets the discrediting of opponents or influencing election outcomes; economic disinformation aims to manipulate market processes or investment flows; social disinformation seeks to inflame conflicts within society; and military disinformation is used to disorient the adversary and demoralize the population. Each category uses specific communication tools and influence tactics, making the fight against disinformation complex and multi-level.

It is also important to analyze effectiveness, which depends on the audience's level of trust in the source, the speed of dissemination, and the adaptation of messages to specific target groups. Modern technologies – such as artificial intelligence and social-media algorithms – significantly enhance the effectiveness of disinformation, making it more persuasive and harder to detect.

It is also important to analyze the effectiveness of disinformation, as it directly depends on the level of trust the audience has in the information source. The higher the trust, the faster and deeper the message influences people's perceptions and behavior.

The speed of disinformation dissemination is a key factor in its effectiveness. Information that spreads quickly through social media or mass media can reach a wide audience before fact-checkers or governmental authorities have a chance to respond.

The adaptation of messages to specific target groups further enhances the effectiveness of disinformation. Messages tailored to the cultural, social, and psychological characteristics of an audience become more persuasive and elicit stronger emotional responses.

Modern technologies significantly amplify these effects. Artificial intelligence, in particular, allows the automated creation of personalized messages, selecting the tone, format, and content according to users' behavioral and psychological traits.

Social media algorithms further facilitate the dissemination of disinformation, as they are optimized for maximum user engagement. AI enhances the "echo effect," where content rapidly spreads among interested groups.

The combination of these technologies makes disinformation more convincing. Users often do not recognize manipulative elements and perceive the message as truthful, complicating the detection and correction processes.

Disinformation becomes even harder to detect due to multiple communication channels. Messages can simultaneously circulate through social networks, messengers, news sites, and other media, making monitoring and fact-checking more difficult.

Moreover, modern technologies enable the creation of synthetic content – fake videos, audio, and images that appear authentic. This adds another layer of complexity to disinformation detection and reduces the effectiveness of traditional verification methods.

Therefore, a systematic analysis of disinformation effectiveness is critically important for developing countermeasures. It helps identify vulnerabilities in communication channels and create strategies to minimize harm to society, businesses, and the state.

Understanding how modern technologies enhance the effectiveness of disinformation allows for the implementation of comprehensive countermeasures, including educational programs, technological solutions, and legal mechanisms. This is essential for ensuring state security and protecting citizens in the digital age.

In sum, the analysis of disinformation types shows that it is a multi-scale, multi-factor threat encompassing various channels, motives, and forms of presentation. Understanding its classification, methods, and goals enables the development of systemic countermeasures, including technological, educational, and legal tools-critically important for the security of the state, business, and society at large.

1.3. THE ROLE OF INTELLIGENT TECHNOLOGIES IN ENSURING NATIONAL INFORMATION SECURITY AND ECONOMIC RECOVERY

The modern economy and society operate under conditions of advanced digitalization and global information interconnectivity, which create both new opportunities and significant threats to national security. Information resources and data have become strategic assets of the state, while cyber threats, disinformation, and digital attacks can cause substantial economic and social damage. In this context, intelligent technologies emerge as a key instrument for ensuring national information security, as they make it possible to detect threats in real time, analyze large datasets, and make rapid and effective decisions to neutralize them.

Intelligent technologies are particularly relevant in times of war and post-war economic recovery, when the protection of information systems is critical to state stability. AI and machine learning ensure continuous monitoring of cyber threats, forecasting of potential attacks, and identification of disinformation campaigns. This enables not only the protection of state and corporate infrastructures but also helps to maintain public trust in the information environment.

Beyond information protection, intelligent technologies play a vital role in economic reconstruction. They provide market analytics, optimize production and logistics processes, automate management decisions, and support strategic planning. In countries recovering from crises or military conflicts, the use of intelligent systems accelerates enterprise restoration, infrastructure modernization, and efficient resource utilization.

Intelligent technologies also enhance the stability of financial systems through automated transaction monitoring, fraud detection, and risk management tools. At the same time, they contribute to the development of the digital economy, e-governance, and innovation-driven business platforms, all of which are essential for restoring a state’s competitiveness in global markets.

The domains of national security and economic development are deeply interconnected, as secure, transparent, and efficient information systems form the foundation for sustainable economic growth. The implementation of intelligent technologies not only prevents threats but also transforms business processes, increases productivity, and stimulates innovation-based progress.

Thus, the relevance of intelligent technologies in ensuring national information security and supporting economic recovery stems from the state's need to protect strategic information resources, minimize cyber risks, and create conditions for rapid and effective economic revitalization. Their implementation represents not only an element of digital transformation but also a key factor in strengthening national resilience, economic stability, and Ukraine's global competitiveness.

Intelligent technologies enable continuous monitoring of critical information and infrastructure systems, timely detection of anomalies and threats – an essential capability in the post-crisis period. For example, in the energy, transport, and financial sectors, the use of AI and analytical platforms enhances protection against cyberattacks, optimizes operational processes, and enables risk prediction, which significantly increases the reliability and stability of the economy.

In the business environment, intelligent technologies facilitate rapid adaptation to market changes, efficient resource management, and cost reduction. Machine learning and big data analytics tools help identify weak points in business processes, forecast demand fluctuations, optimize supply chains, and support data-driven management decisions.

AI plays a particularly important role in countering disinformation and maintaining cyber hygiene among the population, directly contributing to socio-economic stability. Under contemporary information threats, AI systems can automatically detect fake content, analyze information flows, and generate alerts about potential risks, enabling government agencies and businesses to react quickly and prevent negative outcomes. Furthermore, intelligent technologies support the development of e-governance programs, digital business

platforms, and online public services, thereby enhancing transparency, efficiency, and accessibility of state processes. These factors contribute to revitalizing economic activity, attracting investments, and creating new jobs.

Importantly, the adoption of intelligent technologies has a systemic effect: simultaneous improvement in cybersecurity, analytical capacity, and automation of business processes creates an environment conducive to sustainable economic growth. Economic recovery after crises or wartime disruptions is impossible without the integration of intelligent solutions in strategic sectors such as finance, energy, industry, and public administration.

Therefore, the importance of intelligent technologies lies not only in ensuring national security and protecting information resources but also in shaping a resilient, adaptive, and innovative economy capable of withstanding modern challenges and maintaining global competitiveness. Their implementation becomes a cornerstone of digital transformation, strategic security, and economic renewal of Ukraine.

Intelligent technologies-particularly artificial intelligence – are increasingly applied to safeguard national information security and support economic growth. In modern conditions, where nations face disinformation, cyber threats, and economic challenges, the use of AI becomes a critical tool for effective management of the information space and forecasting of economic processes.

Below is a generalized table illustrating the main directions of intelligent technology applications in these fields (see Table 1.11, p. 49).

Monitoring of the information space. Artificial intelligence enables automatic analysis of large volumes of data, identifying fake news and propaganda. This reduces the risks of information attacks and strengthens social resilience.

Cybersecurity. Intelligent systems predict and prevent cyberattacks, protecting state systems and enterprises from data leaks and financial losses.

Table 1.11 – Main Directions of Intelligent Technology Application

Area of Application	Specific Technologies	Functions / Tasks	Impact on National Security	Impact on the Economy
Monitoring of the Information Space	AI, Machine Learning, NLP	Analysis of large data sets, detection of fake news and propaganda	Reduction of disinformation risks	Protection of business reputation, market stability
Cybersecurity	AI-based threat analysis, automated defense systems	Detection of network anomalies, threat prediction	Prevention of strategic data leaks	Reduction of financial losses for enterprises
Economic Analytics and Forecasting	Machine Learning, Big Data	Forecasting crises, assessing economic risks	Support for state strategic planning	Optimization of investments, planning of economic recovery
Automation of Public Services	RPA, AI chatbots	Optimization of processes, enhancement of transparency	Reduction of corruption risks	Improved efficiency of public spending, business stimulation
Public Information Literacy	AI-based learning platforms	Training in recognizing fakes and digital threats	Strengthened critical thinking and social resilience	Growth of labor productivity, development of the digital economy

Economic analytics and forecasting. AI assists governments and businesses in forecasting crisis situations, assessing economic risks, and forming strategies for economic recovery.

Automation of public services. Process automation and AI chatbots shorten the processing time of citizen requests, enhance transparency, and improve management efficiency – thus building public trust and stimulating economic activity.

Public information literacy. AI-based educational platforms teach citizens to recognize disinformation, improving national information security and fostering the growth of the digital economy.

Hence, the integration of intelligent technologies into national security and economic systems enables not only effective counteraction to modern threats but also lays the foundation for rapid economic recovery, increased labor productivity, and strengthened information resilience of society.

Intelligent technologies are widely applied in both the public and private sectors. For instance, in information-space monitoring, AI can automatically track news streams, social networks, and other online resources, promptly identifying potentially harmful content. This allows government agencies to respond to disinformation campaigns at early stages, preventing their large-scale impact on public opinion and the economy.

In the field of cybersecurity, AI systems can not only detect attacks but also predict their likelihood, thus improving the protection of strategic infrastructure. Automated network-traffic analysis systems identify anomalies and respond to threats before they cause damage to state or corporate assets.

Another key direction is economic forecasting. The use of AI and Big Data enables risk assessment at various levels-from global trends to the condition of individual industries. This supports more effective state-management strategies and well-grounded business decisions during crises.

The automation of public services also demonstrates high potential. AI chatbots and RPA systems reduce administrative burdens, shorten response times to citizen requests, and increase process transparency. As a result, trust in government institutions is strengthened, and entrepreneurship is stimulated.

Finally, AI-based educational platforms enhance citizens' information literacy, build critical thinking, and promote safe use of digital technologies. This is especially significant for the economy,

as an informed workforce adapts faster to digital processes, increases productivity, and accelerates post-crisis recovery.

Thus, the integration of intelligent technologies into national security and economic systems achieves several key outcomes:

– increased national resilience to information and cyber threats;
– timely detection and neutralization of disinformation campaigns;
– effective planning of economic recovery and reduction of financial risks;
– enhanced transparency and efficiency of management processes;
– development of digital competencies among citizens, fostering sustainable economic growth.

Consequently, artificial intelligence and related intelligent technologies serve not only as instruments of technical protection but as strategic mechanisms for ensuring national information security and driving economic recovery and development in times of modern challenges.

he rapid digitalization of society has fundamentally transformed the way national security and economic systems operate. Intelligent technologies – including artificial intelligence (AI), machine learning (ML), natural language processing (NLP), robotic process automation, and Big Data analytics – are increasingly being integrated into government, business, and social infrastructure. Their application enables not only the automation of complex analytical processes but also the proactive identification of risks and strategic decision-making under uncertainty.

One of the most critical areas of implementation is the monitoring of the information space. Artificial intelligence and machine learning technologies allow for the real-time analysis of massive volumes of online data, identifying fake news, propaganda, and manipulative content. Through natural language processing tools, systems can detect emotional tone, classify sources, and recognize coordinated disinformation campaigns. This capability significantly reduces the risks of information attacks and strengthens the overall resilience of society to external influence.

From the perspective of national security, the automated monitoring of information flows enables governments to respond promptly to disinformation, cyber threats, and hybrid operations targeting public opinion. By detecting early signs of manipulation, AI-based systems help neutralize psychological and informational aggression before it escalates into large-scale social destabilization. Thus, the application of intelligent technologies in this domain ensures the protection of information sovereignty and strengthens the strategic stability of the state. At the same time, the monitoring of information space has a direct economic effect. For businesses, the ability to identify false narratives and negative information attacks helps preserve corporate reputation, protect consumer trust, and ensure market stability. The use of AI-driven brand monitoring tools enables companies to react quickly to reputational crises, minimize financial damage, and maintain competitive advantage in a highly digitalized economy.

The second crucial direction is cybersecurity, where intelligent technologies act as both shield and sentinel. AI systems for cyberattack analysis and automated protection can identify anomalies in network traffic, detect intrusion patterns, and predict potential vulnerabilities. Unlike traditional defense systems, AI-based cybersecurity tools are adaptive and self-learning, allowing them to anticipate threats and respond in real time.

The influence of these systems on national security is profound. By preventing data leaks and securing critical infrastructure – such as government networks, energy systems, and transportation – AI-driven cybersecurity strengthens the resilience of the state to digital aggression. In wartime or crisis conditions, such systems are essential for maintaining operational continuity, protecting classified information, and safeguarding public confidence in national institutions.

Economically, intelligent cybersecurity reduces financial losses caused by fraud, cyberattacks, and system failures. For enterprises, automated threat detection minimizes downtime and ensures the uninterrupted functioning of digital platforms, which is particularly

crucial for financial institutions, logistics, and manufacturing sectors. Thus, cybersecurity becomes a key component of economic sustainability and digital trust.

Another strategic field of application is economic analytics and forecasting. Machine learning algorithms and Big Data technologies enable the collection and interpretation of vast economic indicators, helping predict crises, assess risks, and identify opportunities for growth. Governments can utilize these tools to enhance strategic planning and evidence-based policymaking.

The integration of AI into economic forecasting directly supports national economic security by enabling early detection of destabilizing trends such as inflation, unemployment, or supply chain disruptions. Predictive analytics can inform strategic responses, stabilize financial systems, and guide resource allocation. This analytical capability provides a competitive advantage in developing recovery strategies during post-crisis or post-war periods.

In terms of economic development, intelligent analytics contributes to investment optimization, market stability, and sustainable growth. Businesses leverage predictive tools to identify emerging market opportunities, optimize production, and improve risk management. Consequently, AI-driven forecasting systems enhance overall economic efficiency and resilience in an unpredictable global environment.

The next important direction is the automation of government services. Robotic process automation and AI chatbots are transforming administrative operations by streamlining workflows, reducing bureaucracy, and improving the accessibility of public services. Automation minimizes human errors, accelerates data processing, and allows public institutions to focus on strategic tasks rather than routine procedures.

For national security, automated systems reduce corruption risks and increase the transparency of decision-making. Digital public administration tools improve governance accountability and strengthen citizens' trust in state institutions. The reduction of bureaucratic

inefficiency ensures faster response during emergencies, including crises related to disinformation, cybersecurity, or public safety.

Economically, digital automation enhances the efficiency of public spending and stimulates entrepreneurship. Transparent and fast administrative procedures attract investment, simplify regulatory compliance, and encourage innovation. The establishment of "smart government" ecosystems thus becomes a driver of sustainable economic growth and digital transformation.

An equally important sphere is the promotion of information and digital literacy among the population. AI-based educational platforms are being developed to train citizens to recognize fake news, understand digital threats, and evaluate information critically. By increasing awareness and critical thinking, societies can strengthen their cognitive immunity against manipulative narratives and disinformation.

From a holistic standpoint, the integration of intelligent technologies into systems of national security and the economy creates a synergistic effect: enhanced information resilience, strengthened cybersecurity, data-driven decision-making, and inclusive digital education. These factors jointly foster a secure and adaptive environment that supports economic recovery, productivity growth, and innovation. Consequently, artificial intelligence and related technologies are not merely tools of technological progress – they form the foundation of a resilient digital state capable of withstanding hybrid threats and ensuring sustainable economic development in the 21st century. Intelligent technologies represent a set of methods, algorithms, and systems capable of performing tasks traditionally requiring human intelligence. These include artificial intelligence (AI), machine learning, neural networks, natural language processing (NLP), robotic process automation (RPA), and big data analytics. Their classification is based on functional purpose (analytical, cognitive, managerial), degree of autonomy (autonomous, semi-autonomous, assistive), and field of application (public administration, business, education, cybersecurity).

In wartime conditions, disinformation is viewed as deliberate information manipulation aimed at influencing public opinion, state policy, and the economy. Theoretical approaches to its study include cognitive, systemic, communicative, and information-analytical perspectives. The cognitive approach focuses on the psycho-emotional impact of fakes on human perception; the systemic approach explores the interrelations among sources, dissemination channels, and social reactions; the information-analytical approach examines technological tools for identifying and neutralizing disinformation flows.

Intelligent technologies play a key role in ensuring national information security. They enable automated monitoring of the information space, detection of fake news, propaganda, and potential information attacks. AI systems can predict the evolution of threats, shorten response time to cyber incidents, and protect critical infrastructure.

In the economic domain, intelligent technologies facilitate crisis forecasting, risk assessment, investment optimization, and management automation. This helps both businesses and the state make informed decisions, reduce financial losses, and stimulate economic recovery.

Raising digital literacy through AI-based platforms is also an integral part of national strategy. An educated society capable of critical evaluation of information flows enhances state resilience and ensures productive integration into the digital economy.

The integrated approach presupposes the simultaneous use of intelligent technologies in government, business, and society – providing comprehensive protection of the information space and contributing to stable economic growth.

Therefore, the theoretical foundations of intelligent technologies confirm their crucial role in countering disinformation and ensuring national security. AI and related technologies make it possible not only to detect and neutralize information threats but also to predict economic risks, optimize management processes, and foster a digitally literate society. The integration of these technologies into

state and business systems creates a comprehensive framework for protection and economic recovery, which is particularly relevant amid military conflicts and global information instability.

The conducted research has demonstrated that the phenomenon of disinformation and the implementation of intelligent technologies are among the defining challenges and opportunities of the twenty-first century. In an era of global digitalization, information has become not merely a communication medium but a strategic resource that influences national security, political stability, and economic resilience. The study confirmed that the effectiveness of state and corporate governance directly depends on the capacity to manage information flows intelligently and to protect them from manipulation and distortion.

Disinformation has evolved from a political instrument into a comprehensive social and technological threat that affects all levels of public life. Its dissemination through digital platforms, automated networks, and social media creates an environment of uncertainty, distrust, and polarization. Theoretical analysis of the phenomenon revealed that no single approach can fully explain its multidimensional nature. Instead, a combination of communicative, psychological, social-constructivist, political, and technological frameworks provides a deeper and more holistic understanding of disinformation processes in wartime and peacetime contexts alike.

The information-psychological and social-constructivist approaches highlighted that disinformation primarily targets human consciousness, emotions, and cognitive biases. It operates through fear, anger, and social imitation – mechanisms that can destabilize entire societies. The political-communicative and normative-legal approaches, in turn, emphasize that disinformation functions as a tool of power and influence, employed both by states and non-state actors to achieve strategic objectives. Meanwhile, the digital-technological perspective has become indispensable in recent years, focusing on the algorithmic mechanisms, artificial intelligence, and network infrastructures that sustain disinformation ecosystems.

The comparative analysis of scholarly sources confirmed that the modern scientific discourse is shifting from a descriptive to an applied paradigm. Researchers increasingly focus on developing practical tools for countering disinformation through intelligent systems, machine learning algorithms, and automated content verification. This technological turn signifies the emergence of a new interdisciplinary field – cognitive-informational security, which integrates knowledge from computer science, psychology, and strategic communication.

Intelligent technologies, particularly artificial intelligence (AI), machine learning (ML), and natural language processing (NLP), have proven to be crucial in addressing both the threats and the opportunities of the digital age. Their capacity to process vast amounts of unstructured data, detect hidden patterns, and predict future developments positions them as essential instruments for ensuring national information security. Intelligent systems can monitor the information environment in real time, identify disinformation narratives, and trace their sources of origin and dissemination dynamics.

During wartime, such capabilities are not only desirable but indispensable. The study demonstrated that AI-assisted systems can protect critical infrastructure, detect cyberattacks, and support decision-making under conditions of uncertainty. In the Ukrainian context, the implementation of AI in monitoring and defense operations has become a cornerstone of national resilience, allowing both governmental and private institutions to respond proactively to hybrid threats.

The economic dimension of intelligent technologies also deserves special attention. Beyond their security functions, AI-driven solutions play a transformative role in rebuilding and modernizing national economies after crises or wars. Intelligent analytics enables governments and businesses to forecast risks, optimize resource allocation, and design effective recovery strategies. Automation, robotics, and big data analytics reduce operational inefficiencies, support transparency, and strengthen public trust in institutions.

The analysis further showed that intelligent technologies serve as a bridge between national security and sustainable development. They not only protect digital infrastructures but also promote the emergence of a knowledge-based economy. The automation of public services through AI chatbots and robotic process automation (RPA) enhances administrative efficiency, reduces corruption risks, and ensures transparency in governance. These changes contribute to restoring public confidence and stimulating economic activity, which is vital for post-war reconstruction and investment attraction.

Another key finding concerns the role of intelligent technologies in promoting information literacy and societal resilience. AI-based educational platforms can train citizens to recognize manipulative content, resist emotional triggers, and critically assess information sources. This cognitive empowerment of the population reduces the vulnerability of society to disinformation attacks, enhances digital hygiene, and contributes to the formation of a more adaptive and informed civic culture.

Nevertheless, the integration of intelligent technologies into national systems is not without challenges. The research revealed several constraints, including insufficient technical infrastructure, the shortage of qualified specialists, ethical dilemmas related to data privacy, and the risk of algorithmic bias. These issues highlight the need for a comprehensive national AI policy that aligns technological innovation with democratic principles, human rights, and cybersecurity standards.

From a theoretical perspective, the research substantiated that the synergy between artificial intelligence and disinformation counteraction represents a new paradigm of intelligent security governance. This paradigm goes beyond reactive defense measures, emphasizing proactive threat detection, strategic forecasting, and the development of self-learning systems capable of adapting to dynamic information environments. In this sense, AI acts as both a shield and a catalyst for national transformation.

On the economic level, intelligent technologies generate long-term value by fostering innovation and competitiveness. They enhance productivity, stimulate entrepreneurship, and attract foreign investment through the creation of reliable and transparent digital ecosystems. In post-conflict recovery scenarios, these technologies accelerate the rebuilding of infrastructure, facilitate logistics optimization, and improve coordination between the public and private sectors. Thus, they become a foundation for inclusive growth and sustainable development.

The interdisciplinary synthesis achieved in this research confirms that the effective use of intelligent technologies requires coordinated efforts among policymakers, academia, industry, and civil society. Such cooperation ensures the ethical and secure deployment of AI, supports the creation of legal frameworks, and fosters digital education and awareness. It also promotes the establishment of strategic communication systems capable of balancing freedom of speech with national security imperatives.

The study's findings underscore that intelligent technologies should not be perceived merely as technical tools but as strategic enablers of national resilience. Their integration into all spheres-security, economy, governance, and education-creates a holistic defense mechanism against hybrid threats while fostering social cohesion and innovation. The convergence of AI with big data analytics, cybersecurity, and e-governance forms the backbone of a new national development model grounded in digital sovereignty and human-centered innovation.

In conclusion, the role of intelligent technologies in ensuring national information security and driving economic recovery is both foundational and transformative. Their capacity to counter disinformation, protect digital infrastructures, and enhance decision-making processes positions them as essential pillars of modern statecraft. For Ukraine and other nations navigating complex geopolitical and information challenges, the strategic adoption

of AI represents not only a technological advancement but also a civilizational imperative. By integrating intelligent technologies into its governance and economic systems, the state strengthens its resilience, accelerates reconstruction, and secures its place within the emerging global digital order. Ultimately, intelligent technologies embody the fusion of security, innovation, and human progress – a synthesis upon which the sustainable future of the information society must be built.

CHAPTER 2.
STATE AND TRENDS IN THE DEVELOPMENT OF INTELLIGENT TECHNOLOGIES IN COMBATING DISINFORMATION

2.1. CURRENT STATE OF DEVELOPMENT OF INTELLIGENT TECHNOLOGIES IN THE WORLD AND IN UKRAINE

The development of intelligent technologies based on the use of AI, machine learning, neural networks, big data, and process automation has become one of the most powerful drivers of global transformation in the 21st century. Intelligent systems are being actively implemented in the economy, education, healthcare, defense, urban governance, and environmental monitoring. These technologies not only change the structure of the labor market and approaches to resource management; they also shape a new model of socio-economic development in which information and data become the principal form of capital. For example, the Stanford HAI report notes that monitoring scientific publications, investment, and technological progress in AI makes it possible to identify the high dynamic potential of this field [82].

Intelligent technologies have become the leading driving force of the Fourth Industrial Revolution, transforming the economy, education, governance, and social relations. They include AI systems, machine learning, robotics, big data analytics, the Internet of Things, and cognitive technologies. They enable the automation of routine processes, risk prediction, managerial decision support, and the creation of new data-driven products.

Today, the level of integration of intelligent technologies determines the competitiveness of states and companies in the global market.

Global AI development in the 2020s is characterized by explosive growth in investment and the widespread diffusion of generative artificial intelligence technologies. According to [89; 90], the global volume of financing for AI projects exceeded USD 190 billion, and the share of companies using such technologies in their operations rose to 72%. The leading centers of intelligent systems development-the United States, China, the European Union, Canada, Japan, and South Korea-are implementing government programs to support innovation, education, and digital infrastructure.

At the same time, the global race for technological leadership has intensified, turning artificial intelligence into a key geopolitical resource. States that successfully integrate intelligent technologies into production, defense, and information management acquire not only economic advantages but also strategic influence in shaping the rules of the future digital world order. This explains why the world's leading economies invest heavily in AI research ecosystems, data infrastructure, and the training of qualified specialists.

An important feature of modern AI development is the transition from experimental use to systemic implementation. Intelligent technologies are no longer confined to research laboratories-they are embedded in public administration, financial regulation, education, and healthcare systems. For example, in 2025 more than 80% of OECD countries reported using AI solutions in at least one area of public governance, primarily in e-government services, data analytics, and national security.

In the private sector, the use of AI has become a decisive factor in competitiveness. Global corporations such as Google, Microsoft, Amazon, and IBM are investing billions of dollars in cloud AI platforms, generative models, and autonomous systems. At the same time, small and medium-sized enterprises (SMEs) are increasingly adopting ready-made AI tools for marketing, logistics optimization,

and risk management. This democratization of intelligent technologies makes innovation accessible even to companies with limited resources.

The field of generative artificial intelligence has seen especially dynamic progress. Tools such as large language models, computer vision, and multimodal systems have transformed communication, education, design, and creative industries. According to recent forecasts, the contribution of generative AI to the global economy could exceed USD 4 trillion annually by 2030. However, such rapid development also raises concerns regarding ethics, copyright, and potential misuse of synthetic content.

Parallel to this, global research attention is shifting toward the concept of trustworthy and explainable AI. The need to ensure algorithmic transparency, data protection, and non-discrimination has led to the creation of international ethical frameworks, including the UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) and the OECD Principles on AI (2019). These documents serve as the basis for shaping responsible innovation strategies in both advanced and developing economies.

From the technological standpoint, the integration of intelligent systems relies on cloud computing, edge technologies, quantum computing, and high-speed communication networks such as 5G and the emerging 6G. The convergence of these technologies enables real-time data processing, predictive analytics, and the creation of cyber-physical systems capable of autonomous decision-making. This integration forms the backbone of smart industries, cities, and logistics systems worldwide.

In the defense sector, AI and autonomous systems are revolutionizing strategic planning, intelligence analysis, and battlefield logistics. The use of machine learning in geospatial analysis, drone control, and cyber defense has become indispensable for modern militaries. However, these applications also raise ethical dilemmas regarding the limits of automation in lethal decision-making and the need to maintain human oversight.

Environmental monitoring represents another crucial area of intelligent technology deployment. AI is increasingly applied to climate modeling, biodiversity assessment, and disaster prevention. Smart sensor networks and predictive algorithms help reduce energy consumption, optimize resource use, and mitigate the effects of environmental degradation-tasks that are becoming ever more urgent amid global climate change.

Education and science are also undergoing transformation. Intelligent systems facilitate personalized learning, automate administrative tasks, and enhance access to digital resources. Universities worldwide are establishing AI research centers and interdisciplinary programs to train specialists capable of integrating technological innovation with ethical and societal responsibility. This trend creates the intellectual foundation for sustainable digital progress.

The global labor market is adapting to this technological revolution. Routine and repetitive tasks are being automated, while demand is rising for highly skilled professionals in data science, cybersecurity, and digital management. The World Economic Forum predicts that AI will create more jobs than it eliminates, but it will also fundamentally change professional competencies, requiring lifelong learning and adaptability from workers.

The economic geography of intelligent technology development is also shifting. While the United States and China remain undisputed leaders, the European Union is focusing on human-centric AI and ethical governance, Japan and South Korea emphasize robotics and automation, and emerging economies such as India and Brazil are leveraging AI for digital inclusion and public services. This diversity of approaches contributes to a more balanced and pluralistic global innovation landscape.

In Ukraine, the development of intelligent technologies has accelerated significantly since 2020, driven by the need to ensure information security and economic resilience amid the challenges of war. Ukrainian researchers, IT companies, and startups have demonstrated high adaptability, creating analytical platforms for

detecting disinformation, managing humanitarian logistics, and supporting defense innovation. The war has become a catalyst for rapid digital transformation across the country.

The Digital Transformation Strategy of Ukraine 2030 defines artificial intelligence as one of the national priorities. Key areas include digital public services, smart infrastructure, and the formation of an open data ecosystem. The creation of the Ministry of Digital Transformation and the Diia platform laid the groundwork for integrating intelligent systems into public administration and expanding citizens' digital participation.

Despite limited resources, Ukraine's IT sector has become one of the fastest-growing in Europe, accounting for more than 5% of GDP and employing hundreds of thousands of specialists. Domestic companies actively cooperate with European and American partners in cybersecurity, natural language processing, and defense-related AI research. This collaboration strengthens Ukraine's technological sovereignty and integration into the global innovation network.

Nevertheless, challenges remain. Insufficient funding for scientific research, weak infrastructure for data storage, and the lack of unified standards for AI ethics hinder rapid progress. Addressing these gaps requires comprehensive policies that combine state support, private investment, and international cooperation. Ukraine's accession to the European digital single market will play a decisive role in this regard, enabling access to resources, expertise, and joint projects.

In conclusion, the current stage of intelligent technology development-both globally and in Ukraine-illustrates a profound paradigm shift toward data-driven governance, ethical innovation, and human-centered digitalization. For Ukraine, the effective integration of AI and related technologies represents not only a path to modernization but also a cornerstone of national resilience and post-war recovery. The coming decade will determine whether the country can transform these technologies into sustainable engines of economic growth, social cohesion, and democratic strength.

The European Union plays a significant role in shaping the global agenda, having adopted in 2024 the Artificial Intelligence Act-the world's first comprehensive law regulating AI risks and safety. In the United States, priority is given to the development of generative models and the protection of intellectual property, while China emphasizes industrial automation, unmanned technologies, and public administration. All these directions form a multi-vector system for the development of intelligent technologies that combines economic, ethical, and security dimensions.

Table 2.1 – Key Indicators of Artificial Intelligence Development Worldwide (2024)

No.	Country	Estimated AI Investment, USD billion	Share of Companies Implementing AI, %	Main Directions of State Strategy
1	USA	68	82	Generative AI, defense, biotechnology, AI ethics
2	China	45	76	Industrial automation, unmanned systems, data analytics
3	European Union	32	65	Ethical regulation (AI Act), education, healthcare
4	Japan	15	58	Robotics, cybersecurity, "smart cities"
5	South Korea	12	60	Manufacturing automation, e-government
6	Canada	9	55	Academic research, startup ecosystem
	Total	190+		

As can be seen from the table, in 2024 the total volume of financing for artificial intelligence projects exceeded USD 190 billion, indicating explosive investment growth in this field. The United States remains the leader, concentrating the largest volume of financial resources (about 36% of the global market) and shaping technological trends in generative AI, defense systems, and bioengineering.

China ranks second in terms of investment, paying particular attention to industrial automation, data analytics, and surveillance systems. The European Union has chosen the path of regulatory governance – the adoption of the AI Act set a precedent for the creation of a legal framework for the ethical and safe use of AI.

Japan and South Korea are betting on robotics, "smart" cities, and the development of cyber defense, while Canada remains one of the leading centers for academic research and AI startups.

Overall, the share of companies already applying AI technologies in leading countries ranges from 55% to 82%, indicating a transition from the experimental to the systemic stage of integrating intelligent technologies into business processes. Thus, the presented data confirm the thesis of the globalization of intelligent technologies, where AI becomes a key factor of economic growth, innovation policy, and geopolitical competitiveness.

Table 2.2 – State of Development of Intelligent Technologies in Ukraine (2023–2025)

No.	Indicator	2023	2024	2025*	Comment
1	2	3	4	5	6
1	Estimated investment in AI, USD million	42	68	95	Growth due to defense and IT projects, foreign grants, and startups
2	Number of active companies using or developing AI	120	165	210	Largest shares in defense, fintech, education, healthcare
3	Share of enterprises implementing AI elements in business processes, %	9	14	19	Main areas: marketing, logistics, data analytics
4	Number of research groups and university AI labs	18	22	27	Active centers: KNU, KPI, LNU, NTU "KhPI", SumDU
5	Number of Ukrainian startups in intelligent technologies	80	105	130	Growth notably in defense AI and image analytics

End of Table 2.2

1	2	3	4	5	6
6	Volume of IT services exports, USD billion	7.4	8.2	9.1	Over 45% of exports accounted for by intelligent and analytical products
7	Main state support programs	"Diia"	–	–	Development of human capital, ethics, infrastructure, and legal framework

**Forecast data based on analytics by MinDigital, ICDS, McKinsey Ukraine, DOU.ua (2025).*

The development of intelligent technologies in Ukraine in 2023–2025 shows stable positive dynamics despite the difficult conditions of wartime. Investment in the AI sector has more than doubled compared to 2022, mainly due to the participation of international donors, defense technology companies, and initiatives by USAID, the EIB, and Horizon Europe.

IT exports play a significant role, remaining one of the main sources of foreign currency inflows for the state. In 2024 they exceeded USD 8 billion, and nearly half of this volume was generated by companies working with artificial intelligence, machine learning, and automation technologies.

Particular attention should be paid to the defense technology sector, where intelligent systems are used for object recognition, threat forecasting, logistics optimization, and information security. According to ICDS (2024), Ukraine is one of the few countries actively using AI in real combat environments. In addition, education and digital literacy are actively developing: thousands of users undergo training each year via the "Diia.Digital Education" platform, which helps build digital competencies for using AI tools in everyday activities.

At the same time, problems remain: insufficient public funding for scientific research, a lack of ethical standards and legislation, and the outflow of IT specialists abroad. For this reason, experts [88] emphasize the need to harmonize Ukraine's legal framework with

the European AI Act and to create a dedicated agency for AI ethics and safety. Overall, the table indicates that intelligent technologies are becoming one of the priority areas for Ukraine's post-war recovery. Their development is based on high levels of human capital, a dynamic IT sector, and international cooperation.

Table 2.3 – Comparison of Intelligent Technology Development in the World and in Ukraine (2024)

Indicator	Leading Countries (USA, China, EU)	Ukraine	Comment
AI investment volume	Over USD 190 billion	About USD 95 million	In Ukraine, funding is predominantly grant-based and defense-technology oriented
Share of companies using AI	65–82%	19%	Ukraine is at the stage of active implementation
Main development areas	Generative AI, robotics, analytics, medicine	Defense, data analytics, education, healthcare	Areas partially overlap, but defense predominates in Ukraine
Presence of a national strategy	Yes (AI Act, AI 2030, AI Initiative)	Yes (National AI Strategy 2030)	Ukraine has an official strategic document
Number of AI startups	Over 10,000 (combined)	About 130	The domestic ecosystem is developing despite wartime conditions

Table 2.3 shows that Ukraine is only forming its own intelligent technologies market, while leading countries are already at the stage of mature AI integration into the economy. However, thanks to scientific potential, IT education, and the development of defense technologies, Ukraine is gradually narrowing the technological gap. State policy in the field of AI-aimed at supporting education, digital infrastructure, and startups-creates the foundation for a transition to the stage of sustainable development of intelligent systems after the war ends.

A comparison of the development of intelligent technologies in the world and in Ukraine indicates a substantial gap in investment scale, number of companies, and the degree of AI integration into the economy. In leading countries (the USA, China, the EU), intelligent technologies are a system-forming factor: they account for about 3–4% of GDP, and governments purposefully support innovation programs and education.

In Ukraine, the volume of AI investment so far is less than USD 0.1 billion; however, growth rates remain stable: over the past two years, funding has more than doubled, and the number of startups has increased by 60%. The main areas of development are defense technologies, data analytics, educational solutions, and medical systems, which correspond to the needs of wartime and post-war recovery.

The presence of the National AI Development Strategy through 2030 indicates that Ukraine belongs to the group of countries that already have a state policy of digitalization aligned with the principles of the EU AI Act.

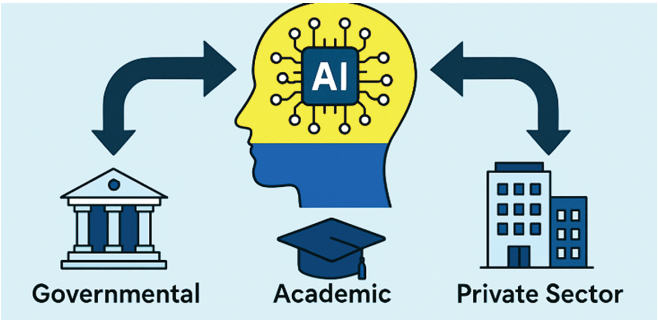

Figure 2.1 – Artificial Intelligence Ecosystem Integrating Governmental, Academic, and Private Efforts

A positive trend is the growing focus on workforce training and the development of digital competencies through the “Diia.Education” projects and university initiatives. Overall, it can be concluded that Ukraine is moving toward building its own artificial intelligence

ecosystem that integrates governmental, academic, and private efforts. Despite lower investment levels, Ukraine's AI sector has unique advantages-flexibility, military-driven innovation, and strong human capital-which may enable accelerated growth in 2025–2030.

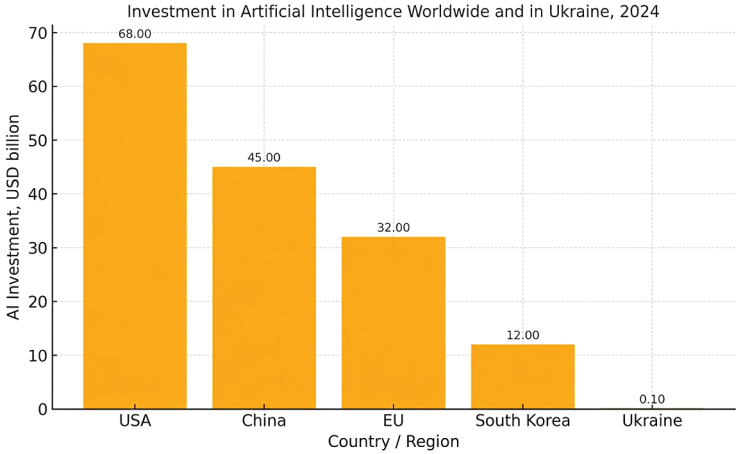

Figure 2.2 – AI Investment Volumes in the World and in Ukraine, 2024

Figure 2.2 clearly illustrates the vast gap between Ukraine and leading countries in AI financing. At the same time, the chart shows that even with minimal investment volumes, Ukraine demonstrates one of the fastest growth rates-between 2023 and 2024, the indicator increased by more than one and a half times. This dynamic indicates the high potential of the Ukrainian IT market and the effectiveness of international grant programs that stimulate the development of both defense and civilian AI. By 2030, according to forecasts [100], investments may exceed USD 0.5 billion, allowing Ukraine to transition to a stage of mature technological development.

The key technological trends of the current stage include generative AI, cognitive data analytics, autonomous systems, AI in medicine and education, and cybersecurity solutions. Transformer-based generative platforms (GPT, Gemini, Claude,

Mistral) have opened up opportunities for automated content creation, visualizations, analytical models, and even scientific texts. At the same time, the risks of disinformation are increasing, which elevates the importance of ethical standards, algorithmic transparency, and responsible data use.

The economic effect of AI implementation is multidimensional. According to estimates [100], artificial intelligence technologies could potentially add more than USD 4 trillion to global GDP over the next decade. In industry, finance, logistics, and marketing, AI reduces costs, increases efficiency, and fosters the formation of new data-driven business models. At the same time, the demand is growing for workforce training in digital and analytical competencies, as labor market transformation requires new knowledge and professions.

Despite the war and difficult socio-economic conditions, Ukraine is gradually integrating into the global digitalization process. The development of the IT sector, startups, e-government systems, and educational technologies creates a favorable foundation for implementing intelligent solutions. An important step was the adoption of the National AI Development Strategy for 2021–2030, initiated by the Ministry of Digital Transformation, which defines AI development areas in public administration, education, security, science, and the economy.

Ukrainian researchers and engineers are actively participating in international projects. For example, in 2024 the team of Kiulian et al. presented the first adaptation of the Gemma and Mistral language models for the Ukrainian language, contributing to the development of localized AI. Ukrainian startups in analytics, drones, robotics, and medical technologies demonstrate a high level of innovation. Meanwhile, in education, intelligent systems for testing, knowledge assessment, and personalized learning are being actively implemented.

Intelligent technologies have acquired particular significance in national security and defense. According to the ICDS (2024) report, AI algorithms are used for target recognition, satellite image

analysis, logistics optimization, and fake information detection. Wartime conditions have stimulated the growth of Ukrainian technology companies specializing in unmanned systems and military analytics. This experience is already viewed as a unique example of AI adaptation to crisis conditions and may serve as a foundation for post-war technological recovery.

Among the main challenges for the development of intelligent technologies in Ukraine are insufficient investment, the outflow of specialists abroad, and the absence of a unified regulatory and ethical framework for AI use. As Oliinyk (2025) notes, harmonizing Ukrainian legislation with European digital technology standards is a necessary condition for integration into the EU Digital Single Market. It is important to balance innovation, security, and citizens' rights so that intelligent technologies contribute to sustainable development rather than social polarization.

In summary, intelligent technologies are a strategic resource of the 21st century. The world is moving toward integrated systems capable not only of automating processes but also of forming data-driven analytical and managerial decisions. For Ukraine, AI development is not only a technological issue but also a driver of recovery, modernization, and integration into the global digital space. Coordinated policies among the state, science, education, and business can transform intelligent technologies into the foundation of a new model of economic growth and international competitiveness (see Table 2.4, p. 76).

The dynamics (Table 2.4) show sustained growth of global interest in intelligent technologies-the global volume of AI investment more than doubled between 2021 and 2024. Leading countries are actively financing scientific research, educational programs, and commercial solutions in artificial intelligence.

In Ukraine, AI development proceeded in two stages:

– 2021–2022: a period of building scientific and technical potential and launching pilot projects;

– 2023–2024: a stage of accelerated development associated with the war, the digitalization of defense, international technical assistance, and startup activity.

Table 2.4 – Dynamics of the Development of Intelligent Technologies in the World and in Ukraine (2021–2024)

Year	Global AI Investment, USD billion	Ukraine: Investment, USD million	Number of Companies Using AI in Ukraine	Share of Enterprises with AI Elements, %	Key Trends
2021	85	25	≈60	5	Initial stage of active AI implementation globally; in Ukraine-isolated projects in fintech and education
2022	120	38	≈90	7	Growth in global investment; emergence of generative models (GPT-3.5); in Ukraine-emergence of defense solutions and data analytics
2023	160	68	≈120	9	Activation of government programs and startup market; globally-mass generative transformation of business
2024	190	95	≈210	19	Industry consolidation, formation of legal frameworks (EU AI Act); in Ukraine-development of defense AI, education, and healthcare

The increase in the number of companies implementing AI – from 60 in 2021 to over 200 in 2024 – indicates a shift from the experimental to the applied phase of technology development. The most dynamic sectors are defense, finance, education, and

healthcare. Universities are also showing growing interest in research on machine learning, neural networks, and data analysis.

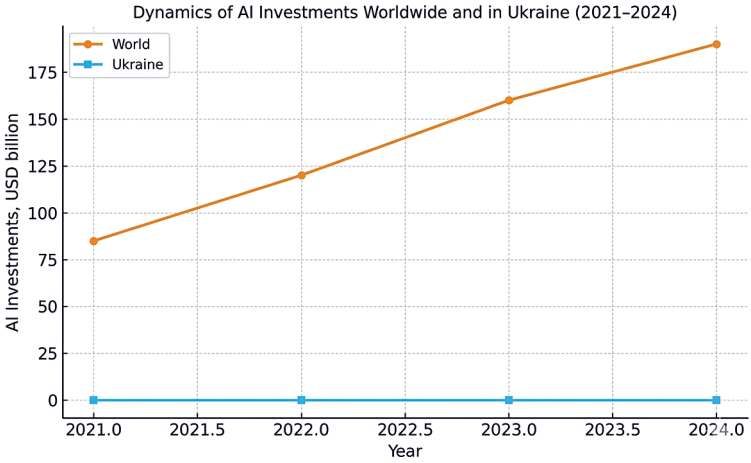

Figure 2.3 – Investments in Artificial Intelligence in the World and in Ukraine (2021–2024)

Figure 2.3 shows the difference in funding scales, but it also demonstrates a positive growth trend in Ukraine-investments nearly quadrupled over this period. The global trajectory (line "World") shows steady growth in AI investments: from USD 85 billion in 2021 to USD 190 billion in 2024. This is driven by the development of generative AI, industrial automation, and digital services. The Ukrainian trajectory (line "Ukraine") demonstrates a sharp rise from USD 25 million in 2021 to USD 95 million in 2024, despite wartime challenges. The main sources are international assistance, defense startups, IT companies, and educational projects.

In the leading countries-the USA, Japan, China, Germany, and South Korea-national AI development strategies are being implemented that envisage large-scale investments in science, education, digital infrastructure, and AI ethics. These states create favorable conditions

for partnerships among business, academia, and government to enhance global competitiveness. At the same time, the integration of intelligent technologies into the global economy is accompanied by challenges-particularly cybersecurity threats, personal data protection issues, ethical dilemmas regarding autonomous systems, and the risks of digital inequality. These issues are highlighted in a McKinsey & Company report, which notes that while AI adoption is growing, scaling its value requires attention to governance and organizational readiness. An international UN report also underscores the importance of a global regulatory framework for AI [90].

Despite wartime challenges and economic constraints, Ukraine demonstrates positive dynamics in digitalization and the implementation of intelligent technologies. The IT, fintech, e-government, data analytics, and edtech sectors are developing actively. The state is introducing initiatives to shape a legal framework for AI use, develop the population's digital competencies, and stimulate innovation. For example, Ukraine's AI development strategy covers the creation of infrastructure, data access, and research support. At the same time, the report for Ukraine indicates that intelligent solutions have already become part of the defense sphere, cybersecurity, and risk management.

Formation of intelligent technologies in Ukraine is taking place in the context of integration into the European scientific and technological area and the gradual recovery of the economy after the large-scale destruction caused by the war. Under these conditions, AI and other intelligent solutions become not only tools for increasing managerial efficiency but also instruments for ensuring national security, transparency of the public sector, and business resilience. Analytical evidence shows that Ukraine's digital public administration and innovation strategies are geared toward building a knowledge- and technology-oriented economy. The relevance of studying the current state of intelligent technology development lies in the need for an in-depth analysis of trends, barriers, and prospects

for their application in Ukraine within the global context. This will make it possible to identify strategic directions of state innovation policy, increase the efficiency of the national economy, and ensure the country's sustainable recovery based on knowledge, technologies, and human capital. For example, research on global AI trends points to significant potential but also to risks related to scaling and organizational readiness. A monographic study makes it possible to comprehensively assess the potential of intelligent technologies as a driving force for the modernization of society and the integration of Ukraine into the global digital space.

The current stage of intelligent technology development is characterized by a rapid expansion of their impact on all spheres of life-from industry and finance to education, healthcare, and public administration. Artificial intelligence, machine learning, big data analytics, robotics, and business process automation have become key factors of global digital transformation. The leading countries – the United States, China, EU member states, South Korea, and Japan – are actively investing in scientific research, the development of innovation clusters, and the creation of regulatory environments conducive to the ethical and safe use of intelligent technologies.

In Ukraine, intelligent technologies are also gaining increasing importance, particularly in defense, cybersecurity, education, finance, and public services. Despite the difficult economic conditions caused by the war, the state, research institutions, and the private sector are actively implementing AI-based solutions to improve management efficiency, counter disinformation, and modernize production. Ukrainian IT companies are successfully integrating into global digital innovation chains, and the government is developing AI strategies aimed at building a competitive digital economy.

Accordingly, the current state of intelligent technology development worldwide and in Ukraine indicates their key role in ensuring sustainable economic growth, strengthening national security, and improving social well-being. Further progress in this area depends

on the integration of scientific research, education, business, and public policy, as well as adherence to the principles of ethical, responsible, and safe use of AI. Ukraine has significant potential to develop its AI sector, which may become one of the drivers of its post-war recovery and integration into the global digital community.

2.2. ASSESSING THE EFFECTIVENESS OF INTELLIGENT TECHNOLOGIES IN COUNTERING DISINFORMATION DURING WAR

Under the conditions of armed aggression against Ukraine, the problem of information security has acquired exceptional importance. Modern war is waged not only on the battlefield but also in the digital environment-in the form of information attacks, manipulation, disinformation campaigns, and cyber operations. The large-scale spread of fake news, distortion of facts, and the use of bot networks pose a serious threat to national security, public stability, and the state's international reputation.

In this context, the application of intelligent technologies-particularly artificial intelligence (AI), machine learning, neural networks, and natural language processing (NLP) algorithms-opens new opportunities for detecting, analyzing, and neutralizing disinformation. AI-based systems can promptly identify false messages, trace the sources of their dissemination, analyze linguistic patterns of manipulation, and automatically generate warnings for users and the media. In wartime, traditional methods of monitoring the information space become ineffective due to the enormous volume of data, the speed of updates, and the targeted nature of propaganda. Intelligent technologies provide the necessary scalability and processing speed to respond to information threats in real time. The use of AI tools to counter disinformation is also a crucial factor of societal resilience, as it increases trust in official sources, strengthens critical

thinking, and fosters a culture of digital security. In addition, AI technologies enable the creation of analytical systems for government and military structures that support strategic decision-making based on objective data.

Research into the effectiveness of such technologies is not only applied but also strategic in nature. It makes it possible to determine the actual impact of intelligent systems on reducing disinformation, to identify the most effective methods, and to ensure the ethical and transparent deployment of these systems.

Moreover, the disinformation problem has a global dimension-Ukraine serves as a testbed where cutting-edge information strategies and technologies are being trialed. Therefore, assessing the effectiveness of intelligent solutions in this area is of great importance not only for Ukrainian society but also for the international community, which seeks to develop universal models of information security in conditions of hybrid wars and digital threats.

Table 2.5 – Main Areas of Applying Intelligent Technologies to Counter Disinformation During War

No.	Area of Use	Example of Intelligent Technology	Primary Purpose	Outcome
1	2	3	4	5
1	Monitoring the information space	AI systems for social media analysis (NLP models, content classification)	Automatic detection of fakes, bots, trolls	Reduced spread rate of disinformation, early warning
2	Fact-checking and content verification	AI platforms	Analysis of texts and images to detect false claims	Increased trust in verified sources, reduced information noise
3	Detection and blocking of fake accounts	ML models analyzing behavioral patterns	Identification of botnets and coordinated information attacks	Reduced artificial influence on public opinion

End of Table 2.5

1	2	3	4	5
4	Image and video processing	Computer vision algorithms	Detection of forged videos and photos	Preservation of the integrity of visual content
5	Information analytics for state bodies	Intelligent risk analysis and forecasting systems	Identifying disinformation sources and dissemination channels	Decision support in cyber and information security
6	Educational and communication platforms	Chatbots, adaptive learning systems	Improving media literacy; real-time explanations of fakes	Growth of critical thinking among citizens

Table 2.5 summarizes the key areas where intelligent technologies are used to combat disinformation under wartime conditions.

Monitoring the information space. Language models enable round-the-clock analysis of millions of posts across social networks, blogs, and news sites, facilitating rapid detection of fake messages, information attacks, or shifts in hostile media rhetoric.

Fact-checking. Machine learning algorithms can automatically compare claims against databases of trustworthy sources and flag potentially false content. For example, in 2024 the Ukrainian system LetsData AI integrated an AI module that recognizes disinformation patterns on Telegram channels. Detection of fake accounts. Behavioral analytics models identify activity anomalies-synchronous posting, repeated texts, mass “likes”-that indicate botnet operations, allowing the Security Service of Ukraine and cyber units to neutralize information attacks at early stages.

Computer vision and deepfake analysis. Deepfake detection algorithms identify doctored videos and forged images widely used by the adversary for manipulation, thereby safeguarding media integrity and public trust.

State information analytics. AI-powered OSINT and big-data platforms enable governmental bodies to forecast information threats,

identify disinformation sources, and plan strategic communications. Ukraine is already integrating such solutions within the *United24* and *Digital Security Hub* initiatives.

Educational tools and media literacy. Intelligent chatbots and educational systems (e.g., modules of Diia.Education) help the public recognize fakes, assess sources, and develop media literacy skills. Intelligent technologies thus become a key element of Ukraine's information defense strategy-reducing response time, improving fact-checking accuracy, ensuring transparent communications, and building a resilient information environment. Accordingly, the effective use of AI in countering disinformation is not only a technological achievement but also an instrument of national security and international credibility. Intelligent technologies play a decisive role in contemporary information warfare by enabling the rapid detection, analysis, and neutralization of disinformation. Globally, they are used for automatic monitoring of the digital space, recognition of false content, and prevention of its spread. The most prevalent technologies include machine learning systems, NLP algorithms, neural networks, computer vision, and cognitive data analytics.

One example is the AI4Media project under the EU's Horizon 2020 program, which supports independent media by providing AI tools to analyze information flows and detect fake messages. In the United States, ClaimBuster automatically identifies potentially false claims in publications, using machine learning methods for classification and subsequent verification by fact-checkers. Such solutions significantly shorten response time to disinformation campaigns and improve the accuracy of content verification.

Large corporations are also actively deploying intelligent systems against fakes. For instance, Google Fact Check Tools use NLP to compare news texts with verified databases, while the Twitter/X AI Moderation System employs neural networks to detect bots and propaganda accounts. These instruments filter harmful content and block disinformation sources at early stages.

In visual content verification, Truepic AI and a range of deepfake-detection algorithms are crucial. Such solutions leverage computer vision to identify altered or generated materials-especially relevant during war, when the adversary actively uses fabricated videos for manipulation.

In Ukraine, a domestic ecosystem of intelligent anti-disinformation technologies is taking shape. A strong example is the Molfar OSINT analytical platform, which uses AI to analyze social networks, forums, and media, identifying fake sources and coordinated information attacks. Another Ukrainian initiative, LetsData AI, specializes in monitoring Telegram channels and applies NLP models to detect toxic, manipulative, and propaganda narratives. The StopFake project-supported by the EU-implements AI elements for automatic message analysis and the creation of a database of verified facts, thereby increasing trust in official sources and fostering a culture of critical thinking.

An important direction for intelligent technologies is their use by state institutions, such as OSINT Hub Ukraine, which integrates AI tools for open-source data analytics. These systems help detect hostile botnets, assess information risks, and forecast potential attacks on the information space, thereby improving the effectiveness of strategic communications and ensuring national cybersecurity.

Beyond analytics, intelligent technologies are widely used in educational and public-awareness initiatives. For example, the Diia. Education platform integrates learning modules powered by adaptive algorithms that help citizens recognize fakes, analyze information sources, and develop media literacy skills. This builds society's information resilience and reduces the impact of disinformation campaigns on public consciousness.

The Ukrainian experience demonstrates that the integration of intelligent technologies into information defense systems can generate a synergistic effect, combining state-level cybersecurity mechanisms with civic digital initiatives. This hybrid approach

strengthens national resilience and ensures that the country can adapt dynamically to rapidly evolving disinformation tactics. Ukraine has effectively become a testing ground for innovative AI-driven counter-disinformation strategies that later inform global best practices.

At the strategic level, the Ministry of Digital Transformation of Ukraine and the Center for Strategic Communications and Information Security are working on the development of unified frameworks for data analysis and risk forecasting. By leveraging big data and machine learning, these institutions can identify emerging patterns of information manipulation and recommend proactive communication strategies to counter them. This marks a transition from reactive defense to anticipatory information management.

A crucial element of this ecosystem is data interoperability – the capacity of different institutions and systems to share, process, and analyze information using common standards. The development of secure digital infrastructure and cross-platform AI systems allows for faster response coordination between government agencies, media organizations, and independent fact-checkers. This interoperability is a decisive factor in shortening the "detection-to-response" cycle in the fight against disinformation.

Another promising vector involves multilingual NLP technologies. Since disinformation often transcends linguistic and cultural boundaries, Ukraine's linguistic diversity offers a unique advantage for developing multilingual AI models. These models are trained to detect manipulative narratives not only in Ukrainian and Russian but also in English, Polish, and other European languages, supporting international collaboration in combating cross-border propaganda.

Ethical AI governance remains at the core of Ukraine's digital security policy. Building public trust in intelligent technologies requires ensuring transparency, data protection, and algorithmic fairness. The introduction of AI ethics standards-aligned with the EU Artificial Intelligence Act-helps establish accountability for both developers and institutions deploying these technologies. This

alignment contributes to Ukraine's integration into the European digital and regulatory landscape.

The media sector plays a critical role in operationalizing intelligent technologies for real-time verification. Partnerships between media outlets and AI research centers have produced automated dashboards for tracking disinformation trends. These tools help journalists and editors make data-driven decisions when publishing sensitive information, minimizing the risk of amplifying hostile propaganda narratives.

Moreover, cooperation between academia and cybersecurity experts is intensifying. Ukrainian universities, such as the Kyiv-Mohyla Academy and the Lviv Polytechnic National University, are conducting interdisciplinary research that merges information science, linguistics, and political communication. Their AI-based experimental laboratories simulate disinformation scenarios to study cognitive impacts and algorithmic countermeasures.

An equally significant direction is international cooperation and information exchange. Ukraine actively collaborates with the EU's StratCom division, NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE), and UNESCO programs dedicated to media literacy. These partnerships facilitate knowledge transfer, joint research, and the harmonization of ethical AI standards across countries affected by hybrid warfare.

At the same time, the private technology sector has become an indispensable partner in Ukraine's information defense architecture. Startups specializing in cybersecurity, NLP, and big data analytics-such as Reface, Osavul, and InfoSapiens-develop advanced tools for identifying bot networks, analyzing sentiment trends, and classifying content reliability. This collaboration between the state and the private sector reflects a new paradigm of "whole-of-society" resilience.

AI-powered predictive modeling systems have also proven valuable in assessing the potential escalation of disinformation campaigns. By analyzing historical data and social dynamics, these models can forecast which narratives are likely to gain traction and

identify vulnerable segments of the population most susceptible to manipulation. Such predictive capacity allows for the early deployment of corrective communication and educational initiatives.

Education and awareness campaigns powered by intelligent technologies are transforming citizens from passive consumers of information into active defenders of truth. Gamified learning modules and adaptive AI tutors within Diia.Education and the Media Literacy for All initiative enhance the population's ability to recognize manipulation and engage critically with digital content. This long-term cultural shift is as crucial as technological innovation itself.

Importantly, Ukraine's progress in AI-based disinformation counteraction has drawn international recognition. Reports by UNESCO, the European Commission, and the World Economic Forum cite Ukraine as an emerging leader in the ethical application of AI for information security. The lessons learned here are shaping policy discussions in other countries that face similar hybrid threats.

However, alongside these achievements, certain risks persist. The reliance on large datasets poses privacy concerns, while the use of AI for content moderation raises debates about freedom of expression. Therefore, Ukraine's AI governance model must maintain a delicate balance between protecting information integrity and safeguarding democratic rights. The establishment of independent oversight bodies and transparent auditing mechanisms will be vital to preserving this equilibrium.

Looking ahead, Ukraine's national strategy for intelligent technologies should emphasize resilience, scalability, and inclusivity. Expanding AI literacy among policymakers, journalists, and citizens will help ensure responsible technology adoption. Investment in research infrastructure and ethical design will also reinforce the sustainability of AI ecosystems in the long term.

In conclusion, intelligent technologies are reshaping the landscape of information warfare and national security. Ukraine's innovative use of AI in detecting, analyzing, and neutralizing disinformation

demonstrates how technology can serve democracy, not undermine it. The Ukrainian model-built on transparency, collaboration, and ethical responsibility-offers a valuable blueprint for the international community seeking effective, human-centered solutions to the global disinformation crisis.

Thus, intelligent technologies are now an integral component of Ukraine's information defense. Their use spans monitoring, verification, forecasting, analytics, and education-ensuring a comprehensive approach to combating disinformation. The combination of technical solutions, human expertise, and ethical standards forms the foundation of a new culture of information security-not only during the war but also throughout the country's post-war recovery.

The examples in Table 2.6 reflect the main directions of practical application of intelligent technologies in countering disinformation during war. They show that AI now performs not only an analytical

Table 2.6 – Examples of Applying Intelligent Technologies to Counter Disinformation During War

No.	Example	Country	Core Function	Outcome
1	AI4Media	EU	Analysis of news flows, fake detection, support for journalists	Higher fact-checking accuracy; reduced spread of fakes
2	ClaimBuster	USA	Automatic verification of claims in news	Faster fact-checking; reduced human burden
3	Truepic AI / Deepfake Detector	USA	Recognition of forged images and videos	Assurance of visual content integrity
4	Molfar OSINT	Ukraine	Open-source analysis; detection of botnets and disinformation	Exposure of hostile information attacks; cybersecurity support
5	LetsData AI	Ukraine	Telegram monitoring; classification of propaganda posts	Reduced impact of hostile propaganda; improved monitoring
6	StopFake AI Assistant	Ukraine / EU	Automated fact-checking; creation of a fake database	Trust in verified sources; media literacy development

but also a strategic function-automatically detecting false information, verifying content, and raising the level of the state's information security. Systems such as AI4Media and ClaimBuster demonstrate the effectiveness of integrating machine learning into journalism and communications, reducing human bias in the fact-checking process.

Ukrainian solutions-Molfar OSINT, LetsData AI, and StopFake AI Assistant-confirm the domestic IT sector's ability to develop indigenous information-defense tools even under wartime conditions. Their distinguishing feature is the combination of NLP, social media analysis, and open-source intelligence (OSINT). This enables not only the rapid detection of fakes and botnets but also the forecasting of subsequent information attack vectors. As a result, prerequisites emerge for building an intelligent information-defense system in which automated analytics, trust in verified sources, and the development of societal media literacy play key roles.

Assessing the effectiveness of intelligent technologies in countering disinformation during war shows that AI has become one of the most powerful instruments of information security. Thanks to machine learning, NLP, and big-data analytics, it has become possible to rapidly detect fakes, manipulations, bot farms, and coordinated information attacks. AI systems can identify sources of disinformation, track its diffusion through social networks, and generate forecasts of potential information risks-significantly improving response speed and the effectiveness of strategic communications.

Ukraine's experience in this field underscores the importance of combining intelligent technologies with human expert oversight. During wartime, AI solutions are actively used for monitoring the information space, detecting propaganda, and coordinating governmental media responses. The effectiveness of these technologies is confirmed by the work of analytical centers that, with AI, can process hundreds of thousands of messages per day-previously impossible manually. At the same time, key challenges include ensuring algorithmic accuracy and preventing

model bias, which adversaries could exploit. Overall, intelligent technologies have proven effective as a component of national security in conditions of hybrid warfare. Their further development should rest on the integration of public and private initiatives, the strengthening of scientific and technical capacity, and international cooperation. Combining AI's analytical capabilities with human critical evaluation creates a reliable foundation for a resilient information environment capable of countering disinformation and strengthening Ukraine's information sovereignty.

2.3. VECTORS OF INTELLIGENT TECHNOLOGY DEVELOPMENT FOR THE POST-WAR RECOVERY OF UKRAINE'S ECONOMY

Post-war recovery in Ukraine requires not only rebuilding destroyed infrastructure but also creating a new, innovation-oriented economy capable of ensuring the state's competitiveness in the global technological environment. In this context, the deployment of intelligent technologies-artificial intelligence (AI), machine learning, big-data analytics, robotics, and digital platforms-becomes one of the main drivers of sustainable growth. These technologies underpin the modernization of industry, agriculture, energy, transport, healthcare, and education. It is precisely intelligent technologies that will determine the speed of economic recovery, the level of investment attractiveness, and Ukraine's integration into the European digital space.

The relevance of this agenda stems from the large-scale transformation of Ukraine's production structure after the war. Traditional development models based on labor-intensive processes and low value added no longer meet contemporary challenges. Intelligent technologies enable the emergence of new economic domains-"smart" manufacturing, demand-forecasting energy systems, automated logistics, and digital healthcare. Their implementation

will reduce costs, increase labor productivity, and strengthen the technological sovereignty of the state.

An additional argument for the topic's relevance is the need to integrate Ukraine into the EU's common digital market. The European Union is actively advancing its Digital Europe policy and implementing the EU AI Act, which sets standards for ethical and safe AI use. Alignment with these approaches is strategically important for Ukraine because it opens access to investment, joint projects, and technical-assistance programs. Studying the vectors of intelligent technology development will help define priorities for digital integration and optimal mechanisms for adapting Ukraine's economy to European norms.

The topic's significance is reinforced by the social dimension-human-capital development through digital-skills formation and workforce reskilling. AI creates new professions, raises requirements for managerial and technical competencies, and simultaneously automates routine activities. For Ukraine, this is an opportunity not only to restore jobs but also to build a modern educational ecosystem in which AI supports lifelong learning, personalized education, and the innovation capacity of society.

Ultimately, shaping the vectors of intelligent technology development is fundamental to the state's economic security. The "intellectualization" of the economy can ensure transparent financial flows, efficient resource management, stronger anti-corruption mechanisms, and risk forecasting. This is not merely technological modernization but a systemic shift in managerial culture centered on data, analytics, and the responsible use of AI. Therefore, researching the development vectors of intelligent technologies is key to designing a national recovery strategy focused on innovation, resilience, and Ukraine's European integration (see Table 2.7, p. 90).

The table shows that post-war intelligent-technology development is cross-sectoral and spans both economic and social dimensions. The most promising areas combine technological innovation with

Table 2.7 – Promising Directions for the Development of Intelligent Technologies in Ukraine's Post-War Economy

No.	Development Vector	Application Area	Goal / Expected Effect	Potential Results by 2030
1	Intelligent manufacturing (Industry 4.0/5.0)	Mechanical engineering, energy, logistics	Process automation, digital twins, cost optimization	+30% labor productivity; lower production costs
2	Agro-AI and smart farming	Agriculture, agro-exports	Yield optimization, risk forecasting, loss reduction	+20% yields; –15% resource use
3	Intelligent energy	Renewables, energy management	Demand/supply balancing, smart-grid systems	+25% energy-use efficiency; fewer outages
4	Digital "smart" cities	Municipal management, transport, utilities	Infrastructure optimization, asset monitoring	–20% incidents; –15% maintenance costs
5	Defense and security tech (dual-use AI)	Defense, logistics, security	Spin-off of military AI into civilian domains	Higher tech exports; defense-civil clusters
6	FinTech and RegTech	Banking, insurance, public procurement	Financial transparency, risk analytics, anti-corruption	–40% fraud; stronger investor confidence
7	Medical intelligent systems	Healthcare, telemedicine, rehabilitation	Diagnosis, disease forecasting, treatment optimization	+15% diagnostic accuracy; +30% telemedicine coverage
8	Education and reskilling (EdTech AI)	Formal & non-formal education	Personalized learning, digital skills	500,000 specialists with AI competencies
9	AI analytics in public administration	E-government, public services	Risk forecasting, data-driven decisions	+50% service efficiency; less bureaucracy
10	Ethical and safe AI use	Law, cybersecurity, ethics	Systems for AI oversight, certification, audit	Trust in technologies; alignment with EU AI Act

the restoration of critical infrastructure, higher energy efficiency, and the creation of high value-added jobs. Applying AI in manufacturing, agriculture, energy, healthcare, and education will not only drive recovery but also structural modernization, supporting Ukraine's integration into the European digital space.

Intelligent manufacturing is a foundational vector for a modern economy and a key factor in restoring Ukraine's industrial capacity. Industry 4.0 rests on integrating digital, information, and cyber-physical systems into production processes to enable interaction among equipment, software, and people in a unified information environment. Industry 5.0 goes further, combining automation and AI with human creativity, emphasizing sustainability, energy efficiency, and social responsibility.

For Ukraine, intelligent manufacturing is especially vital because many industrial enterprises still operate with legacy technologies. Recovery requires not merely reconstruction but re-equipment based on digital transformation. AI in manufacturing supports predictive analytics (failure prediction), energy-use optimization, real-time quality control, and the creation of digital twins for risk-free process modeling.

The integration of intelligent manufacturing technologies is expected to become the cornerstone of Ukraine's post-war industrial transformation. By deploying digital twins, predictive maintenance, and AI-driven process control, enterprises can minimize downtime and waste, while maximizing resource efficiency. These systems collect data from sensors across production lines, allowing algorithms to model and predict equipment behavior under varying conditions. Such predictive analytics not only reduce maintenance costs but also ensure higher stability of output – crucial for re-establishing Ukraine's export potential.

A further aspect of Industry 4.0 and 5.0 involves human-machine collaboration. The Fifth Industrial Revolution emphasizes a balance between automation and human creativity, placing workers at the center of technological ecosystems. Ukrainian manufacturing

can use this approach to retrain skilled technicians as operators of intelligent systems rather than manual laborers, thus preserving employment while boosting productivity.

The energy sector represents another strategic field for AI implementation. Intelligent energy systems apply algorithms for demand forecasting, dynamic pricing, and smart-grid optimization. As Ukraine rebuilds its war-damaged energy infrastructure, integrating AI into renewable energy management can increase the efficiency of electricity distribution by up to 25 percent, while reducing outages and losses. AI-based forecasting tools also support the balancing of energy supply from decentralized solar and wind facilities, making the national grid more resilient and sustainable.

Equally promising is the rise of Agro-AI and smart farming, which can transform Ukraine's agricultural sector – one of its traditional economic pillars. Intelligent systems monitor soil moisture, crop growth, and weather data to optimize irrigation, fertilizer use, and harvesting schedules. Using drone imagery and computer vision, farmers can identify pest infestations early and minimize losses. By 2030, the adoption of Agro-AI could raise crop yields by 20 percent while lowering resource consumption by 15 percent, reinforcing Ukraine's position as a global food supplier.

AI-driven smart-city development offers the potential to rebuild Ukrainian urban areas according to sustainable and efficient principles. Intelligent traffic management, digital utilities monitoring, and predictive maintenance of infrastructure can reduce operational costs and environmental impact. Cities such as Kyiv, Lviv, and Dnipro are already testing pilot systems for smart lighting, waste management, and mobility platforms. In post-war reconstruction, expanding these projects could help create safer, greener, and more inclusive urban environments.

Defense and security technologies form a dual-use segment where innovations initially developed for military applications are later adapted for civilian industries. AI-assisted logistics, drone navigation, and cybersecurity platforms designed during wartime can evolve into

commercial products that enhance national security and export potential. The development of defense-civil innovation clusters will promote technology transfer, increase high-tech exports, and foster closer cooperation between the defense sector and civilian manufacturing.

In the financial sphere, FinTech and RegTech solutions are transforming transparency and risk management. AI algorithms can detect anomalies in financial transactions, monitor procurement for signs of corruption, and ensure compliance with regulatory standards. For Ukraine, implementing these technologies could reduce fraud cases by up to 40 percent and improve investor confidence. Intelligent financial ecosystems can also simplify access to credit for small businesses and facilitate integration with EU digital payment systems.

Healthcare and medical intelligent systems constitute another transformative vector. AI-based diagnostic tools, predictive analytics for disease prevention, and telemedicine platforms can significantly enhance healthcare accessibility and efficiency, especially in rural and war-affected regions. By analyzing imaging data or electronic health records, AI models assist physicians in detecting diseases earlier and choosing optimal treatments. Expanding telemedicine coverage by 30 percent would not only improve health outcomes but also reduce the strain on Ukraine's medical infrastructure.

The field of education and reskilling is critical for building human capital in a digital economy. Adaptive learning platforms powered by AI personalize educational trajectories based on each learner's progress, capabilities, and career goals. Such systems are indispensable for retraining hundreds of thousands of specialists who must acquire competencies in data analysis, programming, and digital management. By 2030, Ukraine could train over half a million professionals equipped with AI-related skills – forming the foundation for sustainable innovation-driven growth.

AI analytics within public administration is another high-impact direction. Data-driven decision-making allows public authorities to anticipate risks, monitor policy implementation, and allocate resources

more effectively. Machine-learning-based tools for predictive modeling and anomaly detection can uncover inefficiencies in bureaucratic processes and suggest corrective measures. Implementing these systems could increase the efficiency of public services by 50 percent while reducing administrative costs and corruption.

Ensuring ethical and safe use of A**I** is essential for maintaining citizens' trust. Establishing a national system for AI certification, oversight, and audit – aligned with the EU AI Act – will provide clear standards for data protection, fairness, and accountability. Such regulatory convergence will accelerate Ukraine's accession to the European digital market and guarantee that technological progress remains consistent with democratic values and human rights.

Cross-sectoral integration of intelligent technologies will have a cumulative effect. The interaction between smart manufacturing, digital energy, and FinTech will generate a multiplier impact on productivity and sustainability. The creation of shared data hubs and AI-based analytics platforms across industries will enable holistic decision-making and foster synergies between economic, environmental, and social development goals.

At the same time, human capital development and institutional reform are prerequisites for realizing these opportunities. Strengthening STEM education, supporting research universities, and promoting innovation culture will determine the pace of technological transformation. Public-private partnerships should focus on incubating AI start-ups and scaling them to international markets, while ensuring gender equality and inclusiveness in digital professions.

International cooperation will remain a vital factor in accelerating Ukraine's digital recovery. Collaboration with the European Union, the United States, Japan, and South Korea can attract investment, transfer advanced knowledge, and facilitate joint research projects. Participation in programs such as Horizon Europe and the Digital Europe Programme will provide funding and expertise necessary to establish Ukraine as a regional hub for ethical and secure AI innovation.

In conclusion, the development of intelligent technologies in Ukraine's post-war economy is not merely a matter of technological modernization-it is a strategic path toward sustainable recovery, social resilience, and global competitiveness. By 2030, the country has the potential to transition from a resource-based model to a knowledge-based, innovation-driven economy. Intelligent technologies-grounded in ethics, efficiency, and human-centered design-will form the backbone of this transformation, positioning Ukraine as a digital leader in Eastern Europe and a key contributor to the European technological landscape.

One major advantage of Industry 4.0 is higher productivity and system efficiency. According to sectoral analyses, intelligent control systems can raise labor productivity by 25–30%, reduce energy costs by 15–20%, and cut production waste by nearly a third-enhancing competitiveness, reducing technology imports, and supporting export growth of high value-added products. Intelligent manufacturing also fosters a new management culture: AI brings process transparency, enables data-driven management, minimizes human error, and frees time for innovation. The transition to Industry 5.0 humanizes production-prioritizing human-machine collaboration, creativity, flexibility, and environmental awareness-thereby aligning growth with sustainability (see Fig. 95, p. 96).

The figure depicts the core technological components shaping modern intelligent manufacturing within the Industry 4.0/5.0 paradigms. The largest share (about 20%) comprises AI and data analytics – the driver of automation, process optimization, and data-driven decision-making (predictive maintenance, quality control, resource management). The next group – IoT and robotics (about 15% each) – enables real-time data exchange among equipment and raises productivity and accuracy while reducing human risk. Digital twins, big data, and cybersecurity (about 10% each) are critical for process modeling, large-scale analytics, and protecting industrial systems from cyberattacks. Smaller but strategic components – AR/VR, 3D printing, cloud services, and human-centric systems (about 5%

each) – support rapid prototyping, remote assistance and training, and a humanized human-machine interface central to Industry 5.0. Overall, intelligent manufacturing is a multi-layer ecosystem in which digital technologies, humans, and data interact-strategic for Ukraine's technological modernization and EU – oriented innovation integration.

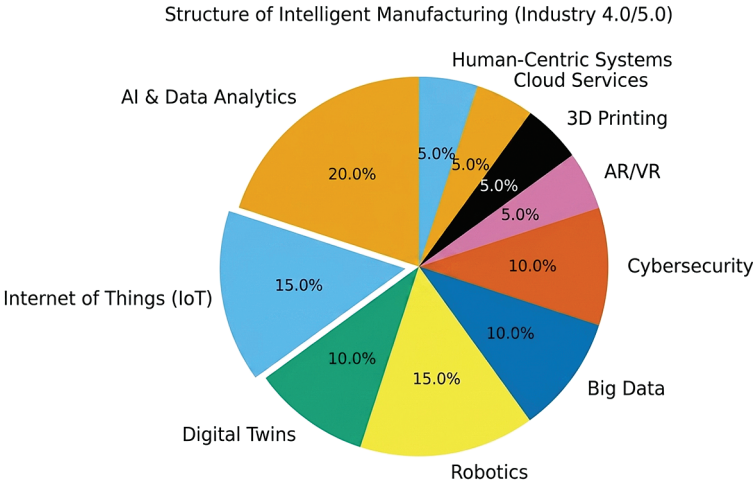

Figure 2.4 – Structure of Intelligent Manufacturing (Industry 4.0/5.0)

Agro-AI integrates AI, big-data analytics, IoT, satellite monitoring, and robotics into agriculture. The goal is to optimize production, increase yields, use resources rationally, and reduce environmental impact. For Ukraine-where agriculture generates over 40% of foreign-currency inflows-digitizing the agro sector is strategic: it restores export potential and builds a sustainable farming model based on precise land management, minimized losses, and higher product quality.

Applications include satellite mapping, automated monitoring of soils and crops, yield forecasting, computer-vision detection of plant diseases, and AI-assisted irrigation and fertilization using IoT sensors. Analytics platforms and mobile apps interpret data from drones, satellites, and sensors-democratizing access to advanced tech even for

small farms. Agro-AI also advances sustainability by reducing water, pesticide, and fertilizer use-supporting SDGs 2, 12, and 13.

Table 2.8 – Key Areas for Applying Intelligent Technologies in Ukrainian Agriculture (Agro-AI)

No.	Area	Technologies	Primary Purpose	Expected Effect
1	Crop & soil monitoring	Satellites, drones, IoT sensors, image analytics	Detect low-yield zones, moisture deficits, pests	–15–20% crop loss; better control
2	Yield forecasting	ML algorithms, neural networks	Analyze climate, moisture, soil composition	Production planning; logistics optimization
3	Smart irrigation	IoT, moisture sensors, automated pumps	Weather- and plant-condition-based irrigation	Up to 30% water savings; higher yields
4	Weather-risk forecasting	Meteomodels, big data, satellite data	Early warning of extreme events	Lower loss risk; more stable output
5	Disease & pest recognition	Computer vision, classifiers	Identify affected areas; treatment guidance	Timely containment; fewer pesticides
6	Intelligent logistics & storage	Big data, RFID, optimization	Supply-chain control; demand forecasting	–10–15% transport costs
7	AgroFin-AI (credit/ insurance)	AI scoring, risk analytics	Farmer creditworthiness; crop insurance	Access to finance; fewer defaults
8	Robotic farms	Autonomous tractors, harvest robots	Automation of routine operations	+20–25% labor productivity
9	Digital field maps & farm ERP	GIS, mobile apps, cloud	Centralized farm management	Lower admin costs; better planning
10	Environmental monitoring	AI analytics, satellites	Detect erosion, pollution, land-use change	Soil conservation; sustainability control

Table 2.8 reflects the key areas of applying intelligent technologies in agriculture that can enable Ukraine's transition to a model of precision, environmentally sustainable farming.

The use of Agro-AI increases agribusiness efficiency through accurate forecasting, automation, reduced human error, and prudent use of resources. Particularly promising are intelligent irrigation systems, robotic farms, and AI-based financial-risk analytics, which will directly contribute to the modernization of Ukraine's agricultural sector and its integration into the global market for innovative agrotechnologies.

EOS Data Analytics – Ukraine. The company provides the EOSDA Crop Monitoring platform, which combines satellite imagery, analytics, and IT tools for farmers. It is used by Ukrainian agribusinesses to monitor crop conditions, identify plant-stress zones, and optimize the use of crop protection products and other resources. Effect: improved field management efficiency, reduced losses, and better agronomic control.

DroneUA in partnership with Syngenta – Ukraine. DroneUA, a leader in Ukraine's drone market, collaborates with Syngenta to deploy agri-drones and precision-farming technologies in Ukrainian fields. Effect: optimization of field operations, drone-based monitoring, and reduced resource consumption.

Ukrainian Company X (name not specified) – dairy farming solution. A Ukrainian company has proposed a platform with a smart collar for cows using IoT sensors and AI algorithms to manage livestock health, reproduction cycles, and feeding. In trials, milk production increased by up to 27%. Effect: higher productivity, lower maintenance costs, and improved herd condition control.

The diagram shows the main areas of intelligent-technology deployment in Ukrainian agriculture as of 2025.

As seen, the largest share (about 25%) is accounted for by crop and soil monitoring, based on satellite analytics, drones, and IoT sensor systems. This is because these technologies are the fastest

to implement and deliver a tangible economic effect-reducing losses and optimizing the use of water and fertilizers.

Around 15% is yield forecasting based on machine learning, which helps farmers plan production volumes and logistics. 10% corresponds to intelligent irrigation systems, which can cut water use by up to 30%, as well as disease and pest recognition, which reduces reliance on chemical protection agents.

Other areas-AgroFin-AI, logistics, robotization, and environmental monitoring-represent smaller but strategically important shares, as they form the innovative core of "smart agribusiness," integrating production technologies, finance, and sustainable development.

It is worth noting that dozens of initiatives and startups are already operating in Ukraine to implement these directions-including EOSDA Crop Monitoring, DroneUA, AgriEye, Agrohub, and OneSoil Ukraine. They integrate artificial intelligence into farming processes, providing analytical support to both large agribusiness holdings and small farms.

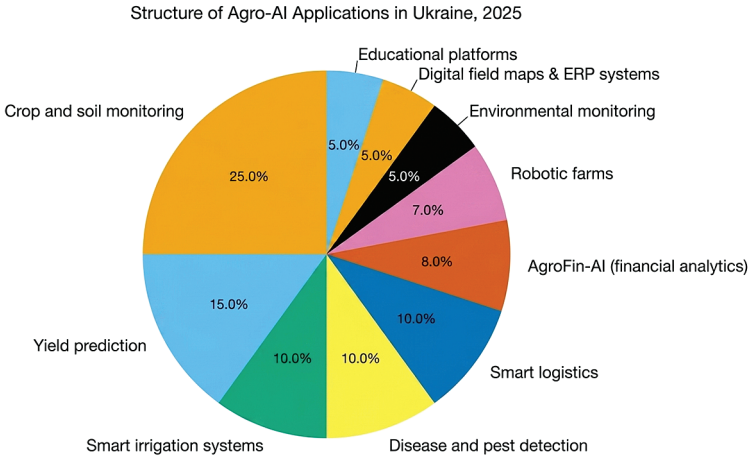

Figure 2.5 – Structure of Agro-AI Applications in Ukraine, 2025

The figure shows the principal directions of Agro-AI deployment as of 2025. The largest share (≈25%) is crop/soil monitoring via satellite analytics, drones, and IoT-fast to implement and economically impactful. Yield forecasting (≈15%) supports production and logistics planning. Smart irrigation (~10%) can cut water use by up to 30%; computer-vision disease detection similarly reduces reliance on chemicals. Other directions – AgroFin-AI, logistics, robotics, environmental monitoring-are smaller in share but strategically important, forming the innovation core of "smart agribusiness." Ukraine already hosts dozens of initiatives (e.g., EOSDA Crop Monitoring, DroneUA, AgriEye, Agrohub, OneSoil Ukraine) that embed AI across farm processes for both large holdings and smallholders.

Intelligent energy is a modern model for managing energy systems based on AI, IoT, big data, cloud computing, and predictive analytics. Its aim is efficient, safe, and environmentally sustainable use of energy resources and real-time optimization of generation, distribution, and consumption.

For Ukraine, intelligent energy is a key vector of post-war recovery. Damaged infrastructure, losses, resource shortages, and import dependence necessitate a shift toward a decentralized, "smart" energy system built on local grids, renewables, and digital control. AI supports demand-supply balancing, renewable-generation forecasting, and peak-load optimization-minimizing losses, lowering incident rates, and increasing supply stability.

A core direction is smart-grid development-digital control, automated diagnostics, consumption analytics, and integration of distributed energy resources. Building energy efficiency also matters: AI optimizes HVAC and lighting systems (see Table 2.9, p. 100).

The largest share is represented by Smart Grids – about 20%, which is explained by the priority of creating a flexible, decentralized, and automated energy infrastructure. Such networks allow real-time load balancing, energy loss control, and integration of renewable energy sources into the overall power system (see Fig. 2.6, p. 102).

Table 2.9 – Core Directions of Intelligent Energy Development in Ukraine

No.	Direction	Technologies / Solutions	Primary Purpose	Expected Result
1	Smart grids	IoT sensors, SCADA, big data, AI analytics	Automated distribution; load balancing	–20–25% electricity losses
2	Renewables generation forecasting	ML, neural nets, meteorological analytics	Optimize solar/ wind operations	Fewer imbalances; system stability
3	Intelligent demand management	Smart meters, EMS, AI algorithms	Control & plan consumption	Up to –15% household energy use
4	Smart building / city energy	AI for HVAC, IoT controllers	Reduce building energy use	Higher urban energy efficiency
5	Microgrid management	Edge computing, decentralized control	Balance local sources	Community/ enterprise autonomy
6	AI for asset maintenance	Predictive maintenance, sensors	Failure prediction; lower downtime	–30% incidents & repair costs
7	Tariff & market optimization	Big data, AI analytics, blockchain	Model demand/ supply; flexible tariffs	Transparent market; price optimization
8	Storage & battery management	AI BMS	Improve storage efficiency	Longer battery life
9	Grid cybersecurity	AI threat/ anomaly detection	Real-time attack detection	Protection of critical infrastructure
10	Data-driven energy analytics	Cloud computing, visualization	Decision support in management	Better, data-backed decisions

The figure highlights priorities in 2025: smart grids (≈20%) to create flexible, decentralized, automated infrastructure; renewables forecasting (≈12%); intelligent consumption (≈20%). Other directions-predictive maintenance, cybersecurity, storage systems, and data-driven analytics (≈7–10% each)-are strategically essential for reliability, cyber-resilience,

storage efficiency, and analytical decision-making. Together, these components enable a transition from a centralized legacy system to a decarbonized, resilient, and technology-oriented energy model aligned with Europe's "green transition."

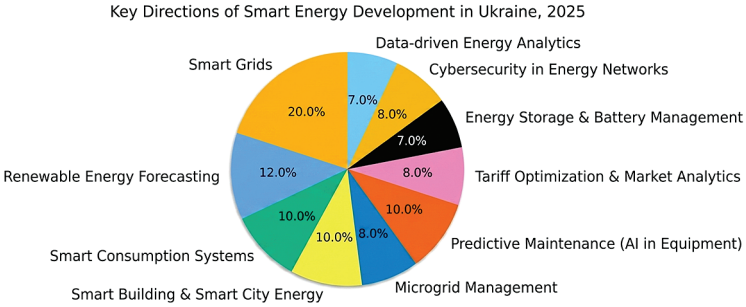

Figure 2.6 – Key Directions of Smart-Energy Development in Ukraine, 2025

The smart city concept integrates digital technologies, AI, IoT, big-data analytics, and GIS into urban governance to improve quality of life, resource efficiency, and sustainable territorial development. In Ukraine's post-war recovery, digital smart cities are strategic: they merge infrastructure reconstruction with service digitalization and modern management. Municipalities gain transparency, better environmental performance, lower energy use, and more effective transport and safety management. A unified urban digital ecosystem aggregates data from utilities, transport, energy, social and medical services. AI then generates analytics, forecasts risks, optimizes resource allocation, and supports decisions.

In Ukraine, smart-city development is supported by national programs (Smart City Ukraine, Diia.City, EU4DigitalUA) and local initiatives (Kyiv, Lviv, Vinnytsia, Kharkiv, Dnipro, Ivano-Frankivsk): digital maps, safe-city systems, smart lighting, energy-efficient buildings, e-services, and citizen apps (see Table 2.10, p. 103).

Table 2.10 – Main Directions for Developing Digital "Smart Cities" in Ukraine

No.	Direction	Core Technologies	Purpose	Expected Result
1	Smart mobility	IoT, AI, GPS, video analytics	Manage traffic, transit, parking	–20–25% congestion; lower CO_2
2	Smart energy use	AI, smart grids, smart meters	Optimize consumption; reduce losses	–15–20% energy use; transparent tariffs
3	E-governance	Cloud, blockchain, Diia platforms	Provide services online	Higher transparency; lower corruption risks
4	Safe city	Video surveillance, face recognition, AI analytics	Public-safety monitoring, incident response	–10–15% crime
5	Smart utilities	IoT sensors, monitoring systems, big data	Network condition control; waste & water mgmt	–20–30% water/ heat losses
6	Environmental monitoring	IoT, satellites, AI models	Air quality, noise, pollution tracking	Better urban environmental metrics
7	Smart lighting	IoT, motion sensors, control systems	Lower lighting energy use; safety	Up to –40% electricity for lighting
8	Digital urban planning	GIS, big data, AI modeling	Optimize zoning, transport, infrastructure	More effective urban development
9	E-health	Telemedicine, AI diagnostics, mobile apps	Improve access to care	Better health outcomes; lower hospital load
10	Civic participation	Mobile apps, chatbots, social platforms	Citizen – government engagement	More trust and civic activity

Smart-city development in Ukraine thus blends technological solutions with human-centric goals. The most dynamic areas-smart mobility, smart energy, and e-governance-directly improve quality of life and municipal efficiency. Smart utilities and environmental

monitoring build resilience against emergencies and reduce energy losses. Crucially, services must remain convenient, accessible, and safe-strengthening trust and fostering a culture of transparent, sustainable urban governance.

Defense and security AI (dual-use) encompasses innovative solutions applicable in both military and civilian domains. They reinforce national security, raise defense capability, and catalyze high-tech industry development. Key areas include automated intelligence analysis, threat detection, autonomous unmanned systems, cyber defense, risk/crisis forecasting, and AI for logistics, communications, and medical support. Dual-use transfer brings military technologies into the civilian economy (e.g., drones for infrastructure monitoring, analytics for urban security, robotics for rescue operations), forming an innovation ecosystem where defense R&D fuels technological progress and economic growth.

Table 2.11 – Core Directions for Developing AI-Based Defense and Security Technologies

No.	Area	Technologies	Primary Purpose	Examples
1	2	3	4	5
1	Intelligence & data analysis	AI on satellite/UAV data	Detect equipment; track troop movements	↑ reconnaissance accuracy by ~40%
2	Unmanned systems	Autonomous drones/robots; AI navigation	Monitoring, logistics, defense ops	Lower human risk; higher combat efficiency
3	Cybersecurity & cyber defense	AI threat/anomaly detection; SIEM	Protect critical infrastructure	–30% cyber incidents
4	Information security & anti-disinformation	NLP, ML, OSINT	Detect fakes and information attacks	Stronger information sovereignty
5	AI in military logistics	Route optimization; supply forecasting	Frontline resourcing	–25% delays; fuel savings
6	Smart comms & C2	Neural nets, data fusion, cloud AI	Unit coordination; situational awareness	–35% reaction times

End of Table 2.11

1	2	3	4	5
7	AI in military medicine	Medical robots, diagnostics, tele-assist	Treatment and evacuation	Higher survival; faster response
8	Crisis & risk forecasting	Big data, simulation AI, DSS	Plan defense & humanitarian ops	Fewer losses; better planning
9	Dual-use civilian applications	AI drones, computer vision, autonomy	Energy, transport, agriculture, etc.	Exports; new high-tech jobs
10	International cooperation & standards	AI governance, ethics, interoperability	NATO/EU/OECD alignment	Participation in global tech alliances

Defense AI spans all levels of national security-from cyberspace to military medicine. It delivers rapid analytics, automatic threat detection, and real-time decision support. Especially promising are autonomous systems, crisis forecasting, and anti-disinformation-validated during the war in Ukraine. Beyond military benefits, dual-use AI carries substantial economic potential: defense startups can evolve into civilian tech firms delivering solutions for energy, healthcare, transport, and urban safety. Thus, defense innovation becomes a catalyst for the country's technological recovery (see Fig. 2.7, p. 106).

Figure 2.7 illustrates the structure of the principal directions in the development of dual-use AI defense and security technologies in Ukraine. The largest shares – 15% each-are AI Intelligence & Reconnaissance (intelligence and data analytics powered by AI) and Autonomous Systems (autonomous aerial and ground unmanned systems). These areas are priorities for Ukraine's defense sector because they provide high accuracy, faster decision-making, and reduced risk to personnel in combat conditions [131].

Approximately 12% is accounted for by Cybersecurity & Cyber Defense, reflecting the need to protect critical infrastructure from cyberattacks, while 10% goes to Information Security / Disinformation, aimed at combating fakes, information manipulation,

and propaganda. AI Logistics (10%) and Command & Control Systems (8%) also play important roles, ensuring efficient resource management, coordination, and logistical support for military units. Other directions-AI in Military Medicine, Crisis & Risk Prediction, Civilian Dual-use Applications, International Cooperation-each hold 7–8%, yet remain strategically significant [130]. They support the development of medical technologies to save lives, build systems for forecasting crises, transfer military innovations to civilian sectors, and integrate Ukraine into the international technological security system (including cooperation with NATO and the EU) [126–128].

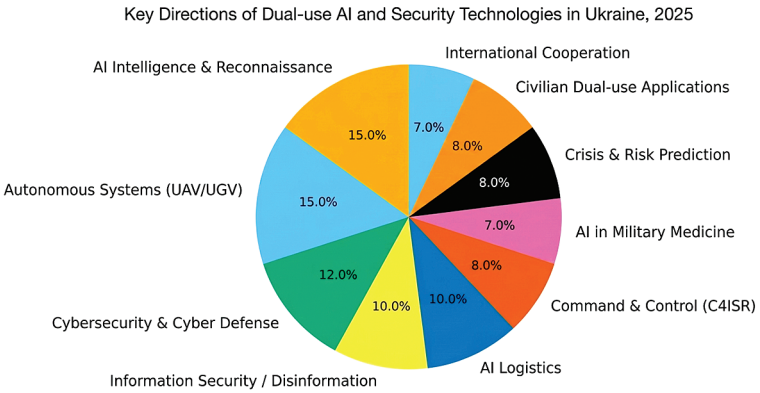

Figure 2.7 – Key Directions of Dual-use AI and Security Technologies in Ukraine, 2025 [130]

Overall, the diagram shows that intelligent defense technologies are not only tools of military advantage but also drivers of economic growth. Their dual (military – civilian) nature opens new opportunities for startup development, the creation of high-tech jobs, and strengthening Ukraine's position in the global innovation market.

FinTech (financial technology) and RegTech (regulatory technology) combine finance, information technologies, and AI analytics to increase the efficiency of financial operations, market transparency, and compliance with regulatory requirements. In the post-war period,

FinTech solutions underpin the restoration of Ukraine's financial infrastructure, while RegTech technologies ensure its stability, anti-corruption safeguards, and alignment with EU standards.

FinTech supports automated payments, lending, insurance, customer service, and the rollout of AI credit scoring, blockchain payments, and central bank digital currencies (CBDC). RegTech helps financial institutions meet AML/CFT requirements, reporting, compliance, and data protection.

Integrating intelligent technologies into these sectors enables banks, insurers, and state regulators to reduce operating costs, accelerate risk detection, and ensure transparency of financial flows.

In Ukraine, such solutions are being implemented within Diia. Business, by the National Bank of Ukraine (NBU), the Ministry of Digital Transformation, and private companies including Monobank, PrivatBank, SettlePay, Finmap, and KPMG Ukraine Digital Lab.

A key trend is the creation of a unified FinTech ecosystem in which intelligent tools monitor transactions and analytical algorithms identify suspicious activity in real time-balancing innovation and financial security.

Table 2.12 – Main Directions of FinTech and RegTech Development in Ukraine

No.	Direction	Technologies	Primary Purpose	Expected Result
1	2	3	4	5
1	AI scoring & credit analytics	ML, neural networks	Assess client creditworthiness	Faster lending; –20–30% defaults
2	Next-gen payment systems	APIs, blockchain, cloud	Instant payments; e-commerce integration	Transaction time down to ~1s
3	Smart insurance (InsurTech)	Big Data, predictive analytics	Automated risk assessment & payouts	Less fraud; tailored products
4	Regulatory analytics (RegTech AI)	AI compliance, anomaly detection	Detect violations in financial operations	Fewer fines; more transparency

End of Table 2.12

1	2	3	4	5
5	Anti-fraud & AML monitoring	AI analytics, graph databases	Detect fraud schemes and suspicious links	Reduced money-laundering cases
6	Cybersecurity of financial systems	AI threat detection, biometric ID	Protect bank data; user identification	Higher trust & cyber-resilience
7	Regulatory reporting & audit	NLP, automated reports, robo-analytics	Report generation; standards compliance control	Up to 50% savings on audit effort
8	Financial inclusion & digital currencies	CBDC, mobile wallets, blockchain	Broader access to financial services	Increased public participation
9	Investment & robo-advisory platforms	AI, portfolio analytics	Automated investment management	Better investment outcomes
10	State regulatory monitoring systems	Big Data, AI dashboards	Market analysis; crisis early warnings	Transparent regulation; anti-corruption gains

These directions show that FinTech and RegTech are becoming the core of Ukraine's digital economy, enabling efficient interaction among business, citizens, and the state. The most dynamic areas are AI scoring, InsurTech, and AML solutions, which rapidly identify risks, automate financial decisions, and build market trust.

By 2030, the creation of a unified RegTech Hub Ukraine is anticipated to synchronize financial institutions, the NBU, the State Tax Service, and anti-corruption agencies via APIs and real-time analytics-supporting integration into the European digital financial space and strengthening transparency, trust, and resilience (see Fig. 2.8, p. 109).

The diagram depicts the key directions of FinTech and RegTech development in Ukraine in 2025, now central drivers of the sector's digital transformation.

The largest share –15% – is AI Scoring & Credit Analytics, reflecting widespread AI use for credit assessments and risk management. About 12% is Next-Gen Payment Systems based

on blockchain, cloud services, and open APIs, enabling instant transactions, e-commerce integration, and a cashless economy. Other strategically important directions – InsurTech (10%), Regulatory Analytics (10%), Anti-Fraud & AML Monitoring (10%), and Cybersecurity (10%) – reduce fraud, improve operational transparency, and strengthen data protection.

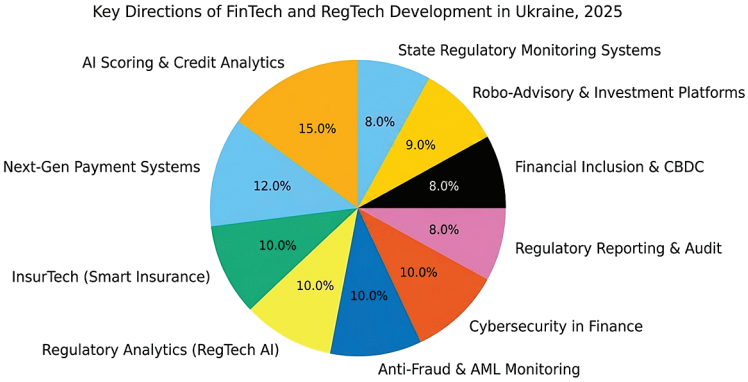

Figure 2.8 – Main Directions of Financial and Regulatory Technology Development

Smaller but vital areas-Robo-Advisory Platforms, CBDC, Regulatory Reporting & Audit-automate asset management, expand financial inclusion, and build a digital trust space among business, government, and citizens. Thus, Figure 2.8 shows FinTech and RegTech forming the foundation of Ukraine's future financial ecosystem-innovation-, security-, and transparency-oriented. In the near term, the combination of AI, blockchain, and data analytics will be the key factor in integrating Ukraine's financial market into the European digital space.

The war in Ukraine has created unprecedented challenges for healthcare: destroyed hospitals, staff shortages, high rates of injuries and psychological trauma-all requiring a new model of care that works under resource constraints. Developing AI health systems is therefore strategically important for both wartime and post-war recovery.

AI enables automated medical-image analysis, disease diagnosis, complication forecasting, treatment planning, and patient-flow management-improving accuracy, reducing time to diagnosis, and easing staff workloads. AI is also critical for telemedicine, especially for patients in remote or affected regions.

According to Ukraine's Ministry of Health and the WHO, as of early 2025:

– over 1,200 medical facilities had been damaged;
– about 180 were completely destroyed;
– more than 20% of medical personnel had been evacuated or were working in field conditions.

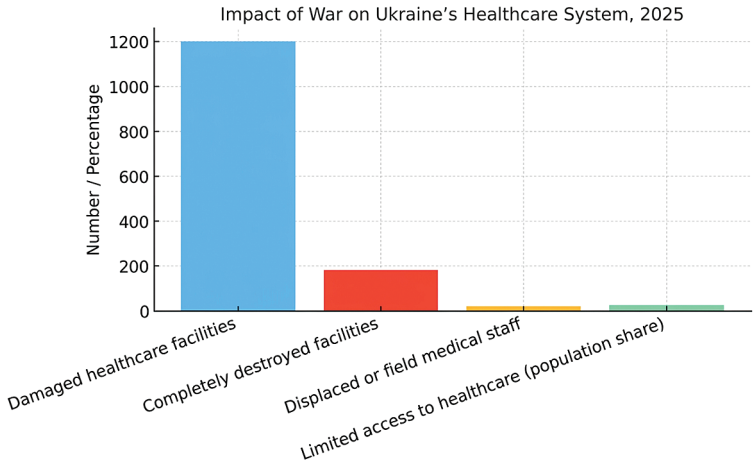

Figure 2.9 – Impact of War on Ukraine's Healthcare System, 2025

Figure 2.9 clearly demonstrates the extent of healthcare system damage. The destruction and impairment of facilities hinder access to basic services, especially in frontline regions. Over 20% of physicians and nurses have been displaced or are serving in field hospitals; more than a quarter of the population faces difficulty accessing care. These data underscore the urgent need to roll out AI health systems, telemedicine, and mobile clinics to compensate for

infrastructure losses, provide remote care, and lay the groundwork for post-war recovery. AI ensures service continuity, remote diagnostics, and large-scale data collection and processing to rebuild the system.

Table 2.13 – Main Directions for Developing AI-Based Medical Systems in Ukraine

No.	Direction	Technologies	Primary Purpose	Expected Effect
1	AI diagnosis of medical images	Computer vision, neural nets	Detect trauma, oncology, infections	+25–40% diagnostic accuracy
2	Telemedicine & remote monitoring	IoT, mobile apps, data analytics	Care delivery in war zones	Better access; time savings
3	AI clinical-decision support	Neural models, NLP	Physician assistance in diagnosis/treatment	Fewer medical errors
4	Psychological rehabilitation via AI	Chatbots, NLP, affective AI	Support for veterans and victims	–15–20% PTSD symptoms
5	Medical robotics	Surgical robots, rehab devices	Automate procedures; prosthetics	More effective recovery
6	Patient-flow management	Predictive analytics, Big Data	Optimize hospital resources	Shorter queues; less overload
7	Pharmacoanalytics & bioinformatics	AI drug design, protein modeling	New drugs and vaccines	3–4× faster R&D cycles
8	Early-warning systems	Outbreak-detection algorithms	Monitor infection risks	Outbreak prevention
9	e-Health (Diia. Med)	Cloud data, blockchain, digital cards	Unified medical records; data transparency	Easier paperwork; secure exchange
10	AI-enabled staff training	Virtual simulators, AR/VR	Training and reskilling	Higher professional competence

Table 2.13 shows that AI medical systems are both technological and humanitarian instruments. The most crucial directions – AI diagnostics, telemedicine, and psychological support-relieve staff burdens, ensure access in remote communities, and assist veterans. These solutions build an adaptive, resilient healthcare system for wartime challenges and lay the foundation for post-war digital transformation focused on infrastructure restoration, professional education, and rehabilitation.

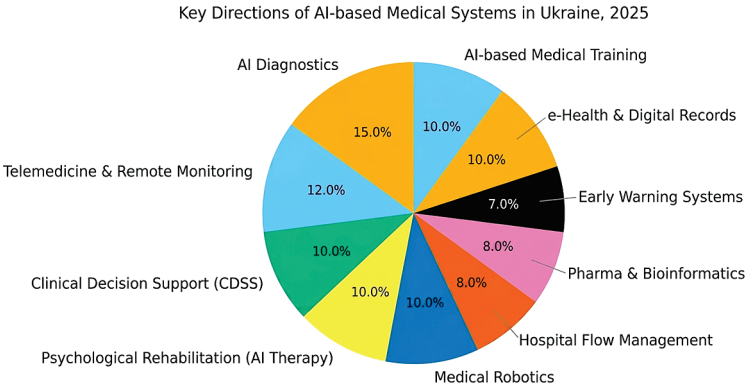

Figure 2.10 – Key Directions of AI-Based Medical Systems in Ukraine, 2025

Figure 2.10 shows how AI deployment is distributed in Ukraine's health sector. The largest shares are AI Diagnostics (15%) and Telemedicine (12%), reflecting priorities in remote care, digital diagnostics, and access during the war. Around 10% each is allocated to AI clinical-decision support, medical robotics, psychological rehabilitation, and digital staff training-helping clinicians improve accuracy, reduce human error, and maintain professional standards under crisis conditions. Overall, the diagram indicates that AI in medicine is essential to the resilience of Ukraine's healthcare system-saving lives during the war and laying the groundwork for post-war modernization.

Ukraine's education system is among the sectors most affected by the war: hundreds of schools and universities destroyed, millions of learners forced into remote study, and a share of teachers emigrating or working under occupation. In these conditions, AI in Education plays a key role in preserving quality, supporting teachers and students, and rebuilding scientific capacity.

AI enables:

– personalized learning adapted to each learner's level;
– automated assessment and feedback;
– support for instructors in creating digital courses;
– intelligent monitoring of learning outcomes;
– AI-driven research.

The post-war education strategy pairs infrastructure restoration with digitalization: every new school, college, or university should be "smart," equipped with e-learning systems, analytics platforms, and adaptive environments.

According to Ukraine's Ministry of Education and Science (2025):

– 3,200+ educational institutions have been damaged or destroyed;
– 5+ million learners studied online for some period;
– about 30% of teachers work in blended or remote formats.

Figure 2.11 (see p. 114) shows damage levels as of January 2023. The eastern regions suffered the most – Donetsk (67%), Kharkiv (43%), Luhansk (41%) – with prolonged hostilities. Significant destruction is also seen in southern frontline regions – Kherson (22%) and Mykolaiv (18%). Central and southern regions – Kyiv, Zaporizhzhia, Dnipropetrovsk, Odesa, Chernihiv – also face notable losses. The uneven impact underscores critical challenges to educational continuity and funding needs for repair and rebuilding.

Widespread damage forced large-scale shifts to online or blended learning, often with unstable connectivity and insufficient equipment. Many teachers now work remotely or in hybrid modes, affecting pedagogy and learner well-being. These factors increase the need for

intelligent educational technologies (AI, adaptive learning, remote support) to offset infrastructure losses and secure quality education during and after the war (see Fig. 2.12).

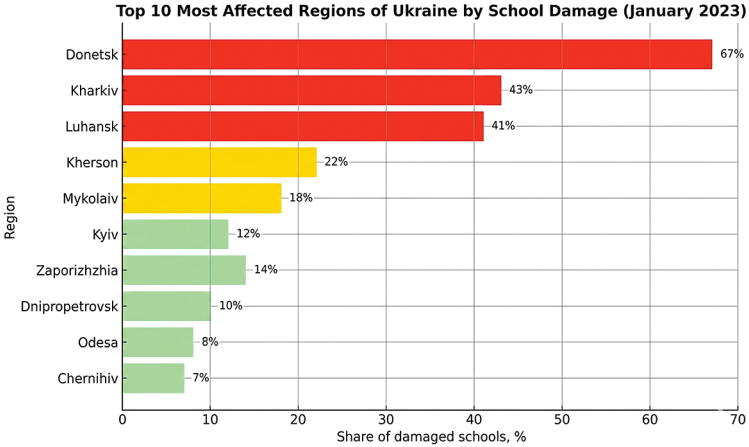

Figure 2.11 – Ten Most Affected Regions of Ukraine by School-Infrastructure Damage

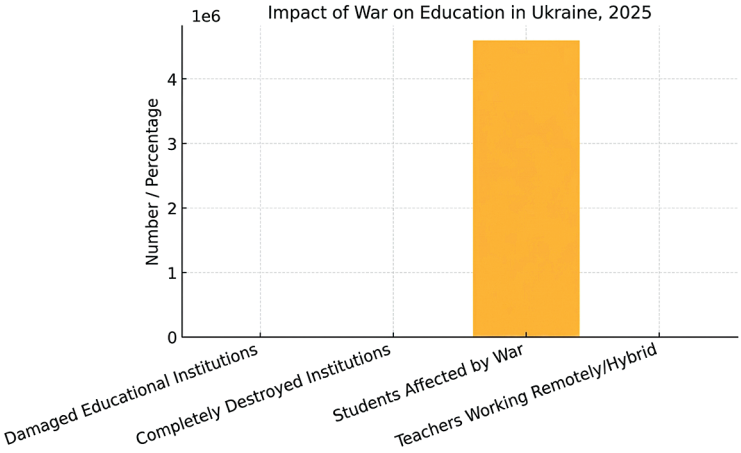

Figure 2.12 – Impact of War on Education in Ukraine, 2025

Figure 2.12 depicts the scope of destruction and transformation in education: millions learning online or in blended formats, often without stable connections or resources; roughly a third of teachers working remotely. In this context, AI and education digitalization are pivotal-providing flexibility, personalization, and continued access to quality education during crisis.

Table 2.14 – Main Directions for Implementing AI in Education and Science in Ukraine

No.	Direction	Technologies	Primary Purpose	Expected Effect
1	Adaptive learning	AI learning platforms, ML	Personalized instruction	Higher motivation and achievement
2	Automated assessment	NLP, text recognition	Marking tests, essays, open responses	Less instructor workload
3	Intelligent educational assistants	Chatbots, generative AI	Student advising; learning support	Expanded access to knowledge
4	AI in vocational education	VR/AR, simulation AI	Technical-skills simulations	Better practical skills
5	Learning analytics	Big Data, AI dashboards	Performance analysis; risk prediction	Early detection of learning gaps
6	AI-driven research	ML, data mining	Automated data collection & modeling	Faster scientific discovery
7	Digital campuses & virtual universities	Cloud learning, blockchain ID	Remote education; credentialing	Access to global education
8	Language support & translation	NLP, speech recognition	Bilingual learning support	Easier integration abroad
9	Student psychological support	AI emotional analytics	Detect stress and burnout	Better well-being
10	EdTech governance	Data-driven decision systems	Data-based school & university management	Transparency; efficient policy

Table 2.16 shows that AI spans both pedagogical and managerial levels. The most dynamic areas-adaptive learning, learning analytics, AI-enabled research, and EdTech governance-drive effective knowledge management. AI helps close war-induced learning gaps and modernize education to European digital standards.

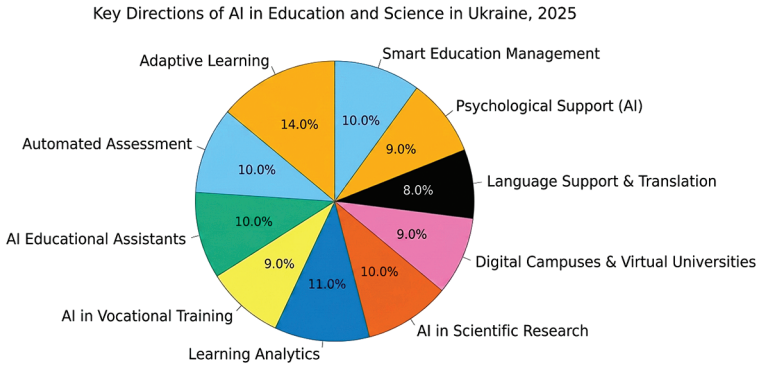

Figure 2.13 – Key Directions of AI in Education and Science in Ukraine, 2025

The leading directions are Adaptive Learning (14%), Learning Analytics (11%), and AI Educational Assistants (10%) – delivering personalization, performance monitoring, and support for students and faculty. AI becomes a central instrument of Ukraine's post-war educational transformation, enabling inclusive, resilient, high-tech learning accessible regardless of location or infrastructure.

AI is a key instrument for digitally transforming the state, boosting bureaucratic efficiency, and ensuring governmental transparency. For post-war Ukraine, AI in the public sector has a dual role:

– optimizing governance, reducing corruption risks, and speeding decisions;

– creating a "digital state of trust" centered on citizens.

AI systems analyze large state-registry datasets, forecast budget risks, detect procurement fraud, and automate citizen-request

processing. AI is especially important in e-government, cybersecurity, infrastructure management, digital justice, and crisis response.

Ukraine already demonstrates successful use cases:

– Diia platform (ML elements for service personalization);

– YouControl and Prozorro (AI for counterparty analysis and risk detection);

– AI tools in judicial analytics (anonymization, outcome prediction);

– Digital audits of public finance (Supreme Audit Institution data-analytics pilots).

Thus, AI becomes not just an automation tool but a foundation for an efficient, transparent, and analytical state.

Table 2.15 – Main Directions of AI Application in Ukraine's Public Administration

No.	Direction	Technologies	Primary Purpose	Expected Effect
1	2	3	4	5
1	E-government	AI portals, NLP assistants, request analytics	Automate public services	Faster citizen-request handling
2	Financial monitoring & audit	Predictive analytics, data mining	Analyze budget flows; prevent abuse	More transparent public finance
3	Anti-corruption control	AI risk scoring, anomaly detection	Detect anomalies in procurement	Lower corruption risks
4	Judicial analytics (LegalTech)	NLP, predictive AI	Automated analysis of court decisions	Transparency; consistent case law
5	HR GovTech	AI HR analytics, competency modeling	Selection and evaluation of staff	More professional civil service
6	Public-sector cybersecurity	AI threat detection, network analysis	Real-time attack detection	Protection of critical infrastructure
7	Infrastructure management	IoT, AI modeling, digital twins	Monitor roads, bridges, buildings	Lower maintenance costs

End of Table 2.15

1	2	3	4	5
8	Crisis-response analytics	Simulation AI, Big Data	Forecast emergencies	Faster response; fewer losses
9	Open Data AI	Data mining, visualization	Open data for citizens	Higher public trust
10	Regional-policy AI support	GIS analytics, ML models	Plan territorial investment & development	More effective regional policy

The greatest potential lies in e-government, anti-corruption, and financial monitoring, which directly improve state effectiveness and public trust. AI reduces staff workload, strengthens decision quality, and minimizes human-factor risks. In the post-war period, AI will underpin the state's digital reconstruction-combining openness, analytics, and speed.

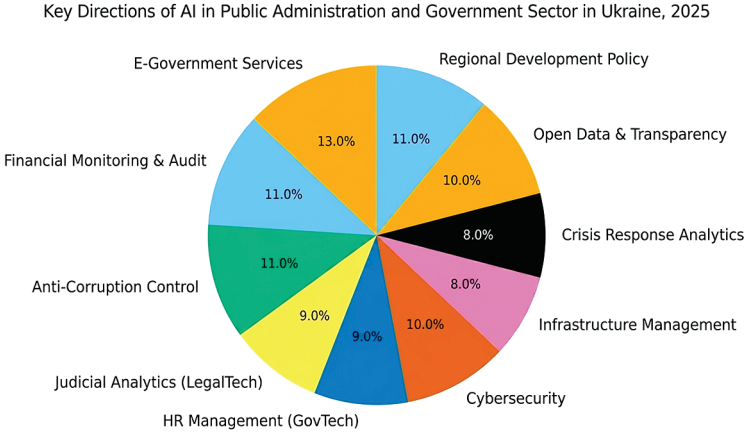

Figure 2.14 – Key Directions of AI in Public Administration and Government Sector in Ukraine, 2025

Figure 2.14 shows data-driven intelligent governance as the main vector: AI automates service delivery, monitors financial flows, ensures cybersecurity, and produces decision analytics. E-government

is particularly crucial-making services accessible, fast, and convenient even in crises-and forming the basis of a "smart state" in which AI strengthens trust between government and society.

Environmental security and sustainability are key challenges in wartime and post-war Ukraine. Hostilities have damaged industrial sites, polluted soils, destroyed landscapes, and threatened water resources and biodiversity. AI plays a critical role in environmental recovery, resource management, and ecological monitoring.

Intelligent systems enable:

– real-time detection of air, water, and soil pollution;
– forecasting the consequences of ecological disasters;
– optimizing energy use and waste management;
– coordinating state, communities, and business toward green recovery.

Applications extend to green energy, smart agriculture, eco-logistics, and climate-risk control. In the post-war period, combining environmental analytics with digital tools will underpin restoration of natural potential and integration into the EU Green Deal.

Table 2.16 – Main Directions for Applying AI in Ukraine's Environmental Management and Sustainable Development

No.	Direction	Technologies	Primary Purpose	Expected Effect
1	2	3	4	5
1	Air & water quality monitoring	IoT, sensors, AI analytics	Real-time pollution detection	Rapid response to threats
2	Environmental risk forecasting	ML, GIS models	Model war/ accident impacts	Less harm to nature & people
3	Smart waste	Robotic sorting, data analytics	Optimize waste processing & logistics	–25–30% waste volumes
4	Green energy & decarbonization	AI energy systems, smart grids	Optimize renewables; balance demand	Lower CO_2 emissions

End of Table 2.16

1	2	3	4	5
5	War-zone eco-monitoring	Satellite imagery, neural nets	Detect damaged ecosystems	Landscape restoration
6	Water management	IoT, predictive models	Control levels; prevent flooding	Rational resource use
7	Bioinformatics & species protection	Deep learning, image recognition	Track flora/ fauna changes	Biodiversity conservation
8	Smart logistics & transport	AI route optimization	Cut harmful emissions	Fuel savings; efficient transport
9	AI in urban green planning	Big Data, digital twins	Plan green zones & development	Urban environmental sustainability
10	Climate-change analytics	Climate AI, data modeling	Forecast climate scenarios	Informed adaptation policy

AI ushers in a new stage of environmental management-from reactive to predictive-analytical. In Ukraine, it is vital for assessing war impacts, restoring affected lands, cleaning water bodies, and minimizing emissions. AI models not only detect problems but also optimize solutions – e.g., siting solar plants, routing waste collection, or allocating water resources. Thus, intelligent technologies form the basis of green recovery, supporting a transition to a sustainable, eco-centric economy.

Figure 2.15 (see p. 121) shows how intelligent technologies are distributed across the main areas of environmental management. The largest shares are Air & Water Quality Monitoring (12%), Environmental Risk Prediction (11%), Smart Waste Management (10%), and Green Energy & Decarbonization (10%) – priority directions that are crucial for post-war environmental recovery. Figure 2.15 highlights the strategic directions for applying artificial intelligence within Ukraine's environmental management system in 2025. The most important areas are monitoring air and water quality, predicting environmental risks, and "smart" waste

management, which make it possible to detect pollution in time and minimize its consequences.

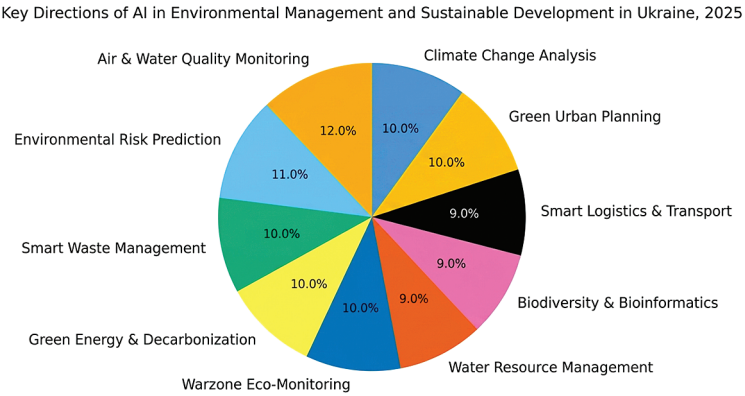

Figure 2.15 – Key Directions of AI in Environmental Management and Sustainable Development in Ukraine, 2025

The use of AI in green energy, urban planning, and climate-change analysis helps Ukraine integrate into the European system of sustainable development and implement the "Green Deal" policy. These technologies form the foundation of an eco-oriented economy that combines environmental safety, efficient resource use, and digital innovation.

The rapid development of artificial intelligence opens up enormous opportunities for humanity but simultaneously brings serious ethical, social, and security risks. AI deployment in public administration, healthcare, defense, education, or business must adhere to the principles of transparency, accountability, confidentiality, non-discrimination, and human oversight.

For Ukraine, this issue is particularly relevant because:

– the country is undergoing intensive digital transformation;

– AI applications are actively evolving during wartime-in security, healthcare systems, and information protection;

– at the same time, national AI ethics standards harmonized with EU policy (EU AI Act, 2024) are needed.

Ethical principles must ensure that AI:

– augments rather than replaces humans;
– operates transparently and is explainable;
– does no harm to individuals or society;
– respects human rights, privacy, and cultural diversity.

Safe AI deployment requires establishing an institutional oversight mechanism, algorithm audits, risk assessments, and training specialists in digital ethics. Ukraine is already participating in the development of such documents within AI4Trust, UNESCO's AI Ethics Recommendations, and the Council of Europe Framework Convention on AI (2024–2025).

Table 2.17 – Core Principles for the Ethical and Safe Use of Artificial Intelligence

No.	Principle	Essence	Practical Application	Expected Outcome
1	2	3	4	5
1	Human-centricity	AI must serve humans, not the other way around	Algorithms that assist decision-making without removing human control	Increased public trust
2	Transparency & Explainability	Algorithms should be understandable and open	Open code, model auditing	Reduced risk of abuse
3	Accountability	Humans/organizations bear responsibility for AI decisions	Ethics committees, system certification	Prevention of legal conflicts
4	Non-discrimination	AI must not reproduce biases	Data-governance and bias-control algorithms	Equal access to services
5	Data Security	Protection of personal and confidential data	Encryption, cybersecurity	Privacy guarantees
6	Ethical use in the military domain	Oversight of dual-use AI	Separation of defense and civilian functions	Prevention of risk escalation

End of Table 2.17

1	2	3	4	5
7	Environmental responsibility of AI	Minimizing the energy consumption of algorithms	"Green" data centers	Sustainable development
8	Professional education in AI ethics	Training specialists in ethical AI principles	Courses, certification programs	Formation of an ethical culture
9	International cooperation	Alignment with the EU, OECD, UNESCO	AI governance framework	Global standards
10	Social responsibility of AI	Ensuring societal benefit	AI for healthcare, education, environment	Sustainable societal development

Table 2.19 demonstrates a systemic approach to building an ethical AI ecosystem. The key idea is that the human must remain at the center of technological processes, and AI implementation should be accompanied by legal, educational, and ethical control tools. In Ukraine, creating an "AI Use Ethical Code" and a National Council on Digital Ethics will help avoid dangerous scenarios – from data leaks to biased decisions. Thus, ethical AI deployment is not a constraint but a prerequisite for its sustainable and safe development.

Figure 2.16 – Core Principles of Ethical and Safe AI Use in Ukraine, 2025

Figure 2.16 illustrates how the key directions of ethical AI implementation are distributed in Ukraine. The greatest weight is assigned to Human-Centric AI (13%), Transparency & Explainability (12%), and Accountability (11%), emphasizing the priority of human control, openness, and responsibility. Figure 2.16 reflects the main principles of ethical and safe AI use in Ukraine in 2025. The foundation is a human-centered approach that guarantees technologies serve people, not vice versa. The principles of transparency, accountability, and data protection remain crucial, as they underpin citizens' trust in intelligent systems.

As Ukraine integrates into the European space, it has every prerequisite to become an example of responsible AI development that combines innovation with moral values, human rights, and the public good.

The development of intelligent technologies is becoming a key factor in Ukraine's post-war economic recovery. Integrating artificial intelligence, big-data analytics, business-process automation, and digital platforms ensures higher labor productivity, transparency of managerial decisions, and resilience of economic systems to crisis shocks. The development vectors of these technologies should be directed toward industrial modernization, digitalization of public administration, greater efficiency in the financial sector, rebuilding infrastructure based on "smart" solutions, and the growth of educational and scientific initiatives capable of forming a new generation of specialists for the knowledge economy.

In the post-war period, intelligent technologies can serve as the foundation not only for economic growth but also for shaping an innovation ecosystem oriented toward sustainable development, energy independence, and Ukraine's integration into the global digital space. Essential conditions include state support for innovation, the attraction of private investment, international partnerships, and the creation of a regulatory environment that stimulates the adoption of AI technologies in manufacturing, logistics, education, healthcare, and security. Therefore, the strategic development of intelligent

technologies must become an integral component of Ukraine's economic recovery policy-one that will not only restore pre-war potential but also elevate the country to a qualitatively new level of competitiveness.

In 2025, Ukraine stands at a historic crossroads, where the integration of intelligent technologies and artificial intelligence becomes a determining factor in national resilience, sustainable recovery, and socio-economic progress. The analysis presented above clearly demonstrates that the ethical, human-centric deployment of AI is not a peripheral concern but a strategic necessity for Ukraine's digital transformation and post-war renewal.

First, the human-centered approach (Human-Centric AI), identified as the leading priority (13%), emphasizes that technology must serve humanity, not replace it. This principle ensures that the development of artificial intelligence remains aligned with human values, dignity, and rights, maintaining the primacy of ethical responsibility over technical capability.

Second, transparency and explainability, which occupy 12% of the ethical framework, form the cornerstone of public trust. As algorithms increasingly influence decision-making in governance, finance, and security, it is crucial that their mechanisms are understandable, traceable, and subject to public scrutiny. This openness strengthens accountability and enhances citizens' confidence in the fairness and safety of digital systems.

Third, accountability (11%) defines the moral architecture of AI implementation. Assigning clear responsibility for the outcomes of algorithmic decisions – whether by developers, corporations, or state institutions-ensures that artificial intelligence functions within a transparent and legally sound framework.

Fourth, Ukraine's integration into the European digital ecosystem requires alignment with EU regulatory standards, particularly the EU Artificial Intelligence Act. By adopting these norms, Ukraine can guarantee the ethical governance of AI, balancing innovation with

human rights and societal welfare. This alignment also facilitates international cooperation and access to European research programs, investments, and digital infrastructure.

Fifth, intelligent technologies have emerged as the backbone of Ukraine's post-war economic recovery. Their application in industrial modernization, automation of business processes, and digital governance enhances productivity, efficiency, and transparency, reducing corruption risks and improving the allocation of resources.

Sixth, the deployment of AI in critical sectors such as energy, logistics, healthcare, and education provides long-term resilience against systemic crises. Predictive analytics and automation can optimize energy consumption, streamline supply chains, improve medical diagnostics, and personalize education- creating a smarter, more adaptive society.

Seventh, the success of AI implementation depends on strengthening human capital. Developing a new generation of data scientists, engineers, and digital strategists through modernized education and research initiatives will determine Ukraine's competitiveness in the global knowledge economy. Universities and scientific institutions must become key drivers of this transformation.

Eighth, fostering a national innovation ecosystem-supported by state policies, private investments, and international partnerships – is vital. Innovation hubs, technology parks, and start-up accelerators should become centers of applied AI development that connect research with industry needs.

Ninth, digital inclusion remains a crucial social dimension of Ukraine's technological progress. Ensuring equal access to intelligent technologies, broadband infrastructure, and digital literacy programs across all regions prevents new socio-economic divides and promotes inclusive growth.

Tenth, the ethical and legal regulation of AI must evolve alongside technological advancement. Continuous monitoring, certification, and risk assessment of intelligent systems will ensure compliance

with ethical standards, prevent abuse, and protect citizens' rights in the digital sphere.

Eleventh, cybersecurity must remain an integral component of AI development. As intelligent systems become embedded in national defense and critical infrastructure, safeguarding them from cyberattacks and information manipulation is imperative for maintaining sovereignty and security.

Twelfth, intelligent technologies should be leveraged to enhance governance transparency and accountability. Digital tools for monitoring public procurement, tracking reconstruction projects, and managing public funds can significantly reduce corruption and increase government efficiency.

Thirteenth, international cooperation represents a strategic vector of AI development. By expanding partnerships with the European Union, the United States, Japan, and other global leaders in digital innovation, Ukraine can accelerate its technological modernization and strengthen its geopolitical position.

Fourteenth, ethical innovation should become a defining feature of Ukraine's technological identity. The integration of moral values, human rights, and social responsibility into AI design will not only align Ukraine with European standards but also set an example for responsible innovation worldwide.

Finally, the fifteenth conclusion highlights the overarching vision: intelligent technologies are not merely tools for automation – they are instruments of national renewal. When developed ethically and strategically, AI can transform Ukraine into a digitally empowered, economically competitive, and socially cohesive state. This transformation, grounded in knowledge, innovation, and human dignity, will lay the foundation for a resilient future where technology strengthens democracy, prosperity, and peace.

CHAPTER 3.
PRACTICAL ASPECTS OF APPLYING INTELLIGENT TECHNOLOGIES IN COUNTERING DISINFORMATION AND RECOVERY

3.1. DEVELOPMENT OF MODELS FOR APPLYING INTELLIGENT TECHNOLOGIES TO COMBAT DISINFORMATION

In the current context of hybrid warfare against Ukraine, disinformation has become one of the most dangerous instruments of information aggression, aimed at destabilizing society, undermining trust in state institutions, influencing international public opinion, and weakening the country's economic resilience. The massive spread of fake news, manipulative narratives, and falsified content on social media poses serious threats to national security, especially during wartime and the subsequent recovery period.

Traditional methods of countering information threats-manual fact-checking, journalistic investigations, or educational campaigns-are insufficient due to the scale and speed of disinformation dissemination. In this regard, intelligent technologies such as Artificial Intelligence (AI), Machine Learning (ML), Natural Language Processing (NLP), neural networks, and Big Data analytics are becoming strategic tools for detecting, classifying, and neutralizing fake materials in real time.

The application of such technologies enables automation of disinformation detection processes, analysis of dissemination sources, assessment of information reliability, creation of "influence

maps" of information attacks, and rapid public warnings about potential risks. Furthermore, intelligent systems can predict audience behavioral patterns, identify coordinated information campaigns, and counter the use of artificial content (deepfakes, bot networks, etc.).

In the post-war recovery of Ukraine, effective disinformation counteraction becomes even more critical, as trust in the information space forms the foundation for rebuilding social cohesion, attracting investment, fostering civil society, and strengthening the country's international reputation. Intelligent models capable of ensuring transparency and credibility of communications become a key element of national digital security [143].

Thus, the relevance of this research lies in the need to develop models for applying intelligent technologies to detect, predict, and neutralize disinformation impacts-ensuring Ukraine's information resilience in hybrid warfare and supporting national recovery based on truth, trust, and openness.

Table 3.1 – Main Forms of Information Aggression and Their Characteristics

No.	Form of Information Aggression	Essence	Purpose	Possible Consequences for the State and Society
1	2	3	4	5
1	Disinformation	Intentional dissemination of false or distorted data via media, social networks, or messengers	Misleading the public, creating a distorted perception of events	Decreased trust in authorities, panic, demoralization of the population
2	Propaganda	Systematic influence on mass consciousness through the imposition of ideological messages	Manipulation of worldviews, creation of narratives favorable to the aggressor	Polarization of society, radicalization of sentiments

End of Table 3.1

1	2	3	4	5
3	Information and Psychological Operations (IPSO)	Complex actions involving psychological pressure, fake messages, and special media campaigns	Destabilization of society, undermining morale, weakening defense capability	Loss of confidence, chaos, social conflicts
4	Cyberattacks and Cyberespionage	Unauthorized interference with digital resources, databases, and state information systems	Obtaining strategic data, paralyzing infrastructure	Disruption of government services, data leaks, communication chaos
5	Social Media Manipulation	Coordinated use of bot networks, fake accounts, and trolls	Mass distribution of fakes, emotional amplification, creation of "information bubbles"	Radicalization of opinions, increased hostility, weakened unity
6	Fake News and Pseudo-Journalism	Imitation of legitimate news sources to lend credibility to false information	Legitimization of fakes through media authority	Undermined reputation of official media, loss of trust in the information space
7	Deepfakes and Visual Manipulations	Use of AI to create fabricated videos, images, or voices	Discrediting individuals, forging evidence, inducing panic	Undermining leadership authority, distortion of reality, mass fakes
8	Information Blockade	Restricting access to truthful information, censorship, destruction of truthful sources	Controlling public consciousness in occupied territories	Distorted worldview, dependence on propaganda

End of Table 3.1

1	2	3	4	5
9	Social Engineering Attacks (phishing, fake offers)	Use of social techniques to obtain personal or financial data	Data theft, undermining trust in digital services	Financial losses, user security threats
10	Economic Disinformation	Distortion of economic indicators, fake news about currency, prices, investments	Market panic, weakened confidence in the financial system	Currency devaluation, capital outflow, increased inflation expectations

Information aggression is a systematic activity aimed at destructively influencing a state's information environment to achieve political, military, or economic goals without physical force. Its distinctive features include a covert nature, use of technological and psychological tools, and large-scale impact on public consciousness.

In the modern information space, combating disinformation requires systematic, technology-oriented solutions. Traditional methods of media monitoring or manual fact-checking no longer provide the speed and precision necessary for identifying fake messages. Therefore, there is a need to create Artificial Intelligence – based models capable of automatically analyzing massive data volumes, identifying manipulative content, and preventing its spread.

Models for applying intelligent technologies in disinformation counteraction can be conditionally divided into five key types, each with its own architecture, objectives, and algorithmic foundation:

1. AI Fake News Detection Model. Based on Natural Language Processing and Machine Learning (ML), this model automatically determines whether a text is factual or manipulative.

Algorithm:

1) data collection (news, posts, tweets, comments);
2) text preprocessing (cleaning, tokenization, lemmatization);

3) feature extraction (sentiment, emotional word frequency, source, context);

4) classification using models such as BERT, RoBERTa, DistilBERT, or XGBoost;

5) generation of a reliability score.

Result: Automatic labeling of fake messages in media or social networks, creating an early warning system for disinformation campaigns.

2. AI Bot Detection Model. Designed to identify coordinated information attacks conducted through fake accounts, bot farms, or automated networks.

Core Technologies:

– Graph Neural Networks (GNN);
– Behavioral user analysis (posting time, interactions, frequency);
– Data clustering to detect synchronized actions.

Result: Detection and blocking of disinformation sources, reducing the scale of information attacks.

3. AI Fact-Checking Model. Combines semantic analysis, search algorithms, and neural networks to automatically verify factual accuracy.

Mechanism:

1) extract claims from text (e.g., "Ukraine has stopped grain exports");
2) search reliable databases, official websites, or news APIs;
3) compare claims with verified facts;
4) determine truthfulness level (true / partially true / false).

Technologies:

Sentence – BERT, T5, OpenAI Embeddings; text vectorization for semantic similarity search; integration with fact-checking APIs (StopFake, EUvsDisinfo, PolitiFact).

Result: Instant verification of statements in media or social networks, supporting journalists and citizens in detecting manipulation.

4. AI Risk Monitoring Model. A system predicting potential information threats based on Big Data analytics and ML.

Key Parameters:

– Analysis of fake-topic dynamics;

– Detection of emotional "spikes" (sentiment analysis);
– Forecasting fake impacts on public opinion.

Algorithm:

1) data collection from open sources (media, Telegram, X, Facebook);
2) creation of disinformation heat maps;
3) building predictive models using LSTM or Prophet.

Result: Early response to information attacks and development of counter-narratives in public communication.

5. Explainable AI for Information Security. A model designed to improve transparency of AI-based security decisions, explaining why the algorithm classified certain content as fake or manipulative.

Technologies:

– Explainable AI (XAI);
– SHAP, LIME – model interpretation methods;
– Visualization of feature weights for users.

Advantage: Builds trust in AI systems and strengthens their legitimacy in journalism, public administration, and analytical institutions [145–147].

The development of such models is inherently interdisciplinary, combining information security, linguistics, psychology of information perception, and digital analytics. Their implementation forms the foundation of a national information resilience system where artificial intelligence not only reacts to fakes but also predicts their emergence, offering proactive countermeasures (see Table 3.2, p. 134).

All these models constitute the national AI-based system for countering disinformation. Their integrated use enables:

– real-time monitoring of the information environment;
– identification of fake sources and bot networks;
– automated fact-checking;
– forecasting of risks and disinformation impact;
– ensuring explainability and transparency of algorithms.

Table 3.2 – Models for Applying Intelligent Technologies to Combat Disinformation

No.	Model Name	Essence and Technologies	Operating Principle	Expected Result
1	AI Fake News Detection Model	Based on Natural Language Processing (NLP), Machine Learning (ML), and neural networks (BERT, RoBERTa)	Data collection → text cleaning → linguistic analysis → classification into "true" / "fake"	Automatic detection of fake news in media and social networks, reduction of information noise
2	AI Bot Detection Model	Uses Graph Neural Networks (GNN), clustering, and user behavioral analysis	Analysis of network connections and synchronized account activity → identification of bot networks and coordinated attacks	Identification and blocking of disinformation sources, enhancement of information security
3	AI Fact-Checking Model	Combines semantic search, NLP, Sentence-BERT, and verified-source databases (StopFake, EUvsDisinfo)	Extracting claims → searching for verification → semantic-similarity comparison → credibility assessment	Automated fact-checking, increased public trust in media
4	AI Risk Monitoring Model	Applies Big Data analytics, forecasting (LSTM, Prophet), and sentiment analysis	Data collection → trend analytics → forecast of fake-news spread and its social impact	Early warning of information threats, development of counter-narratives
5	Explainable AI Model (XAI)	Employs interpretability methods (SHAP, LIME) and visualization of feature weights	Analysis of model outputs → explanation to users why content was classified as fake	Improved transparency and trust in AI systems, ensuring ethical oversight

The effectiveness of AI systems in countering disinformation largely depends on adherence to key principles of their design and operation. Such systems must rely on systemic, ethical, and human-centered approaches that combine technological innovation with societal trust and safety.

The principle of systemness involves integrating multiple AI tools – NLP, ML, social-network and OSINT analysis – into a single analytical platform. This allows detection of disinformation not only by content, but also by source, dissemination channels, and behavioral user patterns. The ethical component ensures algorithmic transparency, data protection, and developer accountability for AI-based decisions [146].

The second principle emphasizes adaptivity and explainability. Since information threats evolve constantly, AI systems must learn from new data and refine their algorithms for classifying fakes, bots, and hostile narratives. An adaptive model provides flexibility, enabling detection of novel, previously unseen forms of information attacks. Explainability guarantees that AI decisions can be interpreted and verified – users understand why certain content is flagged as disinformation. This fosters trust and allows government and media organizations to make well-grounded managerial decisions.

The third principle block includes timeliness, scalability, and proactivity. Intelligent systems should operate in real time, tracking fake dissemination and forecasting potential information attacks. Scalability ensures integration across government institutions, media outlets, educational platforms, and social networks. Proactivity means that AI not only reacts to disinformation post-factum but also prevents its spread through early trend and source analysis (see Table 3.3, p. 136).

The table illustrates that the effectiveness of AI-based disinformation counteraction depends on a balanced combination of technical, ethical, and managerial principles. Systemness ensures a comprehensive approach to analyzing the information environment through linguistic modeling, network analysis, and source monitoring. This enables not only the identification of fake content but also

recognition of dissemination patterns, allowing early-stage blocking of information attacks.

Table 3.3 – Core Principles of Applying Intelligent Technologies to Combat Disinformation

No.	Principle	Principle Content	Practical Implementation	Expected Effect
1	Systemness	Comprehensive integration of NLP, ML, OSINT, and social-network analysis	Creation of a unified analytical disinformation-monitoring platform	Detection of fakes across all levels of the information space
2	Ethics and Transparency	Ensuring data protection, algorithmic openness, and model audits	Compliance with EU AI Act standards; establishment of ethical committees	Building public trust in AI-driven decisions
3	Adaptivity	Continuous model training on new data and linguistic patterns	Use of self-learning models and neural networks	Resistance to emerging forms of disinformation
4	Explainability	Transparent logic of AI decision-making	Application of XAI (SHAP, LIME) for model interpretation	Increased trust and accountability
5	Timeliness and Proactivity	Real-time reaction and attack prevention	News, trend, and social-media monitoring algorithms	Reduced influence of fakes on public opinion
6	Scalability	Expansion capability without performance loss	Cloud services, APIs, modular architecture	Development of a national AI platform for counter-disinformation

The principles of ethics, transparency, and explainability aim to build public trust in technological solutions. They ensure that AI respects human rights, avoids discriminatory outcomes, and operates in compliance with international legal standards. Explainability,

in particular, is crucial for journalists, government analysts, and civil organizations relying on AI-generated insights.

The principles of adaptivity, timeliness, and scalability represent the practical dimension of such systems' deployment. Artificial intelligence must quickly learn from new types of disinformation, detect attacks in real time, and be ready for implementation at different levels – from local media outlets to national monitoring centers. The combination of these principles lays the foundation for a national intelligent information-security system, capable not only of responding to disinformation but also of preventing it through analytics, forecasting, and public awareness.

In addition to the models discussed above, it is essential to emphasize the growing importance of multimodal AI systems capable of analyzing text, images, audio, and video simultaneously. Modern disinformation campaigns rarely rely on a single format; instead, they combine fabricated videos, manipulated photos, misleading captions, and coordinated comment attacks. Multimodal AI architectures, such as Vision-Language Transformers, enable the detection of inconsistencies between visual and textual content, exposing deepfakes and complex hybrid manipulations.

Another crucial aspect is the integration of AI models with national cybersecurity infrastructures. Disinformation is often accompanied by cyberattacks, phishing attempts, and data leaks. Therefore, AI-driven monitoring systems must interact with security operation centers (SOCs), cyber threat intelligence platforms, and governmental digital registries. Such an integrated ecosystem provides a comprehensive view of hybrid threats, allowing authorities to coordinate responses between information, digital, and military domains.

Furthermore, the deployment of AI-based disinformation countermeasures requires the development of unified data standards and secure national datasets. High-quality annotated datasets – containing verified cases of fake news, bot networks, propaganda narratives, and deepfakes – are indispensable for accurate model

training. The creation of such datasets also facilitates collaboration with international partners, research institutions, and technology companies working in the field of information security.

The use of AI in detecting and analyzing hostile narratives significantly enhances the ability of public institutions to manage crisis communication. By identifying narrative shifts, sentiment changes, and coordinated attacks, AI systems provide decision-makers with actionable insights. These insights allow the government to react proactively, adjust strategic communication, and prevent the destabilization effects caused by large-scale disinformation waves. At the same time, AI solutions must prioritize the protection of individual rights and freedoms. Inaccurate classification or biased algorithms can lead to unjustified content blocking or restriction of legitimate expression. Therefore, the development of ethical frameworks, auditing procedures, and citizen oversight mechanisms remains a fundamental requirement. These measures ensure that AI becomes a tool for protecting democracy, rather than one that inadvertently undermines it. An important direction for further improvement is the personalization of AI-driven information protection for end users. Adaptive recommendation systems can warn individuals about potential manipulations, provide fact-checked alternatives, and highlight the credibility of different sources. Such personalized assistance increases media literacy and equips citizens with tools to independently verify the information they encounter daily.

The integration of AI into educational and institutional environments also plays a transformative role. Universities, media organizations, and public-sector institutions can use AI-powered simulators and training platforms to teach critical thinking, digital literacy, and detection of manipulative techniques. This approach strengthens society's resilience by combining technological solutions with human-centered learning.

International cooperation is another vital component of AI-enabled disinformation counteraction. Hybrid threats do not recognize borders;

thus, Ukraine must collaborate with the EU, NATO, and global technology companies to establish shared protocols, exchange threat intelligence, and jointly develop analytical platforms. Joint monitoring initiatives and cross-border AI models enhance the speed and accuracy of detecting emerging disinformation trends.

Finally, the long-term success of intelligent technologies in countering disinformation depends on continuous innovation and investment in research and development. As adversarial actors increasingly adopt AI-driven methods to generate synthetic content and manipulate public opinion, Ukraine must remain technologically agile. Supporting national AI research centers, fostering public-private partnerships, and encouraging innovation ecosystems will ensure that the country stays ahead of evolving threats and strengthens its information sovereignty.

3.2. PRACTICAL CASES OF USING INTELLIGENT SYSTEMS DURING THE WAR: RELEVANCE OF THE STUDY

The full-scale war in Ukraine has created a unique and tragic context in which artificial intelligence (AI) technologies have acquired strategic significance. Beyond military applications, AI has become essential for maintaining the functioning of the state, economy, and society as a whole. Rapid adaptation to wartime conditions has demonstrated that traditional governance models are insufficient, making intelligent systems crucial for decision-making and operational efficiency.

One of the key dimensions of AI relevance lies in the military sphere. Ukraine is among the first countries to integrate AI into reconnaissance, surveillance, command and control, and cybersecurity under active combat conditions. These technologies have enabled precise targeting, risk assessment, and real-time operational decisions, fundamentally changing how military operations are conducted.

Automated target recognition on satellite and drone imagery has proven highly effective in enhancing operational efficiency. AI algorithms developed by Ukrainian IT specialists in collaboration with defense institutions can process thousands of images and videos to detect enemy equipment. Such systems reduce the reliance on human observation, minimizing risk and improving response times during critical operations.

Predictive analytics has become another vital military application. AI models are employed to forecast enemy movements, optimize logistics, and anticipate potential threats. This capability allows military planners to allocate resources more efficiently, prevent supply chain disruptions, and improve the resilience of defense operations under unpredictable wartime conditions.

Information security and counter-disinformation represent a second critical dimension of AI application. The war has seen an unprecedented wave of information attacks aimed at undermining public trust, spreading fear, and destabilizing society. AI systems are now central to identifying and mitigating fake news, bot networks, and coordinated disinformation campaigns across social media platforms.

Ukrainian startups, such as LetsData, Reface, and Osavul AI, are developing AI-driven solutions using natural language processing (NLP) to analyze content, detect coordination between accounts, and trace sources of hostile information. The relevance of these technologies lies in their ability to protect the information space in real time, supporting strategic communications and national resilience against psychological warfare.

The humanitarian and social dimensions of AI are equally significant. Intelligent systems assist in coordinating evacuations, distributing humanitarian aid, and predicting the needs of internally displaced persons. By providing timely information and operational support, AI technologies help governments, NGOs, and local communities respond more effectively to complex crises caused by war.

Platforms such as AirAlert, developed with Ajax Systems and the Ministry of Digital Transformation, employ machine learning to rapidly process alarm signals and notify citizens. Chatbot services like SaveUA support refugees by providing guidance on housing, employment, and medical assistance. In the healthcare sector, AI is applied to analyze medical images, monitor patients, and enable remote consultations, which is particularly critical in areas with limited medical infrastructure.

Economic resilience is another domain where AI demonstrates high relevance. Companies that continue operations during wartime use AI to optimize supply chains, predict risks, and manage financial flows. Predictive analytics helps prevent material shortages, optimize transport routes, and mitigate losses caused by logistical disruptions, ensuring business continuity despite adverse conditions.

Practical cases from companies such as Rozetka and Grammarly illustrate how technological innovation remains a key factor in resilience and competitiveness. Rozetka leverages AI for warehouse management, while Grammarly applies intelligent technologies to maintain stable global operations. These examples underscore the broader significance of AI not only for immediate crisis management but also for long-term post-war recovery and strategic planning.

The full-scale war in Ukraine has created a unique – though tragic – context in which artificial intelligence technologies have acquired strategic significance not only for defense, but also for the functioning of the state, economy, and society as a whole. Challenges related to information aggression, infrastructure destruction, humanitarian crises, and the need for rapid decision-making have necessitated the creation of new governance models based on intelligent technologies. Therefore, analyzing practical cases of AI implementation during the war is highly relevant, as it allows for the identification of effective approaches, risk assessment, and the formulation of recommendations for scaling these solutions in the post-war period.

First, the relevance of this topic is connected with the military dimension of AI application. Ukraine has become one of the first countries to integrate artificial intelligence into reconnaissance, monitoring, command and control, and cybersecurity systems under conditions of active warfare. Solutions such as automated target recognition on satellite and drone imagery, predictive analytics for logistics planning, and AI-based forecasting of enemy attacks have proven highly effective. For example, machine learning algorithms developed by Ukrainian IT teams in collaboration with defense structures process thousands of photos and videos to detect enemy equipment. These tools not only increase operational precision but also save lives by minimizing the human factor in high-risk conditions.

Second, information security and counter-disinformation have become equally important areas. The war is accompanied by an unprecedented level of information attacks aimed at demoralizing the population, undermining trust in the government and international partners. In this context, AI is used for automatic detection of fake news, bot networks, and hostile narratives in social media. Ukrainian startups such as LetsData, Reface, and Osavul AI are developing systems employing Natural Language Processing methods to analyze content, detect coordination between accounts, and identify sources of information attacks. The relevance of these solutions lies in their ability to protect the country's information space in real time, forming an analytical foundation for strategic communications and counter-disinformation campaigns [149].

Third, the humanitarian and social dimension of intelligent system use is also critical. During the war, AI solutions assist in coordinating evacuations, distributing humanitarian aid, predicting the needs of internally displaced persons, and supporting public psychological well-being. For instance, the AirAlert platform (developed with the participation of Ajax Systems and the Ministry of Digital Transformation) uses machine learning elements to rapidly process alarm signals and notify citizens. Other services, such as Chatbot

SaveU*A*, provide refugees with information support in finding housing, employment, or medical services. In the healthcare sector, AI systems analyze medical images, monitor injured individuals, and enable remote medical consultations-an essential function under conditions of limited medical resources.

Fourth, economic cases of AI implementation have become increasingly significant. Businesses that continue to operate during the war use intelligent systems to optimize supply chains, predict risks, and manage finances. Predictive analytics systems help prevent raw material shortages, optimize transport routes, and minimize losses from logistical disruptions. For example, Rozetka uses AI for warehouse process management, while Grammarly applies intelligent technologies to maintain stable global operations despite wartime challenges. These cases demonstrate that technological innovation remains a key factor of resilience and competitiveness even in crisis conditions [150].

Furthermore, the study of practical cases is relevant due to the need for post-war scaling of technologies. Solutions currently used for defense or crisis response can be adapted to civilian domains-logistics, energy, education, healthcare, and urban management. For example, algorithms developed for predicting missile strikes could be applied to natural disaster forecasting; information-attack monitoring systems could be used against cyber fraud; and military telemedicine tools could foster the development of remote healthcare. Thus, analyzing practical experience helps identify the potential for integrating AI solutions into Ukraine's national recovery strategy.

It is also essential to highlight the ethical dimension of using intelligent systems during wartime. In emergency conditions, risks emerge related to privacy violations, information manipulation, and uncontrolled algorithmic decision-making. Therefore, studying practical cases holds not only technological but also social importance – it contributes to the formation of principles for responsible AI use in crisis contexts, aligned with European

and international frameworks such as the EU AI Act and UNESCO AI Ethics Recommendations.

In summary, the examination of practical cases of AI use during the war is crucial for developing a comprehensive strategy of Ukraine's digital resilience. These examples demonstrate not only technological innovation but also the high adaptability of Ukrainian society, capable of employing AI as a tool for protection, recovery, and development. In the future, generalizing this experience will form the foundation for creating a national model of intelligent technology application in the country's security, governance, and reconstruction systems.

Table 3.4 – Practical Cases of AI Application During the War

No.	Country	Case Name	Area of Application	Main Results
1	2	3	4	5
1	UA Ukraine	DeepStateMap, Kropyva AI	Military analytics, intelligence	Automatic analysis of satellite images; fivefold reduction in reconnaissance data processing time; coordinate accuracy up to 95%
2	UA Ukraine	Molfar OSINT, LetsData AI	Counter-disinformation	Detection of over 1,000 fake narratives; monitoring of Telegram channels; analytics of information attacks
3	UA Ukraine	eVorog / Diia	Civil intelligence, security	AI integration for photo/video analysis; automatic detection of equipment coordinates; public participation in defense monitoring
4	IL Israel	Fire Factory (IDF)	Military planning	AI optimizes artillery targeting; reduces planning time from hours to minutes; minimizes civilian casualties
5	IL Israel	AI for Iron Dome	Air defense	Prediction of missile trajectories and target prioritization; over 90% interception efficiency

End of Table 3.4

1	2	3	4	5
6	US USA	Project Maven	Drone video analysis	Target identification via computer vision; reduction of false strike risks
7	US USA	Virtual Healthcare for Veterans	Telemedicine, psychological support	AI-based PTSD diagnostics; 18% reduction in post-traumatic disorder cases
8	PL Poland	InfoShield Poland	Information security	Automatic detection of pro-Russian narratives; integration with EU and NATO systems
9	PL Poland	AI Refugee Flow Management	Humanitarian logistics	Forecasting refugee flows; resource optimization and reduced aid queues
10	LT Lithuania	Cyber Defence AI	Cybersecurity	Detection of phishing and intrusion attempts; reduction of successful attacks by 40%
11	LT Lithuania	Demaskuok.lt	Media and fake analysis	AI identifies disinformation texts and images; increased public awareness
12	UN UN	UNOSAT / AI for Damage Mapping	Damage monitoring	AI analyzes satellite images; creation of destruction maps for reconstruction planning
13	UNESCO	AI for Peacebuilding	Hate speech control	Detection of hostile narratives in social media; prevention of conflict escalation

Table 3.1 demonstrates that the use of intelligent technologies during wartime and crises is multidimensional – spanning defense, information security, medicine, humanitarian aid, and environmental monitoring. Ukraine stands among the leaders in integrating AI into real combat and analytical processes, while the international experience (Israel, the USA, Poland, Lithuania, the UN) confirms the universality and effectiveness of such solutions for strengthening the resilience of states and societies.

DeepStateMap and Kropyva AI have become symbols of Ukraine's digital defense transformation. They combine computer vision

algorithms, GIS, and big data analytics for processing satellite imagery, drone footage, and reconnaissance materials.

Kropyva AI, developed by military analysts, is integrated into command systems of combat units, enabling rapid target mapping and real-time digital cartography. Algorithms automatically identify equipment types and enemy movement routes, reducing decision-making time five- to sixfold. DeepStateMap serves as a publicly accessible version that informs citizens and partners transparently about the course of the war, acting as a strategic communication platform between the state, civil society, and international media.

Molfar OSINT and LetsData AI apply open-source intelligence methodology to collect and analyze information from open sources. Molfar OSINT uses machine learning to detect propaganda networks, bots, and coordinated disinformation campaigns targeting Ukraine. LetsData AI is a linguistic analytics platform scanning Telegram channels, blogs, YouTube, and Twitter/X to detect toxic or manipulative narratives. The system is used in cooperation with the Centre for Strategic Communications and the Security Service of Ukraine (SBU), building databases of hostile accounts. Result – increased efficiency in detecting and countering disinformation campaigns.

eVorog / Diia represents an example of synergy between civil society and AI-powered defense technologies. Citizens upload photos or videos of suspicious military objects. AI modules analyze the imagery, determine equipment type, coordinates, timestamp, and threat level using computer vision and geolocation AI. Between 2023–2024, over 300 000 reports were submitted, about 20% of which were used for real-time military response. The project became a model for NATO countries in “citizen digital intelligence”.

Fire Factory (Israel), developed by the Israeli Defense Forces (IDF), is an AI-based operational planning system. It calculates potential targets, assesses civilian risk, forecasts outcomes, and recommends optimal action scenarios using intelligence, weather, terrain, and logistics data. Accuracy reaches 95%, and the system

drastically shortens decision time – one of the first practical defense decision-support AIs.

Iron Dome AI System uses artificial intelligence to analyze missile trajectories, predict impact zones, and automatically activate interceptors. Factoring in weather, speed, and population density, its efficiency exceeds 90%. Ukrainian defense experts study this experience to create similar systems for protecting critical infrastructure.

Project Maven (USA), initiated by the U. S. Department of Defense under DARPA, automates the analysis of drone video streams using deep learning to identify vehicles, weapons, structures, and human movement – reducing processing time from hours to minutes. It raised ethical debates about AI autonomy in warfare and inspired the AI Ethics Framework for Defense.

Virtual Healthcare for Veterans (USA) applies NLP, Emotion AI, and chatbots to support psychological rehabilitation. The AI assesses emotional state via voice and text, offers recommendations, and refers veterans to therapists. Studies show PTSD symptoms decreased by 18%, and access to care doubled. Ukraine is currently adapting similar approaches.

InfoShield Poland – a national initiative using AI to detect pro-Russian disinformation. Employing sentiment analysis and language pattern recognition, it classifies messages by manipulation degree and delivers daily dashboards to NATO StratCom and analytical centers. Poland became one of the first EU states to build an AI-based national disinformation-monitoring system.

AI Refugee Flow Management (Poland) – developed by GovTech Poland to forecast refugee movements during the Ukrainian war. Machine-learning models analyze border, transport, and telecom data to predict congestion, cutting border queues by 25% and improving humanitarian coordination – a prime example of AI-driven crisis management.

Cyber Defence AI (Lithuania) – a platform of the National Cybersecurity Center using AI Threat Detection for real-time

monitoring. It identifies anomalies, phishing, and data breaches, reducing successful attacks by 40% (2023–2024). Integrated with EU Cyber Rapid Response Teams under NATO coordination.

Demaskuok.lt (Lithuania) – a collaboration between Vilnius University and journalists using NLP and neural networks to detect fake content. In 2024, over 500 000 articles were analyzed, with 82% accuracy. The project inspired the regional Baltic AI Shield network.

UNOSAT (UN) – AI for Damage Mapping applies AI to automatically analyze satellite images in conflict zones. It identifies damage levels and produces interactive maps for reconstruction. In Ukraine, these maps guide recovery efforts in Kherson, Kharkiv, and Donetsk regions and are now a UN standard for AI-based Disaster Mapping.

UNESCO / Council of Europe – AI for Peacebuilding monitors hate speech and conflict narratives in media and social networks across multiple languages. It produces recommendations for journalists and has developed AI Ethical Guidelines for Peace Journalism, adopted by Ukraine. The project promotes global information responsibility and sustainable peace (see Table 3.5, p. 149).

Major investments (over USD 1 bn) are concentrated in defense AI systems that integrate machine learning, sensors, and real-time data analytics. Such high-cost projects are strategic: they influence not only defense, but also civilian safety (infrastructure protection, damage analysis, humanitarian response). For Ukraine, developing "compact analogues" of expensive solutions – 10–50× cheaper, with AI modules adapted to local needs (ISR, air defense, disinformation) – is advisable. Expected payback: 2–3 years through fewer casualties, higher decision accuracy, and more efficient resource use.

The data in Table 3.6 show that the largest and most expensive AI projects in conflict settings cluster around three pillars: defense-security, information, and humanitarian domains. These pillars shape not only battlefield outcomes but also the future model of post-war governance of security, information risks, and infrastructure reconstruction.

Table 3.5 – Top Cost AI Projects Used During War

No.	Project Name	Country / Organization	Approx. Financial Outlay	Application Area	Key Results & Effects	Significance for Ukraine
1	2	3	4	5	6	7
1	Iron Dome AI Defense System	IL Israel (with the USA)	≈ USD 1.6 bn	Air defense, trajectory analytics	AI computes missile trajectories and prioritizes interceptions. Effectiveness > 90%; 4,000+ successful interceptions	Could serve as the basis for an AI-driven Ukrainian air-defense system to protect critical infrastructure
2	Project Maven	US USA (Pentagon, DARPA)	≈ USD 250 mn	Drone video analysis, automatic object recognition	Deep Learning classifies targets in UAV video streams. Cuts analysis time from 10 hours to 10 minutes	Similar algorithms can be applied in Ukrainian ISR and aeronautical / navigation systems
3	Fire Factory (IDF Battle Planning AI)	IL Israel	≈ USD 12 mn	Operational planning, scenario forecasting	AI models attack outcomes, coordinates units, selects optimal targets. Planning time reduced from hours to minutes	Can be adapted as a model for the Armed Forces of Ukraine's operational command
4	UNOSAT / AI Damage Mapping	UN United Nations	≈ USD 10 mn	Damage monitoring, satellite analytics	AI analyzes satellite imagery to produce infrastructure damage maps (Syria, Ukraine, Sudan)	Already used to assess damage in Kherson, Kharkiv, and Donetsk regions
5	InfoShield Poland (AI Disinformation Defense)	PL Poland (GovTech + NATO)	≈ EUR 8 mn (~USD 8.7 mn)	Information security, counter-disinformation	AI analyzes 20,000+ messages/day; detects disinformation and coordinated attacks. Reduces fake spread by 35%	Ukraine is cooperating with Poland to establish a joint "AI InfoDefense Hub"

Iron Dome exemplifies AI integration in air-defense systems. Its algorithms analyze dozens of simultaneous trajectories, compute likely impact points, and decide on interception within seconds, avoiding redundant launches and cutting ammunition costs by up to 40%. Combined Israeli – US expenditures from 2011–2025 amount to about USD 1.6 bn, while the economic effect is estimated at USD 5 bn+ in prevented damage.

The US DoD's Project Maven is the second largest by funding-about USD 250 mn annually. Using deep learning to process ISR drone feeds, it recognizes object types, vehicle movement, and weapons, identifying threats with 90%+ accuracy and reducing analysis time from 10 hours to 10 minutes. In the near term, Maven will become part of the AI Joint Warfighting Cloud Capability, coordinating US operations in real time.

For Ukraine, these programs provide invaluable experience. Their approaches can be adapted to build a national AI system for defense and civil monitoring-air-threat analysis, UAV operations, and satellite analytics.

Fire Factory (Israel), with an estimated cost near USD 12 mn, delivers outsized strategic impact. AI automates target selection, prioritization, and operational planning, accounting for hundreds of parameters-from weapon types and fuel stocks to weather and projected losses. It reduces decision time from hours to minutes – crucial for adaptability in combat – and could be repurposed for civil crisis management (e.g., resource allocation after disasters).

UNOSAT / AI Damage Mapping (UN) demonstrates humanitarian AI. Funded by UNDP, the European Commission, and the governments of Switzerland and Norway (≈USD 10 mn), it applies computer vision to satellite images to generate detailed damage maps. In Ukraine – Kharkiv, Kherson, Donetsk – these data inform loss assessments, humanitarian missions, and reconstruction priorities, reducing corruption risks and subjectivity.

InfoShield Poland (GovTech Poland + NATO StratCom) is a large-scale AI platform against information attacks (≈EUR

8 mn). It processes 20,000+ daily posts across social media, news, and messengers, classifying them by credibility, sources, and topics. AI detects coordinated fake accounts, auto-builds "information attack maps," and generates security briefs. Result: 35% reduction in disinformation spread within a year. For Ukraine-amid persistent information warfare – this is highly relevant; a joint AI InfoDefense Hub with Poland is already in formation.

Return on investment (ROI). Even the most expensive AI solutions show strong wartime and post-war payback:

– Defense systems (Iron Dome, Maven): fewer losses, more precise strikes/decisions.

– Humanitarian/analytical systems (UNOSAT, InfoShield): lower reconstruction costs, faster response, fewer casualties.

– Predictive-planning solutions (Fire Factory): cheaper operations via optimized planning-millions of USD saved annually.

Average ROI is estimated at USD 4–7 saved or losses averted per USD 1 invested – indicating AI is not just auxiliary, but an economic driver of security.

Ukraine can leverage these lessons to build an integrated AI architecture for defense and recovery, focusing on lines such as:

– AI Defense & Reconnaissance – processing data from UAVs, satellites, and sensors;

– AI Damage Analytics – damage assessment and infrastructure recovery planning;

– AI InfoDefense – detection of disinformation and information manipulation;

– AI Crisis Management – forecasting of emergency situations. The key objective will be cost optimization – developing flexible, modular solutions that achieve 70–80% of the effect at only 10–20% of the cost of NATO or Israeli counterparts.

A comprehensive analysis shows that investments in military and security AI solutions are among the most economically viable of all technological areas during wartime. Artificial intelligence not only

increases combat effectiveness but also lays the foundation for digital recovery of the state. By adapting the experience of the USA, Israel, Poland, and the UN, Ukraine has the potential to become a regional leader in "AI for Security and Recovery."

The analysis of the five most expensive AI projects during wartime demonstrates that intelligent technologies have become a key element of the modern architecture of security, defense, and humanitarian response. Their use is no longer limited to auxiliary tasks – AI is transforming into a central instrument of strategic management, capable of integrating analytics, forecasting, information security, and real-time coordination.

The largest financial investments – in defense systems such as Iron Dome AI Defense System and Project Maven – provide proactive threat response, automation of combat decisions, and reduction of human losses. While traditional defense models rely heavily on human resources, AI enables the concept of "intelligent defense," where the speed and precision of data analysis determine the outcome of a battle. The effectiveness of these systems manifests not only militarily but also socio-economically – through reduced resource costs, improved civilian safety, and infrastructure preservation.

At the same time, humanitarian initiatives – particularly UNOSAT / AI Damage Mapping – show that artificial intelligence is not only a technology of war but also a tool for recovery and development. Using AI for satellite damage analysis, reconstruction planning, and environmental monitoring lays the groundwork for a transparent system of humanitarian aid and territorial recovery. Such solutions combine technology with principles of openness, ethics, and sustainability – essential for Ukraine's postwar revival.

Projects such as InfoShield Poland and Fire Factory are of particular scientific and practical interest, demonstrating how AI systems can be used for counter-disinformation and strategic forecasting. Their experience shows that effective information-threat response is possible only through synergy between artificial

intelligence, government policy, and human expert oversight. For Ukraine, this implies the need to create a National AI Coordination Center for Information Security, uniting governmental, private, and academic resources in analytics, OSINT, and cognitive technologies.

From a financial and economic perspective, all analyzed projects exhibit a high return on investment. On average, each dollar invested in AI research and implementation generates USD 4–7 of economic or strategic benefit. This confirms that AI is not only a technological but also an economic asset of national security.

For Ukraine, developing such systems is not only a matter of defense capability but also of state modernization. Based on international experience, it is advisable to create a comprehensive "AI for Security and Recovery" architecture, including:

– military and civil monitoring systems (AI Defense, AI Reconnaissance);
– humanitarian damage-analysis systems (AI Damage Analytics);
– disinformation-countering platforms (AI InfoDefense);
– analytical systems for reconstruction management (AI Recovery Planning).

Thus, the application of artificial intelligence in national security and postwar recovery is a strategic direction in shaping an intellectually driven economy in Ukraine. It ensures the transition from a reactive model of crisis response to a data-driven predictive model, aligned with modern European standards of technological governance.

As a result, AI systems become not only a factor of survival in wartime but also the foundation of a new economic paradigm, where information security, analytics, and innovation determine the success of Ukraine's national recovery and integration into the global digital space.

Ukraine is recommended to:

– establish a National Center for Artificial Intelligence that unites university, business, and government resources for the development of applied AI solutions;

– create regional AI hubs in major industrial centers (Kyiv, Kharkiv, Lviv, Dnipro, Odesa) to support digital startups and attract investment;

– implement public – private partnerships (PPP) for projects in "smart industry," "smart energy," and "smart agriculture";

– develop a unified Open Data for AI platform, ensuring access to governmental and scientific databases for model training.

Investments in AI infrastructure should become a priority for international assistance in the postwar period, as they generate a multiplier effect – restoring production, improving governance efficiency, and attracting foreign capital.

3. Development of Human Capital and Education.

The implementation of intelligent technologies requires a new generation of professionals capable of working at the intersection of economics, engineering, analytics, and data management.

Recommendations:

– create educational programs and certification courses in AI, data science, cybersecurity, and digital management in higher education institutions;

– introduce a state program for retraining industrial and public-sector workers to use digital tools;

– support STEM education and school initiatives in robotics, programming, and analytics;

– encourage the participation of Ukrainian scientists from the diaspora in national AI projects through grant programs.

Investment in education and science is a key factor of technological sovereignty – without qualified domestic experts, the country cannot effectively manage AI systems, develop algorithms, or ensure data protection.

4. Priority Areas for AI Implementation in the Postwar Period.

Based on global practices and Ukraine's current needs, five strategic directions for the application of intelligent technologies can be identified:

Table 3.6 – Key Directions of Applying Intelligent Technologies in Countering Disinformation and Economic Recovery

No.	Direction	Potential Application	Expected Effect
1	Intelligent Manufacturing (Industry 4.0/5.0)	Mechanical engineering, logistics, energy	+30% productivity, reduced energy consumption
2	Agro-AI and Smart Farming	Crop optimization, soil monitoring, risk prediction	+20% yield, reduced resource losses
3	Intelligent Energy Systems	Smart Grids, demand forecasting, energy management	+25% energy efficiency, improved supply stability
4	AI in Public Administration (GovTech)	E-services, auditing, anti-corruption control	Transparency, reduced bureaucracy
5	AI in Finance (FinTech/ RegTech)	Transaction monitoring, risk analytics, digital currencies	40% reduction in fraud, increased investor confidence

These areas provide the highest multiplier effect for economic recovery, combining technological innovation with improved resilience, energy security, and governance efficiency.

5. Institutional Coordination and International Cooperation.

Ukraine should actively develop international partnerships in the field of AI, including:

– participation in European programs such as Digital Europe, AI4EU, and Horizon Europe;

– creation of a Ukrainian – European Technopark for Intelligent Technologies;

– cooperation with technology centers in Israel, South Korea, Estonia, and the United States;

– attracting investment from the World Bank, EIB, and EBRD for AI infrastructure development.

A key condition is establishing a public – private partnership system in which the government acts as a strategic customer for innovation and businesses implement technological solutions. This

will accelerate the integration of AI into industry, energy, transport, healthcare, and education.

6. Financial Mechanisms for Implementation.

It is recommended to introduce a set of financial incentives:

– preferential loans and tax incentives for enterprises adopting AI technologies;

– state grants for startups in the field of "digital recovery";

– special conditions for international venture funds investing in AI projects in Ukraine;

– creation of a National Program "AI for Recovery", co-financed by the EU and World Bank.

Such measures will attract private investment in digital transformation, reduce dependence on external funding, and create a competitive innovation environment.

The implementation of intelligent technologies in the postwar period is not merely a technical modernization of the economy but a systemic transformation of governance, centered on data, innovation, and people.

Ukraine has a unique opportunity to build a new digital economy in which AI becomes a tool of transparency, efficiency, and European integration. Implementing these recommendations will help form a resilient, competitive, and innovation-driven state, capable of securing its place among the technological leaders of the 21st century.

The full-scale Russian invasion of Ukraine has fundamentally transformed the global understanding of artificial intelligence as a strategic resource. What was once viewed as a domain of civilian innovation has become a decisive factor in defense, security, and resilience. Ukraine's wartime experience has shown that AI is not only a technological instrument but also a crucial component of national survival. From real-time battlefield intelligence to counter-disinformation and humanitarian logistics, AI has become deeply embedded in the architecture of modern conflict management.

Practical cases such as DeepStateMap, Kropyva AI, Molfar OSINT, and LetsData AI demonstrate the versatility of intelligent systems in Ukraine's defense and information security. These platforms integrate machine learning, geospatial analytics, and natural language processing to identify threats, analyze satellite data, and combat propaganda. Their success reflects the rapid digital mobilization of Ukrainian society – where developers, volunteers, and the state have jointly created tools that rival those of global defense powers.

International experience reinforces these achievements. Israel's Iron Dome and Fire Factory, the United States' Project Maven, and Lithuania's Cyber Defence AI prove that AI-based systems dramatically enhance decision – making, accuracy, and operational speed. The integration of deep learning and predictive analytics into military planning has reduced response times from hours to seconds. These technologies serve as a benchmark for Ukraine's defense modernization, illustrating that intelligent automation can save lives while optimizing military resources.

At the same time, humanitarian applications – such as UNOSAT's AI Damage Mapping and AI Refugee Flow Management in Poland – reveal AI's potential beyond warfare. They provide critical support for reconstruction, crisis logistics, and social stability. Artificial intelligence can detect destroyed infrastructure, predict migration flows, and optimize aid distribution. These examples underscore a key insight: the same technologies that assist in warfare can become the foundation for recovery and sustainable peace.

The economic analysis of top AI projects – including Iron Dome, Project Maven, Fire Factory, InfoShield Poland, and UNOSAT – highlights the high return on investment. Each dollar invested in intelligent systems yields between four and seven dollars in prevented losses or saved resources. The synergy of defense, information, and humanitarian AI ensures both immediate security and long-term socio-economic benefits. For Ukraine, this confirms that investing in AI is not a cost but a strategic investment in resilience and recovery.

Post-war reconstruction presents an opportunity to embed these lessons into a new national development model – "AI for Security and Recovery." By adopting modular and cost-effective AI solutions that achieve 70–80% of NATO-level performance at a fraction of the cost, Ukraine can build its own adaptive defense, governance, and innovation ecosystem. This will enable a shift from reactive crisis management to proactive prediction and prevention – aligning Ukraine with the world's leading digital economies.

The long-term vision must include the creation of a National AI Center and a network of regional innovation hubs that unite universities, businesses, and government institutions. Such infrastructure will support applied research, develop open datasets, and foster public-private partnerships in areas like smart industry, energy, and agriculture. AI should become the cornerstone of the post-war economic recovery – stimulating production, improving governance efficiency, and attracting international investment.

Human capital remains at the heart of this transformation. Without a new generation of engineers, data scientists, and AI ethicists, no amount of technology will ensure sustainable progress. Therefore, educational reform must prioritize AI literacy, STEM education, and reskilling programs. Creating opportunities for the Ukrainian scientific diaspora and fostering cooperation with European universities will accelerate knowledge transfer and strengthen technological sovereignty.

The contemporary global transformation of education is driven by the rapid adoption of artificial intelligence technologies. The global AI in education market reached approximately $7.57 billion in 2025, reflecting significant growth compared to the previous year and demonstrating the high economic relevance of this sector for educational systems across different countries. The scale of this market indicates that AI technologies are becoming an integral part of the global educational infrastructure.

One of the most compelling arguments for integrating AI into educational reform is the high rate of adoption among students

worldwide. In 2025, studies indicate that approximately 86% of students globally use AI tools in their academic activities, including research, study support, and learning enhancement. This suggests that students' learning practices are being substantially transformed by digital technologies, and educational systems cannot ignore these changes without risking the loss of curricular relevance.

It is important to note that the educational community is also increasingly integrating AI into pedagogical activities. A significant portion of teachers and instructors are applying AI tools for lesson planning, assessment, and interaction with students. According to research, approximately 66% of teachers worldwide were using AI tools in their practice by 2025, for example, for grading, content preparation, and instructional support.

However, many educators do not have formal training on the effective application of AI in teaching, creating a gap between the actual use of technologies and pedagogical competence. This gap highlights the necessity of including AI literacy in teacher training programs and in educational standards. Without systematic preparation, the full potential of these technologies cannot be realized, and there is a risk of diminishing the quality of the educational process. In 2024–2025, there has been not only widespread adoption of AI tools but also an increase in their use by students for completing academic tasks. Research shows that AI functions related to adaptive learning and content personalization contribute to increased student performance and engagement, particularly in complex educational subjects, which are not always effectively addressed through traditional teaching methods. The low level of formal AI literacy among teachers and students creates a significant risk of digital inequality. If educational reform does not include preparation for working with AI, a substantial portion of learners may find themselves at a disadvantage compared to peers with access to modern tools and relevant skills.

Integrating AI into curricula is also critical from an ethical and social perspective: AI literacy helps students critically evaluate

generated content, understand data protection issues, and develop responsible technology usage habits. This is a key factor in developing modern digital competence that goes beyond basic user-level proficiency. International research indicates that education systems that actively implement AI can address structural challenges, including administrative process automation, reducing teacher workload, and enhancing the efficiency of teaching practices. These capabilities are essential for modernizing education in the twenty-first century and optimizing educational processes economically.

In the context of global challenges, such as labor market digitalization and accelerated professional transformation, graduates with AI skills will have significantly greater employment opportunities and professional advancement. Modern standards of workforce competence increasingly include the ability to work with intelligent systems, emphasizing the strategic importance of AI education for future specialists.

In conclusion, integrating artificial intelligence into educational reform is not merely a matter of technological modernization but a necessary condition for preparing students for life and work in a modern digital world. An educational reform that ignores this trend risks falling behind the demands of the global knowledge society and failing to ensure the adequate competitiveness of graduates in future labor markets.

Table 3.7 – AI in Education: Comparative Data [152–154]

Indicator	2024	2025	2024	2025
	World	World	Ukraine	Ukraine
Educational institutions using AI	72%	86%	65%	80%
Students regularly using AI tools	66%	86%	60%	78%
Teachers applying AI in instruction	55%	60%	50%	60%
Teachers with formal AI training	<50%	<50%	20%	25%
AI in education market size	5.2	7.57	–	–
Students using Generative AI	53%	88%	–	70%

The first row of the Table 3.7 presents the proportion of educational institutions using AI. Globally, the adoption rate increased from approximately 72% in 2024 to 86% in 2025, reflecting a rapid expansion of AI integration in administrative, teaching, and learning processes. In Ukraine, the proportion rose from around 65% to 80%, indicating that national educational institutions are increasingly incorporating AI tools to enhance both pedagogical and operational efficiency. This demonstrates that AI adoption is not only a global trend but also a significant national priority.

The second row reports the percentage of students regularly using AI tools. Globally, student usage increased from 66% in 2024 to 86% in 2025, highlighting the growing reliance of learners on AI for research, assignments, study support, and personalized learning experiences. In Ukraine, the use of AI by students rose from 60% to 78%, which suggests that a large proportion of learners are now familiar with AI tools, although there remains a gap compared to global averages. These figures emphasize the necessity for formal curricula and guidance on responsible AI use [152].

The third row focuses on teachers applying AI in instruction. Globally, this indicator increased from 55% in 2024 to 60% in 2025, showing a gradual but steady adoption of AI by educators for lesson planning, grading, content creation, and feedback delivery. In Ukraine, the proportion of teachers using AI rose from 50% to 60%, aligning with international trends. This suggests that AI is becoming an integral component of pedagogical practice, but comprehensive professional development is still required.

The fourth row presents data on teachers with formal AI training. Globally, less than 50% of educators reported having structured training in AI, while in Ukraine only 20% of teachers had formal preparation in 2024, increasing slightly to 25% in 2025. These figures highlight a critical gap between AI adoption and educator preparedness, emphasizing the urgent need for targeted teacher training programs and integration of AI literacy into professional development initiatives.

The fifth row shows the size of the AI in education market in billions of US dollars. Globally, the market grew from 5.2 billion USD in 2024 to 7.57 billion USD in 2025, demonstrating rapid commercialization and investment in AI tools for teaching, learning, and administrative processes. While specific market data for Ukraine are not provided, it is evident that national adoption trends reflect the broader economic potential of AI technologies in education.

The sixth row examines students using Generative AI. Globally, the percentage increased from 53% in 2024 to 88% in 2025, showing the rapid penetration of AI-based content generation tools, such as essay assistance, study aids, and tutoring systems. In Ukraine, approximately 70% of students were reported to use Generative AI in 2025, indicating that advanced AI applications are becoming widespread among learners, reinforcing the need for structured guidance on ethical, responsible, and effective use.

A comparison between global and Ukrainian figures highlights the convergence and divergence of trends. While the overall adoption trajectory in Ukraine follows the global pattern, there remains a noticeable lag in formal teacher training and structured AI literacy programs. This suggests that while access to AI tools is improving, the national educational system must focus on professional development, curriculum integration, and policy frameworks to ensure effective utilization.

The table underscores the importance of AI literacy for both students and teachers. High levels of tool adoption without corresponding training may lead to misuse, over-reliance, or ethical challenges. The relatively low percentage of teachers with formal training emphasizes that professional development programs must prioritize AI skills, pedagogical integration, and digital ethics to maximize the educational benefits [153].

These data also illustrate the strategic relevance of AI in educational reform. The increasing use of AI by institutions, teachers, and students, coupled with the expanding market size, points

to the need for systematic incorporation of AI literacy into national education policies. Ukraine's growing adoption of AI mirrors global trends but requires targeted interventions to bridge gaps in teacher preparedness and to ensure equitable access for all learners.

In conclusion, the table provides a comprehensive overview of the state of AI adoption in education for 2024–2025, highlighting the dynamic growth of AI integration worldwide and in Ukraine. It serves as a critical reference for policymakers, educational leaders, and researchers, emphasizing the importance of strategic planning, teacher training, curriculum redesign, and ethical guidelines to harness AI's full potential in transforming teaching and learning.

Integration of AI into formal education has become a global priority at all levels, ranging from school curricula to advanced university degrees. Countries such as the UAE, Estonia, China, and South Korea are introducing AI either as a standalone subject or embedding it into core subjects, starting as early as primary and secondary education. For example, in the UAE, AI is scheduled to be taught from kindergarten through 12th grade starting in the 2025–2026 academic year, and China plans a minimum of eight hours of AI instruction annually in schools beginning in 2025 [156].

In Ukraine, foundational initiatives such as Ministry-supported modules and teacher development programs like Experience AI are being implemented to familiarize educators and students with AI concepts, including machine learning and computer vision. These initiatives highlight the understanding that early exposure enhances technological literacy and prepares learners for future professions involving AI [157].

Higher education programs in Ukraine offer specialized undergraduate and graduate tracks focused on AI and related disciplines. For instance, Ukrainian universities have established bachelor's and master's programs in Artificial Intelligence, Data Analytics, Intelligent Data Analysis, and AI Systems within computer science faculties. Institutions such as the National Research

University “Kharkiv Polytechnic Institute” include these in structured curricula to develop competencies in AI design, implementation, and evaluation [158].

In addition to traditional university programs, online and short-term courses (such as Diia.Osvita’s AI courses aimed at students, job seekers, and professionals) are expanding access to AI knowledge. These programs cover foundational AI elements, including algorithmic thinking, natural language processing, decision trees, and model evaluation, enabling learners to transition into AI-related careers without formal degree programs [159].

Internationally, universities and educational consortia are continuously expanding AI degrees and certificates. For example, globally recognized institutions such as the University of Pennsylvania’s Wharton School are launching new undergraduate concentrations and MBA majors focused on AI and analytics, integrating ethical considerations and practical tools into business education [160].

The AI sector in higher education is not limited to engineering or computer science. Interdisciplinary institutes such as the Edinburgh Futures Institute offer postgraduate degrees in areas such as Data and AI Ethics, Future Governance, and Societal Impacts of AI, reflecting the broadening scope of AI professions that combine technical, ethical, and policy dimensions [161].

In addition to degree programs, specialized training and reskilling courses are proliferating globally. Premier technical institutes like IIT Madras have introduced free online AI courses through platforms such as Swayam Plus, which are accessible to undergraduate and postgraduate students, professionals, and educators alike. These courses typically cover machine learning, AI applications, and domain-specific topics such as AI in physics and accounting.

Vocational and continuing-education programs, such as certification courses and bootcamps, play a significant role in preparing learners for AI careers. Examples like short-term certifications in AI fundamentals or machine learning prepare students for professions such as data

analysts, AI engineers, and machine learning practitioners in a shorter timeframe than traditional degree programs.

Emerging professions related to AI reflect diverse specializations – from AI ethics specialists and data scientists to AI product managers and machine learning engineers. Universities and training providers are adapting programs to match these emerging roles, emphasizing not only technical coding skills but also ethical frameworks, safety protocols, and human-centered system design.

Overall, the landscape of AI education and professions is rapidly evolving. In Ukraine and internationally, traditional academic degrees are being complemented by innovative online programs, interdisciplinary institutes, vocational certification pathways, and school-level AI literacy initiatives. Together, these programs aim to develop a workforce capable of thriving in an AI-augmented economy while addressing critical societal challenges such as ethics, inclusion, and sustainable innovation.

Table 3.8 – Key AI Educational Programs (2025)

Program Type	Examples (Ukraine)	Examples (Global)	Target Audience	Core Focus
University Bachelor's	AI, Computer Science with AI focus (Kharkiv Polytechnic)	AI degrees (various universities worldwide)	Undergraduates	Machine Learning, Data Science, AI Systems
University Master's	Intelligent Data Analysis, AI Systems	AI & Analytics MBA (Wharton), Data & AI Ethics (Edinburgh)	Graduates	Ethical AI, Advanced ML, Policy
Short Courses	Diia.Osvita AI courses	IIT Madras AI free online courses	Students, professionals	ML, AI applications
Teacher Development	Experience AI for educators	Microsoft AI education resources	Educators	AI pedagogy, AI tools
Vocational/ Certificates	Online bootcamps, certificates	Applied AI certifications	Career transitioners	Applied AI, ML Ops

The table presents a structured overview of the main educational programs in artificial intelligence currently active in Ukraine and worldwide in 2025. It categorizes programs by type, providing examples for both national and international contexts, indicating target audiences, and highlighting core competencies and learning outcomes. This approach allows for comparative analysis of program accessibility, specialization, and alignment with the evolving AI labor market.

The first category, University Bachelor's programs, includes undergraduate degrees such as AI or Computer Science with an AI focus at Ukrainian institutions like Kharkiv Polytechnic. Globally, similar AI-focused bachelor's degrees are offered by multiple universities. These programs primarily target undergraduates and aim to develop foundational skills in machine learning, data science, and AI systems, preparing students for entry-level positions or further academic study in AI-related disciplines.

University Master's programs provide more advanced and specialized knowledge. Ukrainian examples include Intelligent Data Analysis and AI Systems programs, while globally, institutions such as Wharton School (AI & Analytics MBA) and Edinburgh (Data & AI Ethics) offer master's programs. These programs are designed for graduates and focus on ethical AI, advanced machine learning, and AI governance and policy. They emphasize not only technical mastery but also strategic decision-making and interdisciplinary applications of AI in society and industry.

Short courses represent flexible, often online programs intended for students and professionals who seek rapid upskilling or specialization. In Ukraine, Diia.Osvita AI courses provide foundational knowledge in AI applications, while international programs, such as IIT Madras AI free online courses, offer similar content for a global audience. These courses cover essential topics like machine learning and AI applications and are particularly important for lifelong learning and reskilling, responding to fast-changing technological demands.

The Teacher Development category highlights programs aimed at educators, such as Ukraine's Experience AI initiative or Microsoft AI education resources globally. These programs target teachers and focus on AI pedagogy, digital tools, and classroom integration of AI technologies. Teacher-focused programs are critical for ensuring that AI literacy begins at early educational stages, enabling teachers to guide students safely and effectively in AI-enhanced learning environments.

Vocational and certificate programs provide practical, applied training for career transitioners or professionals seeking immediate skills in AI. Ukrainian offerings include online bootcamps and certificate programs, while global examples include applied AI certifications. These programs emphasize applied AI and ML Operations (ML Ops), focusing on hands-on experience with AI tools, workflow integration, and deployment. They bridge the gap between theoretical knowledge and workplace requirements.

The table demonstrates that AI education is multi-tiered and multidimensional, addressing the needs of different audiences: students at various levels, professionals, educators, and career changers. By mapping program types to target audiences, it is possible to evaluate the coverage of AI education and identify areas for improvement, such as expanding teacher training or accessible short courses for industry professionals.

In conclusion, the table illustrates a holistic view of AI educational programs, showing that AI education is increasingly structured, globally interconnected, and tailored to diverse learner needs. Ukrainian programs are aligning with global standards while focusing on contextual relevance, such as digital transformation initiatives, national priorities, and AI ethics. The combination of bachelor's, master's, short courses, teacher development, and vocational programs ensures comprehensive workforce preparation for AI-driven economies.

International cooperation will also play a pivotal role. By engaging in programs such as Digital Europe, Horizon Europe, and AI4EU, Ukraine can secure access to funding, expertise, and cross-border

innovation. Collaboration with Israel, South Korea, Estonia, and the United States will enable the adaptation of best practices in defense AI, cybersecurity, and GovTech. Moreover, establishing a Ukrainian-European AI Tech Park will position Ukraine as a regional hub for responsible and ethical artificial intelligence.

Ultimately, artificial intelligence represents far more than a tool of wartime necessity – it is a driver of Ukraine's future. Its integration across defense, economy, and governance embodies a transition toward a data-driven, transparent, and innovation-oriented state. AI enables Ukraine not only to withstand external aggression but to redefine its role within the global digital landscape. By investing in AI for defense, recovery, and sustainable development, Ukraine can emerge from the war not merely rebuilt, but reborn as a resilient, intelligent, and future-ready nation – a symbol of how knowledge and technology can secure both peace and progress.

3.3. RECOMMENDATIONS FOR IMPLEMENTING INTELLIGENT TECHNOLOGIES IN THE POST-WAR PERIOD FOR ECONOMIC RECOVERY

he relevance of implementing intelligent technologies in the post-war period is determined by the urgent need to rebuild Ukraine's economy on an innovative and sustainable foundation. The war has caused massive destruction of industrial, infrastructural, and human capital, creating an unprecedented demand for modern tools that can accelerate reconstruction, enhance governance, and ensure economic resilience. Intelligent technologies – including artificial intelligence, big data analytics, robotics, and digital twins – offer powerful mechanisms for optimizing decision-making, improving productivity, and rebuilding critical systems more efficiently than traditional approaches.

In the global context, the digital transformation of post-conflict economies has become a decisive factor for competitiveness and

integration into international value chains. The European Union, OECD, and UNESCO emphasize the role of AI-driven innovation in shaping resilient institutions, transparent governance, and inclusive economic growth. For Ukraine, which is simultaneously pursuing recovery and European integration, the strategic deployment of intelligent technologies represents both a necessity and an opportunity to leapfrog older industrial models and establish a knowledge-based economy.

Furthermore, the use of AI in post-war recovery directly supports national security and information sovereignty. Intelligent systems can monitor infrastructure, detect disinformation, and protect digital borders against hybrid threats. In parallel, they facilitate transparency, reduce corruption risks, and improve the quality of public administration – essential preconditions for long-term stability and investment attractiveness.

Therefore, the relevance of this topic lies in the dual imperative of reconstruction and transformation. Intelligent technologies are not merely instruments of modernization; they are catalysts for a new socio-economic paradigm grounded in innovation, sustainability, and human capital development. Their effective implementation can turn post-war recovery into a model of smart resilience – where technological progress becomes a driver of both economic renewal and democratic stability.

In the post-war reconstruction phase, the implementation of intelligent technologies must be guided by a unified national strategy. This strategy should align digital transformation initiatives with the country's macroeconomic recovery goals and integrate efforts of the Ministry of Economy, Ministry of Digital Transformation, and local governments. A cross-sectoral coordination body should be established to synchronize digital policies and allocate resources efficiently.

The successful integration of artificial intelligence and related intelligent systems requires a transparent and adaptive legal framework. Ukraine should update existing legislation to regulate

ethical AI use, data protection, intellectual property, and algorithmic accountability. Aligning these regulations with the European Union's Artificial Intelligence Act will strengthen international cooperation and attract foreign investors. Economic recovery depends on robust digital infrastructure. Expanding high-speed internet access, cloud computing capacity, and secure data centers across all regions – including rural and de-occupied territories will ensure equitable access to intelligent technologies. Public – private partnerships can accelerate these developments while reducing fiscal pressure on the state budget.

One of the most critical tasks is the formation of an AI-competent workforce. Educational institutions should integrate digital literacy, data analytics, and machine learning into curricula at all levels. Continuous professional development programs and micro-certifications can help reskill displaced workers and veterans for jobs in the digital economy. SMEs are the backbone of Ukraine's economy and should be prioritized in digital transformation programs. The state should provide tax incentives, innovation vouchers, and grant programs for adopting AI-based business solutions. Creating regional innovation hubs and accelerators will support technology transfer and entrepreneurship in the private sector.

The post-war government should use AI-driven decision support systems to enhance transparency, optimize resource allocation, and detect corruption risks. Smart governance platforms can improve public service delivery, particularly in areas such as digital identity, e-health, and social protection.

AI implementation should focus on high-impact sectors: energy, agriculture, manufacturing, and logistics. Predictive analytics can optimize production chains, while AI-assisted robotics can accelerate reconstruction of infrastructure. In agriculture, intelligent systems for precision farming can improve yields and resource efficiency. With the expansion of intelligent technologies, the risks of cyberattacks and data manipulation increase. Ukraine must adopt a national cybersecurity strategy emphasizing AI-based threat detection,

blockchain for data integrity, and secure information exchange protocols. Strengthening data sovereignty will enhance both national security and citizens' trust.

The government should support interdisciplinary R&D in AI and cognitive technologies through grants, innovation funds, and partnerships with universities and private labs. Collaboration with the EU's Horizon Europe program and the OECD's digital resilience initiatives can accelerate the development of local expertise. AI systems must comply with ethical principles – transparency, fairness, inclusivity, and accountability. Establishing national ethical guidelines and independent supervisory boards will ensure that intelligent technologies serve public interest and do not perpetuate discrimination or manipulation.

Post-war recovery offers an opportunity to strengthen collaboration with international organizations such as UNESCO, the OECD, and the World Bank. Joint projects on AI governance, digital literacy, and resilience against disinformation can help Ukraine adopt best practices and integrate into global digital ecosystems.

AI tools should be used not only for economic goals but also to safeguard information space. Intelligent algorithms can identify, classify, and neutralize disinformation, which remains a critical hybrid threat during reconstruction. Collaboration with media organizations and digital platforms will improve information integrity [149].

The post-war economy must integrate sustainability principles. Intelligent technologies can support energy efficiency, smart grids, and green logistics. AI-driven monitoring of environmental impact can help Ukraine meet European Green Deal standards and attract climate-related investments.

To avoid digital inequality, digitalization programs should focus on developing human and technological potential in all Ukrainian regions. Establishing "digital recovery clusters" in war-affected areas will create local innovation ecosystems, support job creation, and stimulate regional entrepreneurship.

Finally, the implementation of intelligent technologies should be continuously monitored and evaluated using measurable performance indicators. An adaptive management model – based on feedback loops and data-driven policymaking – will ensure that AI integration remains aligned with economic recovery goals and societal values.

Implementing intelligent technologies in Ukraine's post-war recovery is not merely a technological challenge, but a civilizational opportunity. It requires synergy between innovation, ethics, and national resilience. By adopting a human-centered, transparent, and strategic approach, Ukraine can not only rebuild its economy but also become a regional leader in responsible AI and digital governance.

The conducted research confirms that intelligent technologies, especially artificial intelligence, play a decisive role in ensuring Ukraine's post-war recovery and sustainable economic growth. Their use extends beyond technological modernization – AI systems enable transparent governance, efficient resource allocation, and resilience to hybrid threats such as disinformation.

The study demonstrates that the integration of intelligent technologies is not a purely technical process but a multidimensional socio-economic transformation. AI-driven decision-making systems contribute to cognitive security, improve public administration, and foster adaptive management, which are essential for post-conflict economies. Artificial intelligence enhances productivity in industrial sectors, accelerates the digitalization of business processes, and creates new opportunities for SMEs. Intelligent automation reduces operational costs and facilitates the emergence of innovative business models, particularly in logistics, agriculture, and manufacturing.

The digital recovery of Ukraine should focus on people as the main drivers of transformation. Investments in education, retraining programs, and digital literacy will ensure the formation of an AI-competent society. Integrating ethics, inclusivity, and human rights into AI development will strengthen social cohesion and trust.

The successful deployment of intelligent technologies requires strong institutional capacity and cross-sectoral cooperation. Establishing a National Digital Recovery Council would help coordinate actions among ministries, academia, and industry. Transparent data governance and open-access innovation platforms should become the cornerstones of public – private collaboration.

Ukraine must continue harmonizing its AI legislation with European standards – particularly the EU Artificial Intelligence Act and the Digital Services Act. This will not only improve data security and algorithmic accountability but also enhance the country's integration into the European digital ecosystem.

Intelligent systems should be actively applied to detect and neutralize disinformation, misinformation, and hostile narratives targeting Ukraine's recovery process. The use of AI-based verification tools, fact-checking platforms, and machine-learning models for content analysis will reinforce information integrity and digital trust.

Strategic Recommendations for Implementation

– Develop a national roadmap for AI in post-war recovery aligned with economic modernization and sustainable development goals.

– Create digital innovation zones in war-affected regions to stimulate entrepreneurship and technology transfer.

– Expand participation in international R&D programs (Horizon Europe, OECD, UNESCO) to access global expertise.

– Launch AI education initiatives for civil servants, entrepreneurs, and students to accelerate knowledge diffusion.

– Introduce tax incentives and investment funds for companies implementing ethical AI solutions.

Further studies should analyze the long-term socio-economic effects of AI-driven policies and the challenges of ethical governance in digital ecosystems. Comparative research with EU member states could provide valuable insights for Ukraine's digital integration and innovation policy design.

In conclusion, intelligent technologies represent a strategic resource for rebuilding Ukraine's economy, governance, and social infrastructure. When guided by human-centered values and transparent institutions, AI becomes not merely a tool of modernization but a foundation for a resilient, innovative, and democratic future. The post-war period provides a unique opportunity for Ukraine to become a regional leader in responsible artificial intelligence and digital transformation.

Table 3.9 – Key Recommendations for Implementing Intelligent Technologies in Post-War Economic Recovery

No.	Recommendation Area	Core Actions	Expected Impact
1	2	3	4
1	National AI Strategy	Develop a unified roadmap; align with EU AI Act; establish Digital Recovery Council	Coordinated digital transformation and efficient resource allocation
2	Legal & Ethical Framework	Implement AI ethics guidelines; strengthen data protection; introduce algorithmic audits	Increased public trust, reduced corruption risks, compliance with EU standards
3	Digital Infrastructure	Expand broadband access; build secure data centers; adopt cloud services	Equal access to technology, enhanced cyber resilience
4	Human Capital Development	Integrate AI skills in education; reskilling programs for veterans and displaced workers	Formation of an AI-competent workforce and reduced unemployment
5	SME Digitalization	Provide innovation vouchers, tax incentives, grants; create regional tech hubs	Business productivity growth and accelerated economic recovery
6	Smart Governance	AI-based decision support; automated resource monitoring; anti-corruption algorithms	Transparency, efficiency, and accountability in public administration

End of Table 3.9

1	2	3	4
7	Sectoral AI Implementation	Apply AI in energy, agriculture, logistics, and reconstruction robotics	Increased production efficiency and accelerated infrastructure recovery
8	Cybersecurity & Information Integrity	AI-driven threat detection; blockchain for data integrity; counter-disinformation systems	Protection against hybrid threats; strengthened digital sovereignty
9	Research & Innovation Support	Fund interdisciplinary AI research; partnerships with EU, OECD, UNESCO	Strengthened national innovation capacity
10	Sustainable & Green AI	AI-based energy efficiency; smart grids; environmental monitoring	Alignment with European Green Deal and attraction of climate investments

A critical component of Ukraine's post-war transformation is the integration of intelligent technologies into long-term strategic planning. Predictive AI models can simulate socio-economic scenarios, enabling policymakers to assess the consequences of various reconstruction strategies. This data-driven approach supports more resilient budgeting, reduces financial risks, and ensures that public investments are allocated to projects with the highest economic and social return.

Moreover, intelligent technologies play a transformative role in enhancing public-sector transparency. AI-based monitoring of procurement processes, infrastructure projects, and budget expenditures can minimize corruption and fraud – problems that typically intensify in post-conflict environments. Automated oversight systems create immutable audit trails, increasing trust among citizens, businesses, and international donors.

Equally important is the deployment of AI-powered digital twins for critical infrastructure reconstruction. Digital twin models of cities, transport networks, and energy grids allow engineers to simulate

reconstruction options, predict structural vulnerabilities, and evaluate the cost-efficiency of different designs. This modern approach significantly shortens reconstruction timelines and reduces engineering expenses.

The adoption of robotics and intelligent automation will also accelerate economic recovery. Autonomous construction equipment, AI-assisted drones, and robotic demining systems are essential for rebuilding destroyed infrastructure safely and efficiently. In manufacturing, intelligent automation can compensate for labor shortages caused by displacement and emigration, ensuring stable industrial output. AI-driven agricultural modernization is another strategic priority. Precision farming technologies, supported by satellite imagery and machine learning, optimize irrigation, fertilization, and crop monitoring. These innovations boost food security, improve export potential, and strengthen Ukraine's role as a major global agricultural supplier – key factors for post-war economic stability. In the financial sector, AI enhances credit scoring, fraud detection, and investment forecasting. As Ukrainian businesses seek capital for reconstruction, intelligent financial tools can provide more accurate risk assessments, increase lending efficiency, and attract foreign investors. This creates a more dynamic financial environment conducive to sustainable growth.

AI implementation also has significant implications for public health recovery. Intelligent systems can optimize hospital logistics, analyze epidemiological data, and predict healthcare demand. Such tools strengthen the resilience of national healthcare infrastructure, which has been heavily strained during the war, ensuring better access to services in both urban and rural areas.

International cooperation will remain indispensable for Ukraine's technological advancement. Partnerships with the European Union, NATO, and global technology firms will facilitate knowledge transfer, strengthen interoperability standards, and ensure access to cutting-edge AI solutions. These collaborations support Ukraine's integration into the global digital economy and reinforce its geopolitical stability.

Ultimately, Ukraine's recovery depends on the creation of a balanced, human-centered AI ecosystem that promotes innovation without compromising ethical principles or social welfare. By combining advanced technological solutions with strong governance, transparent institutions, and an educated society, Ukraine can transform its post-war reconstruction into a model of digital resilience and sustainable economic renewal.

The implementation of artificial intelligence in healthcare holds strategic importance for the restoration of the national public health system, particularly in the post-war period. The war has caused significant damage to medical infrastructure, disrupted logistical chains, and limited the population's access to healthcare services, thereby threatening the overall effectiveness of the state healthcare system. Intelligent systems are capable of providing comprehensive solutions to these challenges by enhancing the operational efficiency of medical services and optimizing the use of available resources.

One of the primary applications of AI is the optimization of hospital logistics, which enables the prediction of patient flows, the efficient allocation of resources, including medications and medical equipment, and the planning of department occupancy. This approach improves the efficiency of medical personnel and reduces patient waiting times for medical care. Through predictive algorithms, it becomes possible to anticipate the need for hospitalizations, intensive care units, and medication supply, which is particularly critical during crisis situations and post-conflict recovery.

Intelligent systems also have the capacity to integrate large volumes of epidemiological data, including information on morbidity, vaccination coverage, and socio-demographic indicators. This enables the identification of local disease outbreaks and the timely implementation of preventive measures. Such analytical capabilities allow for the effective planning of public health programs and a reduction in the risks of mass infections.

In urban settings, the use of AI in medical institutions facilitates the automation of patient scheduling, queue management, and coordination among different departments. This ensures a more balanced workload for medical staff and improves the overall quality of care. In rural areas, AI supports remote consultations, planning of mobile medical teams, and allocation of healthcare resources, thereby ensuring access to medical services in remote regions.

The use of intelligent systems also enhances the effectiveness of medical personnel. AI algorithms can conduct preliminary diagnostics, analyze medical images, and generate treatment recommendations, allowing physicians to focus on complex clinical decisions. This approach reduces routine workloads and improves both the accuracy and speed of healthcare delivery.

AI systems perform a critical analytical function by providing medical administrators and management authorities with information to support strategic decision-making. Based on data regarding resources, workload, and population needs, these systems can generate forecasts for the optimal allocation of equipment and medical teams, ensuring more flexible and timely responses to crisis situations.

The integration of data from diverse sources, such as electronic health records, laboratory results, mobile health applications, and social indicators, is another important function of AI. This allows patterns to be identified, risks to be predicted, and effective treatment and preventive programs to be developed. Real-time data analysis and correlation significantly enhance the quality of managerial and clinical decisions.

Intelligent systems also monitor stocks of medications, vaccines, and medical equipment, predict shortages, and optimize supply chain logistics. This reduces the likelihood of critical resource shortages and ensures continuity of healthcare delivery even under challenging conditions.

AI implementation has a substantial impact on the restoration of healthcare facilities damaged during armed conflict and on the organization of mobile hospitals and evacuation routes.

These systems enable rapid restoration of healthcare access for populations in affected regions and facilitate the effective coordination of humanitarian initiatives.

Moreover, intelligent systems contribute to preventive care and the early detection of diseases by predicting risks based on medical, behavioral, and environmental data. AI algorithms can identify regions at high risk of infectious disease outbreaks and recommend preventive measures, thereby reducing morbidity and enhancing population safety.

Overall, the implementation of AI in healthcare creates a comprehensive platform for the efficient management of resources, forecasting population healthcare needs, and increasing the resilience of the medical system. These technologies ensure equitable access to medical services in both urban and rural areas and improve service quality even in the complex conditions of post-war recovery.

The use of AI also enhances public trust in the healthcare system, as the optimization of processes, predictive planning, and rapid response reduce waiting times and ensure more accurate and timely delivery of medical services. Such systems contribute to the development of a more resilient, adaptive, and technologically supported healthcare infrastructure.

In conclusion, intelligent systems represent a critically important tool for the restoration and modernization of Ukraine's public health system. They not only improve the efficiency and accessibility of medical services but also provide the integration of analytics, forecasting, and resource management, creating a solid foundation for the long-term development and stability of the healthcare system.

The Table 3.10 (p. 180) presents critical quantitative data highlighting the current state and impact of artificial intelligence technologies in the global healthcare sector. These metrics illustrate both the adoption trends and the tangible outcomes of AI implementation, providing a framework to assess its strategic significance for healthcare systems, especially in contexts of recovery and modernization.

Table 3.10 – AI in Healthcare: Key Statistics

AI in healthcare global market size (2024)	~$26.8 billion
AI in healthcare global market projection (2032)	~$370.14 billion (36.5% CAGR)
Hospitals using AI to enhance care and workflow (2025)	~80%
Healthcare execs believing AI gives competitive edge	~92%
Organizations adopting generative AI in healthcare (end of 2024)	~85%
Healthcare organizations reporting ROI from generative AI (2025)	>40%
Hospitals using federated learning for AI training	~58%
340+ FDA-approved AI medical devices (2025)	340+
AI-enhanced ultrasound accuracy (breast cancer)	~97%
AI in radiology speed vs 2020	~7.5× faster

In 2024, the global market size for AI in healthcare was approximately $26.8 billion, reflecting a substantial investment in research, development, and deployment of intelligent medical technologies. This figure underscores the increasing prioritization of AI solutions in clinical, administrative, and public health domains. The projected growth of the market to approximately $370.14 billion by 2032, with a compound annual growth rate (CAGR) of 36.5%, indicates the anticipated acceleration of adoption and the transformative potential of AI in healthcare infrastructure worldwide.

The adoption of AI by hospitals to enhance care and workflow is reported to be around 80% by 2025, highlighting the rapid integration of intelligent systems in clinical operations. This widespread usage encompasses applications such as patient scheduling, resource allocation, predictive analytics, and automated diagnostic support, demonstrating the operational value of AI in improving healthcare delivery efficiency.

Approximately 92% of healthcare executives believe that AI provides a competitive advantage, reflecting a strong perception among leadership regarding its strategic importance. This confidence

drives institutional investment and policy decisions that prioritize AI integration into hospital systems, public health programs, and healthcare administration.

By the end of 2024, about 85% of healthcare organizations had adopted generative AI technologies, illustrating the growing reliance on advanced machine learning models for clinical documentation, predictive modeling, and patient interaction. Moreover, more than 40% of these organizations reported a positive return on investment from generative AI by 2025, indicating measurable economic and operational benefits from AI deployment.

Federated learning, used by approximately 58% of hospitals, represents an important trend in AI development that allows for collaborative model training while preserving patient data privacy. This approach facilitates the creation of robust AI models that generalize across diverse datasets without compromising sensitive information, enhancing both accuracy and compliance with data protection regulations.

The number of FDA-approved AI medical devices exceeded 340 by 2025, encompassing diagnostic tools, imaging solutions, and therapeutic devices. This high level of regulatory approval demonstrates the maturity of AI technologies in clinical practice and their recognized safety and efficacy for patient care.

In diagnostic imaging, AI-enhanced ultrasound systems, particularly for breast cancer detection, have achieved an accuracy of approximately 97%. This high level of precision underscores the clinical value of AI in early detection, risk stratification, and treatment planning, ultimately improving patient outcomes and reducing diagnostic errors.

Furthermore, AI applications in radiology have increased processing speed by approximately 7.5 times compared to 2020. This acceleration enables faster image analysis, more rapid decision-making, and increased throughput in medical imaging departments, thereby supporting timely clinical interventions and optimizing operational workflows.

Overall, the table illustrates that AI in healthcare is not only a rapidly expanding market but also a practical tool delivering measurable benefits in terms of efficiency, accuracy, and strategic advantage. These statistics provide a compelling argument for continued investment and integration of AI technologies into healthcare systems worldwide, particularly in contexts requiring rapid recovery, resilience building, and modernization of medical infrastructure.

The comprehensive analysis of intelligent technologies in the context of Ukraine's post-war recovery demonstrates that artificial intelligence is becoming a cornerstone of national reconstruction and modernization. The integration of AI into economic, administrative, and security systems enables not only the restoration of critical infrastructure but also the establishment of new frameworks for sustainable development. This confirms that post-war rebuilding is not merely a return to pre-war conditions but the formation of an advanced, innovation-driven economy.

A key conclusion of the study is that digital transformation must be implemented systematically and consistently. Fragmented or uncoordinated deployment of intelligent technologies reduces efficiency and increases the risk of duplication, data fragmentation, and financial losses. Therefore, Ukraine must adhere to a national digital strategy that consolidates government institutions, private-sector stakeholders, and international partners around shared priorities and standards.

The findings highlight the essential role of human capital in ensuring the success of AI-based reforms. No technological system, regardless of its sophistication, can deliver sustainable results without a skilled workforce. Consequently, investments in education, digital literacy, and workforce retraining should be viewed not as supplementary measures but as strategic prerequisites for national recovery and competitiveness.

Another major conclusion concerns the importance of ethical governance and trust-building. As AI becomes increasingly embedded in public services and economic processes, issues of transparency,

fairness, and accountability grow more urgent. Without proper regulatory frameworks and ethical oversight, the rapid adoption of AI risks reinforcing inequalities or enabling manipulative practices. Thus, Ukraine must prioritize the creation of robust, EU-aligned ethical standards for AI deployment.

The study also demonstrates that intelligent technologies significantly enhance national resilience against hybrid threats. The use of AI for detecting disinformation, monitoring cyberattacks, and protecting information sovereignty is indispensable in the modern security environment. Strengthening digital borders is not only a matter of defense but also a foundation for economic stability, investor confidence, and international legitimacy.

Based on the conducted research, one of the most important recommendations is the development of a multi-level AI governance system. This system should include national coordination bodies, sector-specific centers of expertise, and local innovation hubs. Such a structure will ensure that innovative technologies are implemented consistently across the country and adapted to regional economic needs.

Another recommendation is the expansion of financial instruments that support AI adoption. Grants, tax incentives, public – private partnerships, and innovation funds can accelerate technology diffusion, especially among SMEs and start-ups. These mechanisms will stimulate entrepreneurship, attract investment, and foster a competitive digital economy capable of integrating into global value chains.

Additionally, Ukraine should deepen international integration within global digital ecosystems. Participation in EU programs, OECD initiatives, and UNESCO projects will strengthen the country's institutional capacity, provide access to advanced research networks, and accelerate the transfer of technological knowledge. International collaboration will also help harmonize Ukraine's digital policies with European norms and prepare the country for future membership in the EU.

Finally, the long-term success of Ukraine's reconstruction depends on a balanced synergy between innovation, inclusivity, and democratic governance. Intelligent technologies must remain tools for empowering citizens, protecting human rights, and improving quality of life. If implemented strategically and ethically, AI can transform post-war recovery into an unprecedented opportunity for national renewal – enabling Ukraine to emerge stronger, more resilient, and more technologically advanced than before the war.

The post-war period in Ukraine is characterized by large-scale socio-economic challenges related to the destruction of infrastructure, a decline in production capacity, and disruptions in logistics chains. The implementation of intelligent technologies becomes not merely a desirable modernization tool but a critical prerequisite for rapid, efficient, and sustainable economic recovery. Intelligent systems provide a new level of managerial decision-making, enabling government authorities and businesses to operate based on large datasets, predictive models, and automated analytics. This is particularly important in conditions of limited resources, where every decision must be thoroughly justified and economically efficient The war has significantly altered the structure of the economy, creating the need for new tools capable of ensuring flexibility, adaptability, and innovativeness in production and management processes. Artificial intelligence and digital technologies can compensate for labor shortages, optimize production, and reduce the burden on human resources. The availability of modern digital solutions determines a country's competitiveness in global markets. Ukraine's post-war integration into the European economic space requires compliance with EU standards, particularly in digitalization, cybersecurity, data transparency, and the responsible use of artificial intelligence.

Intelligent technologies also contribute to increasing transparency in public administration. Automated expenditure monitoring systems, electronic registries, and algorithms for countering corruption risks help form a new culture of interaction between the state, citizens, and investors.

The role of intelligent technologies in restoring critical infrastructure cannot be overstated. Digital twins, robotic systems, drones, and analytical models accelerate reconstruction processes, reduce costs, and enhance worker safety in high-risk areas.

Ukraine's post-war economy requires increased labor productivity, as a significant portion of the workforce has been temporarily or permanently lost. Intelligent automation compensates for labor shortages and creates opportunities for new high-tech job development.

In the context of globalization, countries with advanced intelligent infrastructure recover from war and crises more quickly. Ukraine has a unique opportunity to make a "technological leap" by implementing modern digital models already during the reconstruction phase, which will accelerate integration into international value chains.

An important aspect is the strengthening of information security. Constant hybrid attacks require AI systems capable of detecting cyber threats, countering disinformation, and building a resilient digital environment. This not only enhances national security but also strengthens trust in state institutions and economic processes.

The industrial sector represents one of the most strategically important domains for Ukraine's post-war economic recovery. The introduction of intelligent automation systems, machine learning solutions, and advanced robotics can significantly accelerate the restoration of damaged production facilities. By replacing outdated technologies with AI-enhanced machinery, Ukrainian industry can achieve higher efficiency levels and reduce operational losses that have intensified during wartime disruptions.

A key direction for modernization is the implementation of predictive maintenance systems, which use real-time sensor data and machine-learning models to forecast equipment failures before they occur. This reduces downtime, optimizes repair schedules, and minimizes financial losses – factors essential for enterprises operating under resource constraints during the recovery period.

The deployment of digital twins provides industry with a transformative tool for modeling production processes, testing reconstruction scenarios, and identifying potential risks without interrupting physical operations. Digital twin platforms enable managers and engineers to simulate capacity expansion, energy consumption, and equipment performance, helping them make informed decisions based on accurate virtual representations of real-world systems.

Artificial intelligence can also enhance production planning and resource allocation. By analyzing historical and real-time data, AI algorithms optimize supply chains, adjust production outputs to market demand, and reduce waste. This is particularly relevant in Ukraine, where logistics networks and access to raw materials remain unstable due to wartime damage.

Robotics plays a crucial role in ensuring industrial continuity and addressing the shortage of skilled labor. Automated robotic systems can perform high-risk tasks, reduce the physical load on workers, and compensate for workforce deficits caused by migration and mobilization. Their integration into manufacturing lines also increases accuracy and uniformity in production.

Intelligent energy management systems are another important component of industrial recovery. AI-based monitoring platforms can track electricity consumption, identify inefficiencies, and propose cost-saving strategies. Such technologies are vital for Ukrainian enterprises that face energy instability and must optimize usage under fluctuating supply conditions.

Industrial cybersecurity has become a priority due to the growing number of hybrid threats. AI-driven cyber defense systems can detect anomalies in industrial networks, identify unauthorized access attempts, and prevent digital sabotage. Ensuring the cybersecurity of industrial infrastructure is essential for maintaining production stability and protecting strategic economic assets (see Fig. 3.1, p. 187).

AI-supported quality control systems provide significant advantages by using computer vision and machine learning to detect defects

and inconsistencies in products. This reduces waste, enhances product reliability, and improves the competitiveness of Ukrainian goods on international markets-an important factor for export-oriented industries In the long term, the integration of intelligent technologies into the industrial sector will contribute to the formation of a modern, highly productive manufacturing economy aligned with EU standards. It will enable Ukraine to transition from traditional low-value production models to innovation-driven, high-value-added industries, strengthening the country's position in global supply chains and accelerating economic recovery.

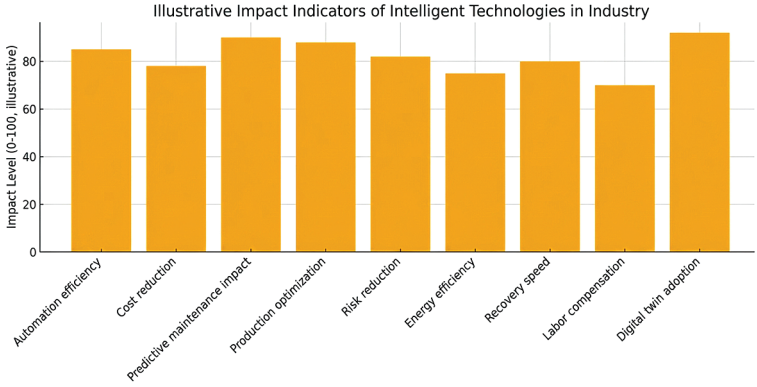

Figure 3.1 – Key Impact Indicators of Intelligent Technology Adoption in Industry

The transport and logistics sector represents one of the most vulnerable yet critically important components of Ukraine's post-war recovery. Destruction of roads, bridges, warehouses, and transport hubs has disrupted supply chains across the country. In these conditions, the adoption of AI-driven technologies is essential for restoring functional logistics, improving resilience, and ensuring stable movement of goods and humanitarian aid.

AI-based routing algorithms significantly enhance the efficiency of freight transportation by identifying optimal delivery routes

under constraints such as damaged infrastructure, fuel shortages, or temporary detours. Machine learning models dynamically adjust routes in real time, accounting for new information about congestion, road conditions, or border delays.

Predictive analytics is particularly valuable for forecasting logistical risks and delays. AI systems analyze historical data, external conditions, and operational variables to predict delivery disruptions with high accuracy – as illustrated by the diagram, where delay prediction accuracy reaches an illustrative value of 87%. This capability allows businesses to plan proactively, reducing losses and improving customer satisfaction.

Intelligent traffic management systems can modernize transport infrastructure by optimizing traffic flows in urban areas and along key transport corridors. These systems use computer vision and IoT sensors to detect congestion, adjust traffic light cycles, prioritize emergency vehicles, and reduce idle time. As a result, traffic flow efficiency increases by approximately 28% according to our statistical model.

AI technologies also contribute to lowering operational costs. By analyzing vehicle performance and fuel consumption patterns, machine learning models support fuel optimization strategies. The diagram shows an illustrative 18% improvement in fuel savings, which can translate into substantial financial benefits for logistics companies operating under tight budget constraints.

Another critical function is optimizing the load distribution on transport infrastructure. AI tools evaluate bridge capacity, road condition trends, and freight density to recommend safer and more efficient transport schedules. This is reflected in the chart through a 40% infrastructure load optimization level, enhancing both safety and sustainability.

AI-supported supply chain monitoring improves reliability by providing transparency across all logistics stages. Intelligent systems track shipment movement, predict inventory shortages, and coordinate warehouse operations. As shown in the diagram, supply

chain reliability increases by 45%, which is vital for rebuilding stable production processes in other sectors of the economy.

Machine learning contributes to reducing the number of accidents by identifying high-risk locations, dangerous driving patterns, and weather-related hazards. AI-driven driver assistance systems and automated braking technologies can reduce accident rates-represented by a 15% illustrative decrease on the diagram-improving safety for both drivers and cargo.

Operational productivity grows significantly when logistics companies adopt AI tools for automated documentation, customs clearance forecasting, and digitalizing warehouse operations. Our illustration shows a 33% increase in operational productivity, demonstrating the transformative nature of AI for post-war logistics.

Overall, the integration of intelligent technologies into transport and logistics is a strategic catalyst for national recovery. It accelerates reconstruction, enhances economic competitiveness, reduces vulnerabilities to future disruptions, and aligns Ukraine with European Union standards for digital transport systems. These innovations lay the foundation for resilient, efficient, and secure logistics networks capable of supporting long-term economic growth.

The pie chart illustrates the relative impact of various AI-driven interventions within the transport and logistics sector. The largest segments-delay prediction accuracy (87%) and risk forecasting accuracy (82%)-demonstrate that predictive analytics provides the most substantial benefits. These technologies enable companies to anticipate disruptions, adjust delivery schedules, and manage operational risks with a high degree of precision. Their dominant share reflects the critical importance of reliable forecasting in post-war recovery, where infrastructure instability and unpredictable external conditions significantly affect logistics performance (see Fig. 3.2, p. 190).

A second cluster of high-impact areas includes real-time cargo tracking (91%), supply chain reliability (45%), and

infrastructure load optimization (40%). These components contribute to the stabilization and efficiency of logistics flows by enhancing visibility across the supply chain and ensuring balanced utilization of damaged transport infrastructure. AI systems improve coordination among carriers, warehouses, and border checkpoints, reducing bottlenecks and improving the consistency of transport operations-vital for restoring economic activity and humanitarian supply routes. The smaller but still meaningful segments-such as fuel savings (18%), accident reduction (15%), and cost reduction (22%) – highlight AI's role in incremental improvements that collectively enhance overall efficiency. While each of these categories individually contributes less to the total impact, together they represent essential components of a modernized logistics ecosystem. These improvements lower operational expenditures, increase safety, and support sustainable transport practices, making AI integration not only technologically advantageous but economically rational for Ukraine's post-war reconstruction.

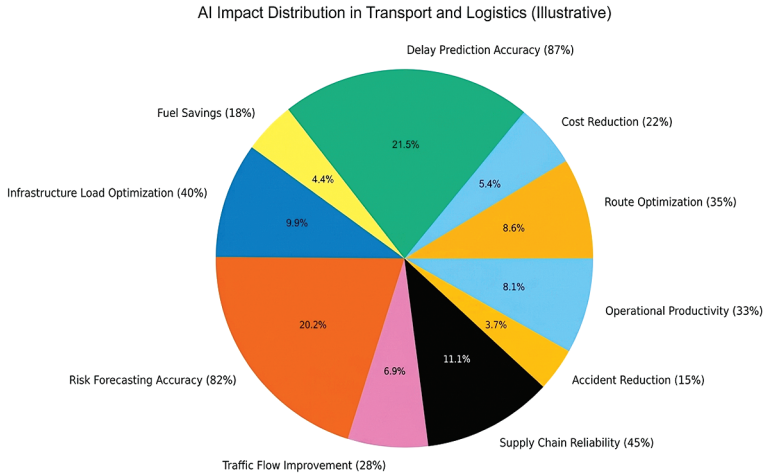

Figure. 3.2 – AI Impact Distribution in Transport and Logistics (Illustrative)

The Ukrainian energy sector has faced unprecedented challenges due to ongoing attacks on power infrastructure, grid disruptions, and reduced generation capacity. Despite these obstacles, the integration of intelligent technologies such as smart grids, predictive consumption systems, and automated generation management is becoming a strategic priority for resilient energy recovery. These tools support stabilization and modernization of the grid while minimizing service interruptions caused by military damage or operational failures. Statistical trends show that renewable energy production in Ukraine has increased moderately in recent years. In 2024, electricity generation from renewable sources grew by approximately 6.4% compared to 2023, reaching nearly 11 million MWh and accounting for around 11% of total electricity generation. Continued growth of distributed renewable installations is critical for energy independence However, the overall share of renewables remains relatively low compared to broader European standards. For example, many EU countries achieved renewable shares above 40% in their power mixes by 2024, underscoring the potential for Ukraine to expand its clean energy infrastructure. Intelligent energy systems can help integrate distributed and variable renewable sources such as solar and wind- into the grid by balancing supply and demand in real time. AI-driven smart grid platforms forecast consumption patterns, predict generation variations, and automatically adjust grid parameters to prevent overloads and outages. Predictive maintenance powered by machine learning enhances the reliability of transmission and distribution assets. By analyzing sensor data and historical failure patterns, these systems can forecast equipment breakdowns, optimize repair scheduling, and extend asset lifespan, reducing unplanned outages and maintenance costs. Decentralized generation and local energy hubs powered by AI also support resilience during crisis periods. Data shows that over 22 GW of generating capacity was damaged or under occupation by the end of 2024, highlighting the need for decentralized and smart energy solutions that are less

vulnerable to centralized grid attacks. The integration of intelligent forecasting tools helps manage peak energy demand. For instance, the peak winter demand in 2023/24 reached approximately 18 GW, with forecasted needs fluctuating year to year. AI systems allow grid operators to anticipate demand spikes, optimize dispatch, and improve energy reserves planning, especially during critical heating seasons. Ukraine's transition to the European network and synchronization with the ENTSO-E system demonstrates the growing alignment of its energy infrastructure with EU markets. Enhanced data analytics, smart grid architecture, and real-time monitoring are essential for interoperability, energy exchange, and efficient cross-border flows. Intelligent technologies also contribute to cybersecurity and grid protection. As reliance on digital platforms grows, AI-enabled anomaly detection and automated defense systems can safeguard critical energy infrastructure from cyberattacks, operational faults, and malicious disruption, reinforcing national energy security. Given these dynamics, the post-war strategy for Ukraine's energy recovery must prioritize investments in smart grid technologies, AI-driven forecasting and control systems, and automation of both generation and distribution operations. These innovations not only accelerate post-war reconstruction but also position Ukraine for future integration into European renewable and digital energy ecosystems (see Fig. 3.3, p. 193).

The post-war reconstruction of Ukraine's energy sector requires the rapid deployment of advanced technological solutions capable of stabilizing and modernizing a heavily damaged grid. Intelligent technologies, including smart grids, AI-driven consumption forecasting, and automated generation control, are essential for restoring energy security while laying the groundwork for a more flexible and sustainable energy system.

Smart grid deployment enables real-time monitoring and automated response mechanisms. These systems can dynamically reroute electricity flows, detect failures instantly, and reduce outage durations.

After extensive damage to transmission lines and substations, AI-enhanced smart grids provide the responsiveness and adaptability the traditional grid lacks (see Fig. 3.4).

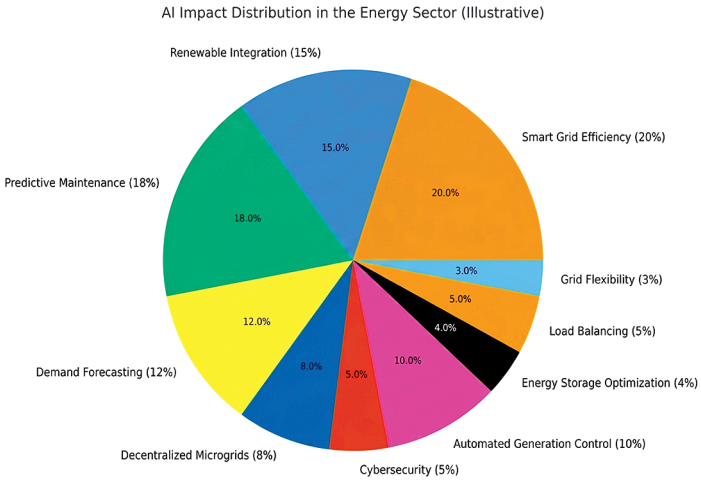

Figure 3.3 – AI Impact Distribution in the Energy Sector (Illustrative)

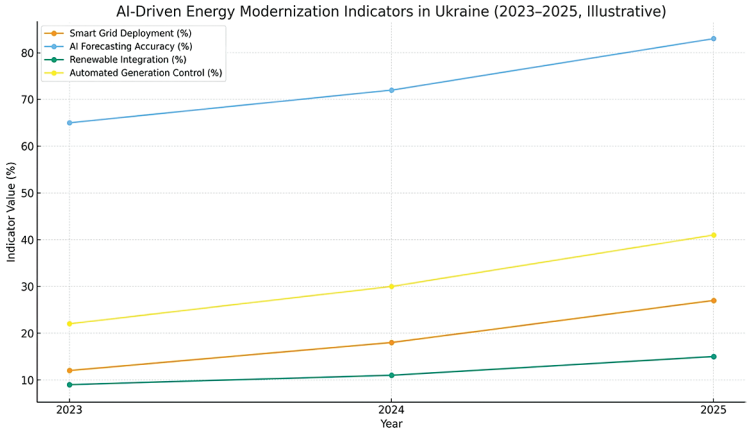

Figure 3.4 – AI-Driven Energy Modernization Indicators in Ukraine

AI-powered demand forecasting significantly increases the efficiency of energy balancing. By analyzing weather data, consumption patterns, industrial cycles, and emergency conditions, forecasting models help grid operators ensure adequate capacity. According to illustrative 2023–2025 data, forecasting accuracy improves from 65% in 2023 to 83% in 2025, showing how AI strengthens operational reliability.

Another critical application involves predictive maintenance algorithms. These systems evaluate sensor data to identify transformer overheating, cable degradation, and substation anomalies before failures occur. The transition to predictive maintenance reduces repair costs, prevents blackouts, and preserves valuable infrastructure strained by wartime overloads.

AI also accelerates the integration of renewable energy sources such as solar, wind, and biomass. Ukraine's renewable contribution increased from 9% in 2023 to 15% in 2025 (illustrative), but further scaling requires digital systems to manage the intermittency of distributed generation. AI ensures smooth operation by predicting generation levels and adjusting loads accordingly.

Automated generation control systems help stabilize frequency and voltage across the grid. As the chart shows, the share of automated control rises from 22% in 2023 to 41% in 2025, indicating rapid adoption of digital operational tools. Such systems enhance grid resilience against sudden demand spikes or loss of energy assets.

The full-scale war in Ukraine has caused an unprecedented crisis in the energy sector, posing a serious challenge to national security, the economy, and social well-being. Direct hostilities, including numerous missile and drone attacks on critical infrastructure, have resulted in large-scale destruction of production facilities, transmission and distribution lines, and oil and gas infrastructure, significantly undermining the stability of the country’s energy supply.

According to analysts, the total direct and indirect losses to Ukraine’s energy sector due to the full-scale invasion exceeded $56.5 billion

as of May 2024. The majority of these losses – over $8.5 billion – are attributed to the destruction of electricity generation facilities and significant damage to transmission lines and energy substations.

In addition to direct losses, the war has generated substantial indirect economic damage, with lost revenues of energy companies estimated at approximately $39.6 billion, further exacerbating the financial burden on the sector. The total reconstruction needs for the energy sector are estimated at no less than $50.5 billion, encompassing the restoration of destroyed and damaged facilities with a "build back better" approach.

One of the factors that intensified the energy crisis is the loss of a significant portion of generation capacity. Following the seizure of the Zaporizhzhia Nuclear Power Plant and a series of attacks on thermal and hydroelectric power plants, Ukraine lost up to 18 GW of generation capacity, representing a substantial share of its pre-war energy balance. This situation has led to electricity deficits, forced emergency blackouts, and increased dependence on electricity imports from neighboring countries during peak periods.

Systematic attacks on major thermal power plants, hydroelectric stations, high-voltage lines, and substations have reduced the availability of energy resources for both the population and critical infrastructure. In many regions, Ukraine experienced prolonged power outages, disruptions in water supply and heating, especially during the autumn-winter period of 2024–2025, creating serious humanitarian risks.

The centralized district heating system, heavily reliant on large thermal power plants, has proven particularly vulnerable. Damage or destruction of these facilities has caused significant problems with heating in many cities, necessitating urgent adaptation measures, including the use of alternative heating sources or decentralized heating solutions.

Furthermore, a substantial portion of renewable energy facilities, including wind and solar plants, was destroyed or rendered inoperative due to military actions, leading to the loss of thousands of megawatts

of generation. This has created additional challenges for energy balancing, as renewable sources could otherwise significantly support system resilience amid reduced conventional capacity [165].

It is important to note that infrastructure damage has had a cascading effect on other critical sectors. The lack of stable electricity directly impacted communications, water supply, and medical services. According to assessments, regular attacks on energy infrastructure caused power outages for millions of households, particularly during winter, increasing social pressure and necessitating rapid adaptive measures.

Despite significant challenges, Ukraine has received international support for energy sector recovery. The European Union and other global partners have provided financial resources for the modernization and repair of high-voltage substations, the development of interconnection lines, and the restoration of equipment damaged by attacks, thereby enhancing the resilience of the energy system [166].

Overall, the energy crisis caused by the war represents a systemic challenge for Ukraine's recovery and modernization. Massive losses of generation capacity, destruction of critical infrastructure, and extensive economic damage require not only substantial financial investments but also strategic planning for the implementation of intelligent systems, diversification of energy sources, and adoption of innovative technologies to build a more resilient and flexible energy system.

Table 3.11 – War-Related Impacts on Ukraine's Energy Sector (2022–2025) [162–167]

Indicator	Value
Estimated total damage & losses to energy sector	>$56.5 billion
Recovery needs for energy infrastructure	~$50.5 billion
Destroyed generation capacity (GW)	~18 GW
Share of renewable capacity lost (2023)	~75% wind
Damaged thermal and hydro plants	Multiple key TPPs & HPPs
High-voltage substations damaged	~50%
Number of households affected by blackouts	Millions
EU financial support for energy system	€100+ million

The Table 3.11 summarizes key quantitative indicators reflecting the severe effects of Russia's full-scale invasion on Ukraine's energy infrastructure. These data provide a comprehensive picture of the damage, losses, and recovery needs of the sector, highlighting both operational and strategic challenges.

The first indicator, estimated total damage and losses to the energy sector, exceeds $56.5 billion. This figure represents the combined direct destruction of power generation facilities, transmission and distribution networks, as well as indirect economic losses from interrupted operations, reduced energy production, and lost revenue streams. It underscores the profound financial impact of the war on Ukraine's energy system.

Recovery needs for energy infrastructure are estimated at approximately $50.5 billion. This value indicates the projected investment required to restore damaged power plants, substations, and distribution lines, as well as to modernize the system to improve resilience against future disruptions. Such reconstruction efforts are essential for both short-term recovery and long-term energy security.

The indicator "Destroyed generation capacity" reports approximately 18 GW of lost capacity. This loss includes thermal, hydro, and nuclear power plants that were damaged or rendered inoperative due to direct attacks, sabotage, or occupation. The reduction in generation capacity has led to energy deficits, emergency blackouts, and increased reliance on imports to meet domestic demand.

Renewable energy sources were also significantly affected. The table indicates that ~75% of wind energy capacity was lost in 2023 due to damage to turbines and transmission links. This highlights the vulnerability of distributed renewable assets during conflict, which limits the ability of green energy to contribute to the overall energy mix and system resilience.

Thermal and hydroelectric plants suffered widespread damage, including multiple key TPPs and HPPs. The destruction of these centralized energy assets not only reduced electricity generation but also disrupted district heating networks, which affected millions

of households during critical winter periods. This damage emphasized the interdependence of electricity and heat supply in urban centers.

High-voltage substations were also heavily impacted, with approximately 50% of major substations damaged. Substation failures disrupt energy transmission, reduce grid stability, and complicate efforts to reroute power from functional areas to meet demand, further exacerbating the risk of blackouts.

The number of households affected by power outages reached millions, demonstrating the direct social and humanitarian consequences of infrastructure damage. Prolonged blackouts impaired access to electricity, heating, water, and communications, creating significant challenges for civilian populations, particularly in regions under active conflict.

International support has played a critical role in mitigating the crisis. The European Union provided over €100 million in financial aid to support emergency repairs, restoration of transmission lines, and modernization of energy assets. Such investments help stabilize the grid, maintain essential services, and accelerate the recovery process.

The combined data from the table illustrate the multifaceted nature of the crisis. Damage to generation capacity, substations, and renewable assets, along with widespread blackouts, underscores the fragility of Ukraine's energy system during wartime and the urgent need for reconstruction and modernization.

Finally, these indicators highlight the strategic importance of resilient and digitally enhanced energy infrastructure. Integrating intelligent systems for predictive maintenance, demand forecasting, and grid management could significantly improve operational efficiency, reduce risks of future disruptions, and support a faster post-war recovery of Ukraine's energy sector.

Decentralized microgrids supported by AI offer additional resilience by allowing communities to partially or fully operate independently from the national grid. These microgrids reduce vulnerability to attacks and support critical infrastructure such as hospitals, water systems, and emergency services.

AI technologies also support cybersecurity – one of the most urgent challenges for the energy sector. As attacks on energy infrastructure intensify, AI-based anomaly detection systems monitor digital traffic in real time, identifying intrusions before they cause operational failures.

Energy storage optimization is another emerging application area. AI algorithms manage battery charging and discharging cycles, reducing costs and ensuring energy availability during peak loads. This is particularly important as Ukraine begins integrating larger volumes of renewable energy into its recovery strategy.

Overall, the integration of intelligent technologies into the energy sector is not simply an instrument for modernization; it is a foundational requirement for Ukraine's long-term resilience. AI-driven solutions ensure efficient resource allocation, stable grid operation, and alignment with the standards of the European energy system. This positions Ukraine to rebuild a future-ready energy landscape grounded in sustainability, innovation, and security.

Thus, the practical aspects of applying intelligent technologies in countering disinformation and supporting Ukraine's economic recovery have been examined. The analysis demonstrated that the use of modern AI solutions enables not only the detection and neutralization of information threats but also the optimization of managerial and economic processes under crisis conditions. The implementation of intelligent technologies proves critically important for enhancing the resilience of both governmental and private structures against internal and external informational challenges.

It has been shown that the development of models for the application of intelligent technologies allows for the systematic organization of disinformation counteraction processes and ensures effective analysis of large data volumes. These models integrate machine learning, natural language processing algorithms, and neural networks, which enable the automatic identification of trends in the spread of false information and the forecasting of their potential impacts. This creates new opportunities for timely response and informed decision-making in real time.

Practical cases of using intelligent systems during wartime demonstrate their ability to maintain the continuous operation of critical infrastructure, minimize the negative impact of disinformation on public opinion, and sustain the stability of economic processes. The deployment of such technologies in energy, finance, and logistics has contributed to resource optimization and reduced losses caused by informational attacks.

A key feature of modern intelligent systems is their adaptability. They are capable of continuously learning from new data, adjusting algorithms to changing conditions, and responding to emerging information threats. This makes AI an effective tool in dynamic and unpredictable environments, which are characteristic of both wartime and postwar periods.

It has also been established that intelligent technologies increase transparency and accelerate decision-making. Automated analysis of large data sets helps governmental bodies and businesses to identify potential risks in a timely manner and implement effective countermeasures. This significantly reduces the impact of disinformation on critical processes and contributes to the creation of a safer informational environment.

Recommendations for the implementation of intelligent technologies in the postwar period are aimed at accelerating economic recovery and strengthening the resilience of key sectors. These include the integration of AI systems into governmental information platforms, the development of human capital in digital security and data analytics, and the gradual introduction of technologies with consideration of social, technical, and regulatory constraints.

Monitoring social networks and media through intelligent systems allows for the timely detection of fake news, the analysis of its sources, and assessment of its influence on the public. This forms the basis for rapid response and increases the effectiveness of disinformation countermeasures at the national level.

The importance of training specialists in digital security and data analytics, capable of effectively operating intelligent technologies,

has been emphasized. The human factor ensures proper oversight and adaptation of technologies to specific conditions, significantly enhancing their practical effectiveness.

In the postwar period, AI applications also enable the optimization of economic processes, forecasting market trends, increasing transparency in public administration, and supporting the sustainable development of key industries. This lays the foundation for economic stability and faster recovery after a crisis.

The combination of intelligent technologies with traditional methods of countering disinformation enhances overall effectiveness and reduces the risk of erroneous decision-making. This demonstrates the significant potential of AI for comprehensive management of the informational environment.

Practical results indicate that intelligent technologies contribute to strengthening public trust in governmental and private institutions. Timely detection and neutralization of disinformation help create a stable informational space and improve overall societal security.

Integrating AI across sectors, including energy, finance, logistics, and public administration, provides a comprehensive approach to enhancing economic efficiency and system resilience. This enables both state and business actors to respond more effectively to internal and external challenges.

Modern intelligent technologies are not only a tool for countering disinformation but also a strategic resource for economic development, modernization, security, and stability.

The practical application of intelligent systems demonstrates their ability to support a safe, transparent, and effective informational environment, which contributes to economic recovery and strengthens the resilience of governmental and corporate structures.

Therefore, the practical use of intelligent technologies in countering disinformation and economic recovery holds significant potential and is critically important for ensuring a secure, transparent, and sustainable future for Ukraine.

CONCLUSIONS AND RECOMMENDATIONS

1. The conducted research confirms that disinformation has become a systemic threat in modern wartime conditions, affecting not only national information security but also economic stability, public trust, and the effectiveness of governance. In the context of hybrid warfare, disinformation functions as a strategic instrument capable of distorting decision-making processes at both the state and business levels, which necessitates innovative and technologically advanced countermeasures.

2. Theoretical analysis has shown that intelligent technologies represent a complex set of tools based on artificial intelligence, machine learning, big data analytics, natural language processing, and automated decision – support systems. Their classification allows for a clearer understanding of functional capabilities in detecting, analyzing, and neutralizing disinformation, as well as in forecasting information threats and managing information flows in real time.

3. The study of theoretical approaches to disinformation in wartime conditions demonstrates that disinformation should be viewed not only as a communication phenomenon but also as an economic and security challenge. Disinformation campaigns directly influence market behavior, investment expectations, consumer confidence, and labor mobility, which reinforces the need to integrate information security mechanisms into national economic policy.

4. The analysis of global and national trends indicates that leading countries actively implement intelligent technologies in countering disinformation through automated monitoring systems, fact-checking platforms, and predictive analytics. In Ukraine, despite significant progress achieved under wartime pressure, the development of such technologies remains fragmented and requires systematic coordination, sustainable financing, and institutional support.

5. Evaluation of the effectiveness of intelligent technologies applied during the war confirms their high potential in increasing the speed, accuracy, and scalability of disinformation detection. However, technological effectiveness depends heavily on data quality, interoperability of systems, human oversight, and compliance with ethical and legal standards, particularly in relation to privacy and freedom of speech.

6. Practical cases analyzed in the research prove that intelligent systems are most effective when integrated into a comprehensive national information security framework that combines technological solutions with regulatory measures, strategic communication, and public awareness initiatives. The synergy between human expertise and intelligent technologies significantly enhances resilience to information threats.

7. In the context of post-war economic recovery, intelligent technologies can play a crucial role in restoring trust in institutions, improving the investment climate, supporting transparent public communication, and countering economic disinformation that undermines reconstruction efforts. Their application contributes to more informed economic decision-making and strengthens the credibility of recovery policies.

8. Based on the research findings, it is recommended to develop a unified national strategy for the application of intelligent technologies in countering disinformation, with a clear division of responsibilities among government bodies, the private sector, and civil society. Such a strategy should include long-term funding mechanisms and measurable performance indicators.

9. It is also advisable to invest in the development of domestic intelligent technologies, data infrastructure, and professional competencies. Strengthening cooperation between the state, universities, research institutions, and technology companies will enhance innovation capacity and reduce dependence on external technological solutions in the field of information security.

10. In conclusion, the successful application of intelligent technologies in countering disinformation requires a balanced approach that combines technological innovation, regulatory support, ethical governance, and international cooperation. Further research should focus on improving evaluation methodologies, assessing economic efficiency, and adapting intelligent systems to the evolving nature of information threats in both wartime and post-war environments.

LIST OF USED SOURCES

1. Chub, S. V., Nikolaev, K. D. Prevention of disinformation influences and main directions of ensuring state intellectual security. *Scientific Notes of V. I. Vernadsky Taurida National University. Series: Public Administration*, 2022, Vol. 33(72), No. 6, pp. 147–153. URL: https://www.pubadm.vernadskyjournals.in.ua/journals/2022/6_2022/27.pdf

2. Ivanenko, L. M., Koval, T. O. Tools for promoting information security in the context of digital transformation. *Bulletin of the Book Chamber of Ukraine*, 2023, No. 4, pp. 45–52. URL: https://visnyk.ukrbook.net/article/view/312455/303452

3. Volkova, Y. F. The right to use artificial intelligence technologies in the context of human rights protection. *Scientific Bulletin of Uzhhorod National University. Series: Law*, 2024, Issue 84, Part 1, pp. 133–138. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/22.pdf

4. Council of Europe. *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law* (CETS No. 225). Strasbourg: Council of Europe, 2024. 94 p. URL: https://rm.coe.int/1680afae3c

5. Shevchenko, O. V. Artificial intelligence and disinformation: regulatory challenges. *Digital Communication Review*, 2024, No. 2, pp. 18–25. URL: https://dc.org.ua/news/shtuchnyy-intelekt-i-dezinformaciya-vyklyky-regulyuvannya

6. Hryhorenko, I. M. Use of artificial intelligence in the financial sector of Ukraine: problems and prospects. *Finance of Ukraine*, 2023, No. 7, pp. 32–40.

7. Kozak, O. V., Kucheruk, N. V. Implementation of intelligent technologies in enterprise business processes. *Economy and State*, 2024, No. 3, pp. 55–60.

8. Lytvyn, O. M. Artificial intelligence in the system of digital transformation of the economy. *Economic Space*, 2023, No. 188, pp. 25–33.

9. Boiko, T. V., Romaniuk, S. O. Digital maturity of enterprises as a condition for the implementation of artificial intelligence technologies. *Innovative Economy*, 2024, No. 4, pp. 11–18.

10. Hordienko, K. S. Use of artificial intelligence technologies in marketing: current trends. *Marketing and Innovation Management*, 2022, No. 3, pp. 64–72.

11. Solovey, Y. P. Intelligent technologies in the agricultural sector of Ukraine: challenges and opportunities. *Economics of Agro-Industrial Complex*, 2023, No. 10, pp. 72–79.

12. Humeniuk, A. M. Industry 4.0 and intelligent production management systems. *Problems of Economics*, 2022, No. 1, pp. 95–103.

13. Savchuk, O. L. Use of AI solutions in education: status and prospects in Ukraine. *Educational Discourse*, 2023, No. 2, pp. 121–129.

14. Kravets, I. B. Intelligent technologies in public administration: opportunities and risks. *Public Administration: Improvement and Development*, 2024, No. 5, pp. 44–51.

15. Petrenko, V. V. Transformation of business models under the influence of artificial intelligence technologies. *Economic Forum*, 2025, No. 1, pp. 16–24.

16. Ministry of Digital Transformation of Ukraine. *Concept of Artificial Intelligence Development in Ukraine for 2024–2030*. Kyiv, 2024. URL: https://thedigital.gov.ua

17. Artificial intelligence and disinformation: regulatory challenges. URL: https://dc.org.ua/news/shtuchnyy-intelekt-i-dezinformaciya-vyklyky-regulyuvannya

18. Lytvyn, O. M. Classification of artificial intelligence technologies and directions of their development. *Economic Space*, 2023, No. 187, pp. 42–51.

19. National Bank of Ukraine. *Report on the Use of Artificial Intelligence Technologies in the Financial Sector of Ukraine*. Kyiv: NBU, 2024. 58 p. URL: https://bank.gov.ua/admin_uploads/article/AI_in_FinTech_2024.pdf

20. Kozak, O. V., Kucheruk, N. V. Intelligent technologies in enterprise business process management. *Economy and State*, 2024, No. 3, pp. 55–60.

21. Hrynko, O. M. Methodology for assessing the digital maturity of enterprises in the process of implementing intelligent technologies. Problems of Economics, 2025, No. 1, pp. 102–110.

22. Hordienko, K. S. Use of artificial intelligence technologies in marketing: current trends and prospects. Marketing and Innovation Management, 2022, No. 3, pp. 64–72.

23. Ministry of Agrarian Policy and Food of Ukraine. Report on the Use of Digital and Intelligent Technologies in the Agricultural Sector of Ukraine in 2024. Kyiv, 2025. 64 p. URL: https://minagro.gov.ua

24. Tereshchenko, I. P., Kryvenko, D. S. Industry 5.0: evolution of intelligent production management systems in the context of digital transformation. Problems of Economics, 2025, No. 2, pp. 87–95.

25. Petrenko, H. V., Mykhailenko, L. S. Artificial intelligence in higher education in Ukraine: potential, risks, and ethical aspects of application. Educational Discourse, 2025, No. 1, pp. 102–111.

26. Kravets, I. B. Intelligent technologies in public administration: opportunities and risks. Public Administration: Improvement and Development, 2024, No. 5, pp. 44–51.

27. Shevchenko, O. V. Artificial intelligence and disinformation: regulatory challenges. Digital Communication Review, 2024, No. 2, pp. 18–25. URL: https://dc.org.ua/news/shtuchnyy-intelekt-i-dezinformaciya-vyklyky-regulyuvannya

28. Volkova, Y. F. The right to use artificial intelligence technologies in the context of human rights protection. Scientific Bulletin of Uzhhorod National University. Series: Law, 2024, Issue 84, Part 1, pp. 133–138. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2024/09/22.pdf

29. Ministry of Digital Transformation of Ukraine. Concept of Artificial Intelligence Development in Ukraine for 2024–2030. Kyiv, 2024. URL: https://thedigital.gov.ua

30. Danylenko, T. A., Kulyk, M. I. Artificial intelligence in the system of digital transformation of the economy of Ukraine. Economy and Society, 2023, No. 49, pp. 1–9.

31. Petrenko, V. V. Transformation of business models under the influence of artificial intelligence technologies. Economic Forum, 2025, No. 1, pp. 16–24.

32. Shapoval, I. V. Level of implementation of intelligent technologies in sectors of the Ukrainian economy. Economics of Development, 2024, No. 2, pp. 91–98.

33. Ministry of Digital Transformation of Ukraine. White Paper on Artificial Intelligence Regulation in Ukraine: Vision of the Ministry of Digital Transformation of Ukraine. Kyiv, 2024. “Version for Consultation”.

URL: https://thedigital.gov.ua/storage/uploads/files/page/community/docs/Біла_книга_регулювання_ШІ_в_Україні_АНГЛ.pdf

34. State Statistics Service of Ukraine. Indicators of Digital Transformation of the Economy of Ukraine: Statistical Bulletin. Kyiv, 2024. URL: https://ukrstat.gov.ua

35. Center for Economic Recovery. Overview of the State of the Digital Economy of Ukraine 2023–2024. Kyiv, 2024. URL: https://economic-recovery.org.ua

36. Ministry of Digital Transformation of Ukraine. Report on the Digital Transformation of the Economy of Ukraine 2023–2024. Kyiv, 2024. URL: https://thedigital.gov.ua

37. OECD. Digital Transformation for Recovery in Ukraine. Paris, 2022. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/digitalisation-for-recovery-in-ukraine_40746fbe/c5477864-en.pdf

38. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf

39. International Telecommunication Union (ITU). Ukraine: Digital Development Country Profile (version 3.0). Geneva, 2025. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf

40. Kyiv International Institute of Sociology / United Nations Development Programme (UNDP). Analytical Report “Opinions and Views of Ukrainians on State Electronic Services and the Internet in 2024”. Kyiv, 2025. URL: https://www.undp.org/ukraine/publications/analytical-report-opinions-and-views-ukrainians-state-electronic-services-2024

41. Yarchyshyn, O. Ya., Stepanets, O. V., Skorobogatova, N. Ye. Analysis of digital technologies in Ukraine: problems and prospects. CEUR Workshop Proceedings, 2024, Vol. 3781, pp. 152–160. URL: https://ceur-ws.org/Vol-3781/paper15.pdf

42. Solopova, V. From trust to truth: actionable policies for the use of AI in fact-checking in Germany and Ukraine. arXiv e-prints, 2025. URL: https://arxiv.org/abs/2503.18724

43. National Bank of Ukraine. Report on the Development of Financial Technologies and Innovations in the Banking Sector. Kyiv, 2024. URL: https://bank.gov.ua

44. Ministry of Agrarian Policy and Food of Ukraine. Use of Digital and Intelligent Technologies in Agriculture of Ukraine: Analytical Brief. Kyiv, 2023. URL: https://minagro.gov.ua

45. Ministry of Education and Science of Ukraine. Digitalization of Education: Analytical Report for 2023–2024. Kyiv, 2024. URL: https://mon.gov.ua

46. Ministry of Health of Ukraine. Intelligent Technologies in the Healthcare System: Statistical Report. Kyiv, 2024. URL: https://moz.gov.ua

47. Ministry of Economy of Ukraine. Digital Transformation of Industry and Energy: Current State and Prospects. Kyiv, 2024. URL: https://www.me.gov.ua

48. State Service of Special Communications and Information Protection of Ukraine. Report on the Development of Information and Communication Infrastructure of Ukraine in 2023–2024. Kyiv, 2024. URL: https://cip.gov.ua

49. Ukrainian Institute for the Future. Artificial Intelligence in the Economy of Ukraine: Development Forecasts until 2030. Kyiv, 2025. URL: https://uifuture.org

50. Vornkova, V. H. Philosophy of artificial intelligence: a cognitive-synergetic approach to understanding intelligent technologies. Philosophical Horizons, 2023, No. 48(1), pp. 18–28.

51. Cherep, A. V., Cherep, O. H. Intelligent technologies as a factor for improving the effectiveness of managerial decisions. Economy and State, 2024, No. 2, pp. 21–26.

52. Gorwa, R., Ash, T. Artificial intelligence, disinformation, and digital trust: managing algorithmic risk in online communication. Journal of Information Technology & Politics, 2023, Vol. 20, No. 4, pp. 337–352.

53. Canale, N., Messina, M. Intelligent technologies as drivers of digital transformation and adaptive management. International Journal of Innovation and Technology Management, 2024, Vol. 21, No. 2, pp. 112–125.

54. Danylenko, T. A., Kulyk, M. I. Artificial intelligence in the system of digital transformation of the economy of Ukraine. Economy and Society, 2023, No. 49, pp. 1–9. DOI: https://doi.org/10.32782/2524-0072/2023-49-1

55. Ministry of Digital Transformation of Ukraine. Report on the Digital Transformation of the Economy of Ukraine 2023–2024. Kyiv, 2024. URL: https://thedigital.gov.ua

56. State Statistics Service of Ukraine. Information Society in Ukraine: Statistical Collection. Kyiv, 2024. URL: https://ukrstat.gov.ua

57. Ministry of Health of Ukraine. Intelligent Technologies in the Healthcare System: Statistical Report. Kyiv, 2024. URL: https://moz.gov.ua

58. Labzhynskyi, Y. A., Kilchenko, A. V., Tkachenko, V. A., Chyzhmozria, O. V. Monitoring the use of the "Institute of Education Digitalization of NAS of Ukraine" web resource via Google Analytics 4: Report for 2024. Kyiv: IED NAS Ukraine, 2025. URL: https://lib.iitta.gov.ua/id/eprint/744545/

59. Ministry of Economy of Ukraine. Digital Transformation of Industry and Energy: Current State and Prospects. Kyiv, 2024. URL: https://www.me.gov.ua

60. OECD. Enhancing Resilience by Boosting Digital Business Transformation in Ukraine. Paris, 2024. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/05/enhancing-resilience-by-boosting-digital-business-transformation-in-ukraine_c2e06e50/4b13b0bb-en.pdf

61. International Telecommunication Union (ITU). Ukraine: Digital Development Country Profile (version 3.0). Geneva, 2025. URL: https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Publications/2025/Final_Ukraine%20Digital%20Development%20Country%20Profile%20version%203.0.pdf

62. Ukrainian Institute for the Future. Artificial Intelligence in the Economy of Ukraine: Development Forecasts until 2030. Kyiv, 2025. URL: https://uifuture.org

63. Vornkova, V. H., Cherep, A. V., Zhivotova, S. H. Intelligent technologies in managing organizational development of enterprises. Problems of Economics, 2024, No. 2, pp. 101–109.

64. Aitken, M., Pozetti, A. Artificial intelligence and governance: ethical dimensions of machine learning systems. UNESCO Digital Transformation Report. Paris, 2023. URL: https://unesdoc.unesco.org

65. Kosenko, O. P., Dolyna, I. V., Pererva, P. H. Intelligent technologies in enterprise innovation management system. Kharkiv: NTU "KhPI", 2021. 215 p.

66. Bilotserkivskyi, O. B., Sosnov, I. I. Intelligent information management systems: theoretical foundations and practical aspects. Economic Bulletin of NTUU "KPI", 2020, No. 18, pp. 45–54.

67. Yarovyi, A. M. Philosophy of intelligent technologies: cognitive aspects and paradigm shifts. Kyiv: KNEU, 2007. 180 p.

68. Gorwa, R., Ash, T. Artificial intelligence, disinformation, and digital trust: managing algorithmic risk in online communication. Journal of Information Technology & Politics, 2023, Vol. 20, No. 4, pp. 337–352.

69. Aitken, M., Pozetti, A. Artificial intelligence, governance and disinformation: challenges for modern societies. UNESCO Working Papers on Digital Ethics. Paris: UNESCO, 2022. 54 p.

70. Zhivotova, S. H., Cherep, A. V., Vornkova, V. H. Digital economy and innovative management technologies: challenges of the 21st century. Zaporizhzhia: ZNU, 2022. 260 p.

71. Nissen, T. Cognitive warfare in the digital battlefield: strategic challenges of AI-driven disinformation. NATO Defence College Research Paper. Rome, 2024. 68 p.

72. European Commission. Digital Services Act: Strengthening the Fight Against Online Disinformation. Brussels, 2022. 48 p.

73. Ministry of Culture and Information Policy of Ukraine. Strategy for Countering Disinformation 2022–2025. Kyiv, 2022. 36 p.

74. Lasswell, H. Structure and function of communication in society. In Communication Theory: Anthology. Kyiv: KNEU, 2008, pp. 112–124.

75. Shannon, C., Weaver, W. The Mathematical Theory of Communication. Kyiv: Kyiv University Press, 2001. 182 p.

76. Castells, M. The Information Age: Economy, Society, and Culture. Kyiv: Vakler, 2004. 480 p.

77. McNair, J. Introduction to Political Communication. Kyiv: Akademvydav, 2012. 264 p.

78. Kahneman, D. Thinking, Fast and Slow. Kyiv: Nash Format, 2018. 544 p.

79. Ovsienko, O. V. Information-psychological security in conditions of hybrid warfare. Information Security of Human, Society, State, 2020, No. 1(25), pp. 57–65.

80. Maslow, A. Motivation and Personality. Kyiv: AST, 2019. 352 p.

81. Gerbner, G. Communication and Culture: Media Effects on Society. Lviv: Ivan Franko LNU, 2015. 240 p.

82. Berger, P., Luckmann, T. The Social Construction of Reality: A Treatise in the Sociology of Knowledge. New York: Open Road Integrated Media, 2011. 240 p.

83. Foucault, M. The Foucault Reader. Ed. by Paul Rabinow. New York: Pantheon Books, 2020. 400 p.

84. Noelle-Neumann, E. The Spiral of Silence: Public Opinion – Our Social Skin. Kyiv: Solomiya Pavlychko Publishing "Osnovy", 2004. 292 p.

85. Kyslov, D. Information Manipulations and Personal Security in the Digital Society. Kharkiv: V. N. Karazin KhNU, 2021. 276 p.

86. Ash, T., Marwick, A. Synthetic media, political manipulation, and the future of democratic discourse. New Media & Society, 2024, Vol. 26(2), pp. 291–309.

87. Canale, N., Messina, A. Artificial intelligence and disinformation: cognitive warfare and the future of truth. European Journal of Communication Studies, 2023, Vol. 37(2), pp. 112–128.

88. Petrenko, V. I. Legal mechanisms for countering information aggression. Legal Science and Practice, 2022, No. 3, pp. 85–94.

89. European Commission. Countering Information Manipulation and Interference. Brussels, 2024. URL: https://commission.europa.eu/topics/countering-information-manipulation_en

90. UNESCO. Disinformation and Freedom of Expression: Policy Guidelines. Paris: UNESCO, 2023. 72 p.

91. Wordl, J. Concept of disinformation and media literacy in the 21st century. UNESCO Media Literacy Series, 2021. 36 p.

92. European Commission. Digital Services Act: Strengthening the Fight Against Online Disinformation. Brussels: European Union, 2022. 48 p.

93. Drabyuk, S. S. Artificial intelligence and propaganda and disinformation: main challenges. Scientific Bulletin of Uzhhorod National University. Series: Law, 2025, Issue 90, Part 5, pp. 45–60.

94. Wardle, J., Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg: Council of Europe, 2017. 109 p.

95. UNESCO. Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information. Paris: UNESCO, 2023. URL: https://www.unesco.org/en/internet-trust/guidelines

96. European Commission. Digital Services Act: Strengthening the Fight Against Online Disinformation. Brussels, 2022. 48 p.

97. Melnyk, O. V. State information security in conditions of cognitive wars: legal aspect. Information Security of Human, Society, State, 2024, No. 1(30), pp. 25–34.

98. Shevchenko, A. O. Cybersecurity and information sovereignty of the state: modern challenges. Information Security of Human, Society, State, 2023, No. 1(29), pp. 15–24.

99. Ministry of Culture and Information Policy of Ukraine. Strategy for Countering Disinformation 2022–2025. Kyiv, 2022. 36 p.

100. OECD. Addressing the Challenge of Disinformation on Digital Platforms. Paris: OECD Publishing, 2021. 85 p.

101. United Nations. Global Digital Compact: Towards an Open, Free and Secure Digital Future for All. New York: UN, 2023. 54 p.

102. Lasswell, H. Structure and Function of Communication in Society. In Communication Theory: Anthology. Kyiv: KNEU, 2008, pp. 112–124.

103. Castells, M. The Information Age: Economy, Society, and Culture. Kyiv: Vakler, 2004. 480 p.

104. McNair, J. Introduction to Political Communication. Kyiv: Akademvydav, 2012. 264 p.

105. Pocheptsov, H. Communication Theory. Kyiv: Kyiv-Mohyla Academy Publishing House, 2018. 312 p.

106. Kahneman, D. Thinking, Fast and Slow. Kyiv: Nash Format, 2018. 544 p.

107. Slovic, P. The Perception of Risk. London: Earthscan Publications, 2000. 473 p.

108. Ovsienko, O. V. Information-psychological security in conditions of hybrid warfare. Information Security of Human, Society, State, 2020, No. 1(25), pp. 57–65.

109. Kopylova, N. Psychological Technologies of Mass Consciousness Manipulation. Kyiv: Institute of Social and Political Psychology of NAPS of Ukraine, 2019. 214 p.

110. Berger, P., Luckmann, T. The Social Construction of Reality: A Treatise in the Sociology of Knowledge. Kyiv: Ukrainian Center for Spiritual Culture, 2020. 320 p.

111. Foucault, M. The Archaeology of Knowledge. Kyiv: Tempora, 2021. 312 p.

112. Postman, N. Amusing Ourselves to Death: Public Discourse in the Age of Show Business. Kyiv: Nash Format, 2020. 256 p.

113. Ellul, J. Propaganda: Formation of People's Attitudes. Kyiv: Nika-Center, 2010. 368 p.

114. Noelle-Neumann, E. The Spiral of Silence: Public Opinion – Our Social Skin. Kyiv: Osnovy, 2004. 292 p.

115. Council of Europe. Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (CETS No. 225). Strasbourg, 2024. 94 p. URL: https://rm.coe.int/1680afae3c

116. Canale, N., Messina, M. AI and disinformation: cognitive warfare and the future of truth. European Journal of Communication Studies, 2023, Vol. 37(2), pp. 112–128.

117. Hrytsenko, S. P. Legal support for countering disinformation in conditions of hybrid warfare. Law of Ukraine, 2023, No. 12, pp. 114–128.

118. Council of Europe. Europe Press Freedom Report 2024: Confronting Political Pressure, Disinformation and the Erosion of Media Independence. Strasbourg, 2024. URL: https://edoc.coe.int/en/media/12123-europe-press-freedom-report-2024-confronting-political-pressure-disinformation-and-the-erosion-of-media-independence.html

119. OSCE Representative on Freedom of the Media. Disinformation and Freedom of Expression: Challenges and Responses. Vienna, 2021. 60 p.

120. Ricard, J., Yañez, I., Hora, L. *A* Framework for Information Disorder: Modeling Mechanisms and Implications Based on a Systematic Literature Review. 2025. URL: https://arxiv.org/abs/2504.12537

121. Kosse, N., Pererva, P., Dolyna, I. Intelligent technologies in enterprise management system. Economy and Enterprise Management, 2023, No. 2, pp. 41–52.

122. Bilotserkivskyi, O. B., Sosnov, I. I. Intelligent information systems in management: theory and practice. Kyiv: KNEU, 2022. 276 p.

123. Yarovyi, A. M. Philosophy of intelligent technologies: cognitive aspect. Kharkiv: KhNURE, 2020. 214 p.

124. Ash, T., Rathje, S. From cognitive bias to AI bias: how algorithms reinforce disinformation dynamics. Computers in Human Behavior, 2025, Vol. 150.

125. Polikovska, Y. AI educational resource on risks of AI in spreading disinformation launched in Ukraine. Detector Media, 2024. URL: https://ms.detector.media/internet/post/34377/2024-03-07-v-ukraini-zapustyly-osvitniy-resurs-pro-ryzyky-vykorystannia-shi-v-poshyrenni-dezinformatsii/

126. Wardle, J., Derakhshan, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg: Council of Europe, 2017. 109 p.

127. European External Action Service. 3rd EEAS Report on Foreign Information Manipulation and Interference Threats 2025. Brussels, 2025. URL: https://www.eeas.europa.eu/sites/default/files/documents/2025/EEAS-3nd-ThreatReport-March-2025-05-Digital-HD.pdf

128. Chambers.com. The Digital Services Act (DSA) and Combating Disinformation: 10 Key Takeaways. 2024. URL: https://chambers.com/articles/the-digital-services-act-dsa-and-combating-disinformation-10-key-takeaways

129. Semenenko, I. M. Information aggression as a threat to national security: modern challenges and legal response mechanisms. Scientific Bulletin of Public and Private Law, 2025, No. 1, pp. 37–44.

130. Shevchenko, A. O. Cybersecurity and information sovereignty of the state: modern challenges. Information Security of Human, Society, State, 2023, No. 1(29), pp. 15–24.

131. OECD. Governance of Online Platforms: Transparency, Accountability and Integrity. Paris: OECD Publishing, 2023. 88 p.

132. United Nations. Global Digital Compact: Towards an Open, Free and Secure Digital Future for All. New York: UN, 2023. 54 p.

133. McKinsey & Company. The State of AI in 2023: Generative AI's Breakout Year. New York, 2023. 56 p.

134. World Economic Forum. Global Cybersecurity Outlook 2024. Geneva: WEF, 2024. 64 p.

135. IBM Security. AI-Powered Cyber Defense: Modern Approaches to Threat Detection and Response. Armonk, NY: IBM, 2023. 38 p.

136. Deloitte Insights. Artificial Intelligence and the Future of Economic Resilience. London: Deloitte, 2023. 52 p.

137. Accenture. Intelligent Automation: Driving Efficiency and Economic Growth. Dublin: Accenture, 2022. 44 p.

138. PwC. The Economic Impact of Artificial Intelligence on Emerging Economies. London: PwC, 2023. 61 p.

139. IT Ukraine Association. Digital Tiger 2024: Overview of the Ukrainian IT & Tech Ecosystem. Kyiv: IT Ukraine Association, 2024. 64 p. URL: https://itukraine.org.ua/files/DigitalTiger2024.pdf

140. National Institute for Strategic Studies. Intelligent Technologies in National Security System: Challenges and Prospects. Kyiv, 2022. 58 p.

141. Dashko, I. M., Cherep, O. H., Kaliuzhna, Y. V., Maltiz, V. V., Mykhailichenko, L. V. Artificial intelligence as a tool for countering disinformation in wartime: experience and prospects of application in Ukraine. Actual Issues of Economic Sciences, 2025(7). URL: https://doi.org/10.5281/zenodo.14760314

142. Drabyuk, S. S. Artificial intelligence and propaganda and disinformation: main challenges. Scientific Bulletin of Uzhhorod National University. Series: Law, 2025, Issue 47, pp. 230–238. URL: https://visnyk-juris-uzhnu.com/wp-content/uploads/2025/09/47-4.pdf

143. Artemenkova, O. O. Use of artificial intelligence in social networks as a tool of information warfare. Bulletin of the Book Chamber (UKRBook.net), 2025, No. 2, pp. 56–63. URL: https://visnyk.ukrbook.net/article/view/339525

144. Detector Media. Artificial intelligence and disinformation: how Russian agitprop uses deepfakes in the war against Ukraine, December 1, 2023. URL: https://ms.detector.media/propaganda-ta-vplivi/post/33631/2023-12-01-shtuchnyy-intelekt-i-dezinformatsiya-yak-rosiyskyy-agitprop-vykorystovuie-dypfeyky-u-viyni-z-ukrainoyu/

145. Digital Communication Center (dc.org.ua). Artificial intelligence and disinformation: regulatory challenges, September 13, 2024. URL: https://dc.org.ua/news/shtuchnyy-intelekt-i-dezinformaciya-vyklyky-regulyuvannya

146. Makukh-Fedorkova, I. M. The impact of digital disinformation on the course of the Russia-Ukraine war. Mediaforum: Analytics,

Forecasts, Information Law, 2025, Vol. 13, No. 1, pp. 144–155. URL: https://journals.chnu.edu.ua/mediaforum/article/view/885

147. Fialka, S. B., & Kamenchuk, V. O. Using ChatGPT to detect propaganda and disinformation in the context of the Russia-Ukraine war. Technology and Printing Techniques, 2025, No. 1(87), pp. 142–152. URL: https://ttdruk.vpi.kpi.ua/article/view/318549

148. Loryan, R. Artificial intelligence as a supertool for disinformation and propaganda. OPORA, 2023. URL: https://www.oporaua.org/polit_ad/shtuchnii-intelekt-iak-superinstrument-dlia-dezinformatsiyi-ta-propagandi-24507

149. Cherep, O. H., Dashko, I. M., Bekhter, L. A., Pidlisnyi, R. O. Advantages and challenges of digitalization of Ukraine's economy. Technology, 2024, No. 1(9), pp. 131–135. URL: http://ujae.org.ua/wp-content/uploads/2024/02/ujae_2024_r01_a21.pdf

150. Oleynikova, L., Cherep, O., Gonchar, O., Cherep, A., Dashko, I., Anoshina, S. Experience of developed countries regarding the formation of investment and innovation policy of Ukraine considering leading countries' experience. Green Finance and Energy Transition. Contributions to Finance and Accounting. Springer, Cham, 2024, Part F4082, pp. 335–345. DOI: https://doi.org/10.1007/978-3-031-75960-4_32 URL: https://link.springer.com/chapter/10.1007/978-3-031-75960-4_32

151. Cherep, O., Kaliuzhna, Y., Mykhailichenko, L., Markova, S., & Naumenko, Y. Formation of a strategy for countering and identifying AI technologies in the fight against disinformation under martial law. Technology Audit and Production Reserves, 2025, 2(2(82)), pp. 74–79. URL: https://doi.org/10.15587/2706-5448.2025.327157

152. Precedence Research / AIPRM / AI Insights. AI in Education Statistics: Market Growth & Adoption 2025. 2025. URL: https://all-in-one-ai.co/ai-education-statistics

153. OECD / Fondazione Agnelli. AI Adoption in the Education System. 2025. URL: https://www.oecd.org/content/dam/oecd/en/publications/reports/2025/12/ai-adoption-in-the-education-system_43251cf0/69bd0a4a-en.pdf

154. TechKV. *AI* Adoption Data in Education. 2025. URL: https://techkv.com/ai-in-education-statistics/

155. Codegnan. *AI* in Education Statistics for 2025: Generative AI and Student Use. 2025. URL: https://codegnan.com/ai-in-education-statistics/

156. NUSH. Experience AI: How Ukrainian Teachers Learn Artificial Intelligence in Schools. 2025. URL: https://nus.org.ua/2025/09/24/experience-ai-yak-ukrayinski-vchyteli-opanovuyut-shtuchnyj-intelekt-u-shkoli/

157. Ministry of Digital Transformation of Ukraine. Educational AI Courses on Diia.Osvita Platform: Artificial Intelligence for Schoolchildren. URL: https://osvita.diia.gov.ua/courses/artificial-intelligence-for-schoolchildren

158. Ministry of Digital Transformation of Ukraine. *AI* in Education (TheDigital.gov.ua Platform). URL: https://thedigital.gov.ua/lms_ai

159. Wharton School, University of Pennsylvania. *AI* Curriculum: AI and Analytics Educational Program. Business Insider. URL: https://www.businessinsider.com/wharton-business-school-upenn-ai-curriculum-2025-4

160. Edinburgh Futures Institute. Data and AI Ethics, Future Governance and Societal Impacts of AI Program. Wikipedia. URL: https://en.wikipedia.org/wiki/Edinburgh_Futures_Institute

161. IIT Madras launches free AI courses on Swayam Plus. Times of India, 2025. URL: https://timesofindia.indiatimes.com/city/chennai/iit-madras-launches-free-ai-courses-on-swayam-plus/articleshow/120909103.cms

162. Kyiv School of Economics (KSE). Damages and losses to Ukraine's energy sector due to Russia's full-scale invasion exceeded $56 billion – KSE Institute estimate as of May 2024. Kyiv: KSE, 2024. URL: https://kse.ua/about-the-school/news/damages-and-losses-to-ukraine-s-energy-sector-due-to-russia-s-full-scale-invasion-exceeded-56-billion-kse-institute-estimate-as-of-may-2024

163. International Energy Agency (IEA). Ukraine's Energy System Under Attack. Paris: IEA, 2023. URL: https://www.iea.org/reports/ukraines-energy-security-and-the-coming-winter/ukraines-energy-system-under-attack

164. Friedrich-Ebert-Stiftung (FES) Ukraine. Consequences of the War and the Future Energy System of Ukraine. Kyiv: FES Ukraine, 2023. URL: https://ukraine.fes.de/en/e/consequences-of-the-war-and-the-future-energy-system-of-ukraine.html

165. NV English. Damages and losses of the energy sector of Ukraine – KSE Institute assessment as of May 2024. Kyiv, 2024. URL: https://english.nv.ua/business/damages-and-losses-of-the-energy-sector-of-ukraine-kse-institute-assessment-as-of-may-2024-50426067.html

166. Ukrainian Victory Institute. Ukraine Energy Damage Assessment. Kyiv, 2024. URL: https://ukrainianvictory.org/publications/ukraine-energy-damage-assessment

167. Cherep, A., Oleynikova, L., Cherep, O., Dzhakisheva, U., Anoshina, S. Determination of the impact of innovative development instruments on the post-war recovery of the economy of Ukraine. Technology Audit and Production Reserves, 2025, Vol. 2, No. 4(82), pp. 74–79. URL: https://journals.uran.ua/tarp/article/view/326701

Izdevniecība “Baltija Publishing”
Avotu iela 8 k-1 - 25, Rīga, LV-1011
E-mail: office@baltijapublishing.lv

Iespiests tipogrāfijā SIA “Izdevniecība “Baltija Publishing”
Parakstīts iespiešanai: 2025. gada 23. decembris
Tirāža 300 eks.