e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

https://www.eu-scientists.com/index.php/sdel

Digital Technologies as Key Vectors of Modernization of Ukraine's Military-Industrial Potential

Andriy Shakhovets [1] *

[1] *State University "Kyiv Aviation Institute" (Ukraine). PhD Student at the Department of International Economic Relations.*

*** *Corresponding Author,*** e-mail: shah.andriy@gmail.com

ARTICLE INFO

Research Article

DOI: 10.70651/3083-6018/2026.5.17

Received:
7 April 2026
Accepted:
10 May 2026
Published online:
12 May 2026

ABSTRACT

The article examines the role of digital technologies as key vectors for the modernization of Ukraine's military-industrial potential under conditions of full-scale war and global transformations in the security environment. It is substantiated that digitalization has become one of the main factors determining the effectiveness, adaptability, and technological resilience of the defense-industrial complex. The study analyzes contemporary trends in the digital transformation of the defense sector, including the implementation of artificial intelligence systems, automated command and control platforms, digital logistics solutions, cyber defense mechanisms, unmanned technologies, and digital twins in production and military planning processes. Special attention is devoted to the development of Ukraine's military-tech ecosystem during 2020–2025, particularly the activities of the BRAVE1 platform, the integration of DELTA and Kropyva situational awareness systems, and the introduction of electronic services such as Army+ and Reserve+. The article demonstrates that the use of digital instruments significantly improves operational decision-making, increases transparency of logistics and procurement processes, enhances coordination between military and civilian institutions, and strengthens the integration of Ukraine into international defense and technological cooperation. The research identifies the main barriers to digital transformation of the military-industrial complex, including fragmented management approaches, insufficient financial support, a shortage of highly qualified personnel, cyber threats, dependence on imported technologies and electronic components, and the absence of a unified digital policy framework. The consequences of damaged industrial infrastructure and unstable logistics during wartime are also highlighted as critical challenges limiting the pace of digital modernization. The article substantiates priority directions for further digital development of Ukraine's defense-industrial complex, such as the creation of an integrated digital infrastructure, implementation of PLM, ERP and MES systems, expansion of cyber resilience mechanisms, development of artificial intelligence technologies, support for defense-tech startups, and strengthening international technological partnerships with NATO and EU member states. It is concluded that digitalization should be considered not only as a technological upgrade but also as a strategic process aimed at ensuring technological sovereignty, strengthening national security, increasing the competitiveness of the defense industry, and forming an innovative and sustainable defense ecosystem in Ukraine.

KEYWORDS

digitalization, military-industrial complex, defense-industrial potential, digital technologies, artificial intelligence, cybersecurity, digital transformation, defense industry, military innovations, technological autonomy.

e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

https://www.eu-scientists.com/index.php/sdel

Цифрові технології як ключові вектори модернізації військово-промислового потенціалу України

Андрій О. Шаховець [1] *

[1] *Державний університет «Київський авіаційний інститут» (Україна). Аспірант кафедри міжнародних економічних відносин.*

*** *Автор-кореспондент,*** e-mail: shah.andriy@gmail.com

СТАТТЯ

Дослідницька

DOI: 10.70651/3083-6018/2026.5.17

Отримана: 07.04.2026 р.
Прийнята: 10.05.2026 р.
Опублікована: 12.05.2026 р.

АНОТАЦІЯ

У статті досліджено роль цифрових технологій як ключових векторів модернізації військово-промислового потенціалу України в умовах повномасштабної війни та глобальних трансформацій у безпековому середовищі. Обґрунтовано, що цифровізація стала одним із головних чинників, які визначають ефективність, адаптивність та технологічну стійкість оборонно-промислового комплексу. У дослідженні проаналізовано сучасні тенденції цифрової трансформації оборонного сектору, включаючи впровадження систем штучного інтелекту, автоматизованих платформ командування та управління, цифрових логістичних рішень, механізмів кіберзахисту, безпілотних технологій, а також цифрових двійників у процесах виробництва та військового планування. Особливу увагу приділено розвитку вітчизняної military-tech екосистеми протягом 2020–2025 років, зокрема діяльності платформи BRAVE1, інтеграції систем ситуаційної обізнаності DELTA та «Кропива», а також упровадженню таких електронних сервісів, як «Армія+» та «Резерв+». У статті доведено, що використання цифрових інструментів суттєво оптимізує процеси прийняття операційних рішень, підвищує прозорість логістики та закупівель, покращує координацію між військовими та цивільними інституціями, а також посилює інтеграцію України у міжнародне оборонне та технологічне співробітництво. У ході дослідження ідентифіковано основні бар'єри на шляху цифрової трансформації військово-промислового комплексу, серед яких виокремлено фрагментарність управлінських підходів, недостатнє фінансове забезпечення, дефіцит висококваліфікованих кадрів, кіберзагрози, залежність від імпортних технологій та електронних компонентів, а також відсутність єдиної цифрової політики. Крім того, як критичні виклики, що обмежують темпи цифрової модернізації, виділено наслідки пошкодження промислової інфраструктури та нестабільність логістики у воєнний час. У статті обґрунтовано пріоритетні напрями подальшого цифрового розвитку оборонно-промислового комплексу України, такі як створення інтегрованої цифрової інфраструктури, впровадження систем PLM, ERP та MES, розширення механізмів кіберстійкості, розвиток технологій штучного інтелекту, підтримка defense-tech стартапів та зміцнення міжнародного технологічного партнерства з країнами-членами НАТО та ЄС. Зроблено висновок, що цифровізацію слід розглядати не лише як технологічне оновлення, а й як стратегічний процес, спрямований на забезпечення технологічного суверенітету, зміцнення національної безпеки, підвищення конкурентоспроможності оборонної індустрії та формування інноваційної і стійкої оборонної екосистеми в Україні.

КЛЮЧОВІ СЛОВА

цифровізація, військово-промисловий комплекс, оборонно-промисловий потенціал, цифрові технології, штучний інтелект, кібербезпека, цифрова трансформація, оборонна промисловість, військові інновації, технологічна автономія.

1. Introduction

The current development of Ukraine's military-industrial potential is taking place in the context of profound transformations of the global security environment and the rapid spread of digital technologies. At the same time, the digitalization of the defense-industrial complex remains uneven and insufficiently systematic: individual innovative solutions are implemented fragmentarily, without integration into a holistic strategic model. This creates risks of technological dependence, limits the efficiency of production processes and complicates Ukraine's integration into international standards of defense cooperation.

The main challenges of the digital transformation of Ukraine's military-industrial potential are manifested in the fragmentation of implemented solutions that are not supported by a single institutional framework and strategic guidelines. The situation is complicated by limited financial resources and an insufficient level of investment in digital infrastructure, as well as an acute shortage of digital technology specialists in the defense industry. Additional risks are the threats of cyber-hacks, data leakage and technological dependence on external suppliers. In addition, low adaptability to global standards and regulatory requirements complicates Ukraine's integration into international defense cooperation.

In general, the problem is that to ensure technological autonomy, strategic stability and competitiveness in the global security environment, it is necessary to form a holistic system of priority areas for the digital transformation of Ukraine's military-industrial potential.

2. Literature Review

In modern scientific discourse, digital technologies are increasingly considered a key factor in the modernization of the military-industrial potential of states. Ukrainian and foreign researchers emphasize that the digitalization of the defense industry not only increases the efficiency of production processes, but also forms a new management model based on the speed of decision-making, transparency of procedures and integration with civilian digital systems.

The works of Ukrainian authors [1; 18; 21] emphasize that the digitalization of the defense-industrial complex of Ukraine faces several systemic problems – from the fragmentation of decisions and personnel shortages to resource constraints and security risks. At the same time, the need to create a holistic institutional framework and strategic guidelines that would ensure technological autonomy and integration into global standards is emphasized.

Thus, in the work of O. Primak, an analysis of the key problems of the digitalization of the defense-industrial complex of Ukraine is carried out, emphasizing its strategic importance for reforming the industry and ensuring national security. The author identifies the stages of enterprise digitalization and suggests practical mechanisms for its acceleration [16].

The study by the authors Shnukalo A., Lyubarsky S., Gangal A., Shkorupsky V., Yarmolchyk M. is devoted to the analysis of the role of digital technologies in the system of scientific and informational activity, which is of particular importance in the context of modern military-political challenges. The work emphasizes that digitalization is a key factor in the integration of scientific processes into the global information space and ensuring effective interaction between the civilian and military sectors. The authors propose the use of innovative tools from large data sets and artificial intelligence to cloud services and electronic repositories, which are able to improve the quality of information processing and promote the development of defense science [18].

At the same time, the work has certain limitations: it is focused mainly on the conceptual level, without sufficient empirical testing or analysis of international experience. The proposed technologies are outlined in general terms, which reduces the practical value of the recommendations for specific institutional conditions in Ukraine. The lack of a comparative analysis with the practices of NATO countries or the USA limits the ability to assess the competitiveness of the proposed solutions in a global context.

Foreign studies [3; 4; 6; 7; 8; 10; 17] demonstrate that digital technologies in the military-industrial sector are considered a strategic resource capable of ensuring the competitiveness of the state in the global security environment. Special emphasis is placed on the use of artificial intelligence, big data, robotics and cybersecurity as basic areas of digital transformation.

In particular, D. Fiott's research focuses on the digitalization of EU defense policy and the problem of strategic autonomy. The strength of his work lies in the systematic analysis of institutional challenges, but they remain mostly conceptual, without a detailed assessment of the practical mechanisms for introducing digital technologies into production processes [6].

G. Chapman, in his articles [4], criticizes the excessive dependence on "dual-use" technologies that combine civilian and military applications. His position is important for understanding the risks of technological dependence, but it is rather journalistic in nature and not always supported by empirical data.

L. Scarazzato studies the European defense industry, its fragmentation and digitalization trends. His works have significant comparative value, as they allow us to assess the problems of integration and standardization within the EU. At the same time, they focus less on technological details and more on institutional and economic aspects [17].

P. Barbara is mentioned in the context of research on innovation ecosystems and digital models in the military sphere. His works are useful for understanding network forms of interaction, but require additional verification, since their academic base is less clearly defined [3].

All the sources listed form a multidimensional vision of the digital transformation of the defense-industrial complex: from conceptual models [6; 17] to risk criticism [4] and practical cases [7; 10]. Their common weakness lies in their fragmentation and attachment to specific national contexts, which complicates their direct application in Ukraine. At the same time, they are valuable material for comparative analysis and the formation of one's own strategy for the digitalization of the Ukrainian defense-industrial potential.

An analysis of recent research and publications indicates the formation of a scientific paradigm where digital technologies act as key vectors for the modernization of Ukraine's military-industrial potential. They determine not only technological development, but also institutional stability, personnel training and integration into international defense cooperation. Despite the significant contribution of both foreign and Ukrainian researchers to the study of the processes of digitalization of defense industries, there are still areas in scientific works that require deeper study, precisely in the context of strategic guidelines for the modernization of Ukraine's military-industrial potential. Existing research is mostly focused on individual technological solutions or institutional approaches, but there is no holistic vision of digital transformation as a systemic process that should take into account the balance between ensuring national security and integration into global defense cooperation.

3. Problem Statement

The purpose of the article is a comprehensive study of the role of digital technologies in the transformation of the defense-industrial complex, the definition of strategic guidelines for their implementation, and the outline of practical mechanisms for ensuring the technological autonomy of the state.

4. Methods and Materials

The theoretical basis of the study was the scientific works of domestic and foreign authors devoted to the digital transformation of the defense-industrial complex, the development of military innovations, artificial intelligence, cybersecurity and modernization of management systems in the defense sector. The research used general scientific methods of analysis, synthesis, generalization and comparison to identify key trends in the digitalization of the military-industrial potential of Ukraine, as well as a systematic approach to determine strategic directions for its modernization in the context of modern security challenges.

5. Results and Discussion

Digital technologies today are one of the key factors in the transformation of Ukraine's military-industrial potential. In the context of ongoing war and global competition in the security sector, it is digitalization that determines the ability of the defense industry to quickly adapt to new challenges, ensure technological autonomy, and integrate into international standards of cooperation.

Since the beginning of the war with Russia, Ukraine has been actively integrating artificial intelligence into military technologies, considering it as one of the key tools for increasing the efficiency and innovation of the defense sector. In 2024, within the framework of the AI for Defence summer school, students worked on creating FPV drones with autonomous guidance elements, counter-disinformation systems, and voice AI assistants to provide medical assistance directly on the battlefield. In parallel, Ukrainian miltech companies are developing solutions for automatic threat detection, analysis of drone video, and ensuring cyber protection of military networks [5].

In 2020–2025, Ukraine carried out a large-scale digital transformation of the defense sector, which became a response to the challenges of a full-scale war. This process included the creation of new digital platforms, reform of military medical commissions, integration with medical systems and synchronization of state registers, which significantly increased the efficiency of managing mobilization, personnel and logistics processes.

Starting from 2022, a military tech ecosystem has been rapidly developing in Ukraine, which is changing approaches to logistics management, combat operations and defense planning. The Brave1 state accelerator has brought together more than two thousand projects, becoming a key platform for testing, certification and implementation of innovative solutions. Among the most successful startups are Zvook (acoustic missile and drone detection systems), Osavul (AI for monitoring the media environment and countering information operations), Swarmer (drone swarm technologies), Buntar Aerospace (electronic warfare-resistant drones), Bavovna.ai (navigation systems for drones without satellite communication) [1; 2; 9].

Digital combat management platforms, in particular Griselda, integrate artificial intelligence for automated collection, filtering and verification of data about the enemy. They operate in interaction with the Nettle, Delta, and Armour systems, providing real-time situational awareness, which reduces reaction time and increases the accuracy of the defeat. In the logistics sector, autonomous ground platforms, such as SIRKO-S from SkyLab, are actively used, capable of transporting cargo, evacuating the wounded and maintaining communication between units. In parallel, FPV drones, fire training simulators (UNITS from Logics7), sea and underwater kamikaze drones are being developed – a unique contribution of Ukraine to global military tech [2; 5; 19; 20]. Ukraine is also forming a common market for defense startups with Europe – BraveTech EU, which allows European companies to test their products in combat conditions and integrate the best solutions into the Defense Forces [11; 13; 14; 22].

The central element of the transformation was the introduction of electronic document management in the Armed Forces. The Army+ application, presented in 2024, provided the opportunity to submit electronic reports, receive UBD status, use social services, undergo training and make personnel requests without paper bureaucracy. The Reserve+ platform became a key tool for military conscripts, allowing them to update their account data, submit requests for deferment, receive referrals to the Military Medical Commission and interact with the "Oberig" registry [1; 2; 9].

In 2025, the Ministry of Defense completed the transition to electronic military medical commissions: the Military Medical Commission's resolutions are now issued in the Medical Information System of the Armed Forces of Ukraine and automatically transferred to the "Oberig" registry and the Army+ and Reserve+ applications. This reduced the time for document processing, reduced the risks of data loss and ensured the transparency of the medical examination process.

An important stage was the introduction of electronic accounting of the mobilization resource: by mid-2025, the "Oberig" register was filled by more than 90% and synchronized with other state databases (Ministry of Justice, Ministry of Internal Affairs, Central Election Commission, Ministry of Health). This allowed for automatic receipt of information on marital status, education, place of work and medical indicators, which significantly simplified the management of mobilization processes and reduced the burden on the Central Military District. Digitalization also covered logistics processes: procurement, logistics and property accounting. The DOT-Chain and AOZ systems optimized defense procurement, and electronic document management reduced the food supply cycle from 60 to 15 days [9; 12; 15].

As a result, the digital transformation of the defense sector of Ukraine in 2020–2025 was not only a technological breakthrough, but also an institutional reform that changed the culture of management in the army. It provided flexibility, transparency, speed of decision-making and integration with civilian systems – critically important factors in the conditions of modern warfare. The evolution of military-industrial potential appears not only as a technical or economic category, but as an indicator of the

strategic ability of the state to guarantee national security, influence geopolitical processes and maintain technological sovereignty. In the conditions of hybrid war and high-tech confrontation, it is digital tools that ensure the speed of decision-making, the accuracy of combat operations, the efficiency of production processes and the transparency of logistics. The introduction of situational awareness systems, artificial intelligence, innovative platforms, and digital production technologies is shaping a new quality of the defense industry, which allows Ukraine not only to increase its own combat capability but also to integrate into global security standards and defense technologies (see Table 1).

Table 1. The role of digitalization in the development of Ukraine's military-industrial potential

Digitalization direction	Tools and technologies	Impact on military-industrial potential (MIP)
Digital Warfighting	DELTA Situational Awareness System	Reduction of decision-making time; integration of intelligence information
Artificial Intelligence and Analytics	AI-data processing from UAVs and combat operations	Increase in planning accuracy and effectiveness of weapons use
Innovative Platforms	Brave1 State Platform	Accelerate the transition from the development stage to serial production
Digital Procurement and Logistics	Automated Accounting and Supply Systems	Reduce resource losses; increase transparency and controllability of processes
Digitalization of Production	CAD/CAM Solutions, Digital Twins, ERP Systems	Reduce product costs; shorten production cycles and increase efficiency

Source: Formed by the author.

Summarizing the above data, it can be stated that the digitalization of the defense-industrial complex of Ukraine covers key areas – from combat management and analytics to production and logistics – and ensures a systematic increase in the efficiency of the defense sector. The integration of modern digital tools helps to reduce decision-making time, optimize production processes, reduce costs and increase transparency. In the complex, this forms a new quality of the functioning of the military-industrial complex and determines its ability to meet modern challenges and integrate into international security standards.

During a full-scale war, digital technologies are a determining factor in strengthening the defense capability, adaptability and efficiency of the military-industrial complex of Ukraine. At the same time, the digitalization process faces several structural, organizational, technical and security barriers that slow down the pace and scale of the implementation of innovative solutions. Identifying these obstacles and determining priority areas of digital development is critically important for the formation of a sustainable defense-industrial ecosystem capable of providing a technological advantage in the conditions of military confrontation.

The digital transformation of Ukraine's defense-industrial complex under martial law appears not only as a technological challenge but also as a strategic necessity that determines the state's ability to innovate, adapt, and maintain defense autonomy. In the modern world, digital technologies are becoming the driving force behind changes in production, management, logistics, and combat systems. For Ukraine, this process is of strategic importance, but at the same time, it faces systemic barriers that slow down the integration of complex IT solutions, innovative platforms, and cyber resilience mechanisms.

However, the digitalization process in Ukraine faces several barriers, including:

- financial constraints – insufficient investment in research and development and production automation;
- personnel shortage – lack of highly qualified engineers and IT specialists capable of implementing modern technologies;
- import dependence – even under conditions of import substitution, critical microcircuits remain a problem area;
- regulatory barriers – complex procurement and certification procedures slow down the integration of digital solutions.

The war period creates specific challenges for the digital transformation of Ukraine's defense-industrial complex. Among the key barriers, it is worth noting the fragmentation of management decisions, resource shortages, cyber risks, a weak regulatory framework, and infrastructure instability.

The lack of a unified digital strategy and insufficient integration between state institutions and enterprises leads to the dispersion of initiatives and a decrease in overall efficiency.

Taken together, these factors create a complex environment that slows down the pace of digital modernization of the industry and requires systemic reforms to overcome existing limitations. Additional constraining factors are limited access to modern technologies, a shortage of highly qualified specialists in the fields of artificial intelligence, IIoT, DevSecOps and systems engineering, as well as the lack of regulation of intellectual property and export control issues. In this context, the study of barriers to digitalization of the defense-industrial complex of Ukraine is particularly relevant. It is a necessary stage for determining the directions of industry transformation that will take into account crisis conditions, international standards and national priorities, ensuring the formation of a sustainable and technologically competitive defense ecosystem. Analysis of barriers allows not only to identify critical points of loss, but also to outline the directions of policy, regulation, institutional coordination and investment necessary to ensure sustainable digital modernization of defense production, Table 2.

Table 2. The main obstacles to the digitalization of Ukraine's military-industrial complex during the war period

Obstacle	Characteristics	Consequences for defense potential	Suggestions for minimization
Destruction of production infrastructure	A significant part of defense enterprises has suffered physical destruction or lost production capacity due to hostilities.	Reduced production capabilities, supply chain disruptions.	Implementation of the policy of relocation of production to safe regions; creation of backup digital hubs and mobile production complexes.
Lack of centralized digital policy in the military-industrial complex	No single body or regulatory strategy is coordinating the digital transformation of the defense sector.	Fragmentation of digital initiatives, duplication of efforts, low standards alignment.	Creation of the National Center for Digital Transformation of the Military-Commercial Industry; development of the State Strategy for Digital Defense Policy with clear priorities.
Cyber threats and information attacks	Increasing cyberattacks on defense systems, databases, and communication channels.	Compromise of critical data, disruption of combat communications, loss of information sovereignty.	Implementation of the Zero Trust Architecture system, cyber intelligence, continuous security audit; strengthening cooperation with NATO cyber agencies.
Lack of financial and human resources	A significant part of the funding is directed to operational military needs, and specialists are relocated or mobilized. Slowing down the pace of digital developments, reducing the innovative potential. Implementation of a public-private partnership system, attracting donor programs; creation of military-digital educational hubs for training personnel.	A significant part of the funding is directed to operational military needs, and specialists are relocated or mobilized. Slowing down the pace of digital developments, reducing the innovative potential. Implementation of a public-private partnership system, attracting donor programs; creation of military-digital educational hubs for training personnel.	A significant part of the funding is directed to operational military needs, and specialists are relocated or mobilized. Slowing down the pace of digital developments, reducing the innovative potential. Implementation of a public-private partnership system, attracting donor programs; creation of military-digital educational hubs for training personnel.
Unregulated legal framework for digital defense activities	Lack of a regulatory framework for AI, autonomous systems, dual-use data. Legal uncertainty, risks of unauthorized use of technologies. Development of a special	Lack of a regulatory framework for AI, autonomous systems, dual-use data. Legal uncertainty, risks of unauthorized use of technologies. Development of a special	Lack of a regulatory framework for AI, autonomous systems, dual-use data. Legal uncertainty, risks of unauthorized use of technologies. Development of a special Law on the digital

Obstacle	Characteristics	Consequences for defense potential	Suggestions for minimization
	Law on the digital transformation of the defense sector, harmonized with EU and NATO directives.	Law on the digital transformation of the defense sector, harmonized with EU and NATO directives.	transformation of the defense sector, harmonized with EU and NATO directives.
Dependence on foreign technologies and components	Import dependence on suppliers of electronics, sensors, microprocessors. Technological vulnerability, risk of blockade or stoppage of supplies. Development of an import substitution program, support for domestic component manufacturers, formation of strategic reserves.	Import dependence on suppliers of electronics, sensors, microprocessors. Technological vulnerability, risk of blockade or stoppage of supplies. Development of an import substitution program, support for domestic component manufacturers, formation of strategic reserves.	Import dependence on suppliers of electronics, sensors, microprocessors. Technological vulnerability, risk of blockade or stoppage of supplies. Development of an import substitution program, support for domestic component manufacturers, formation of strategic reserves.
Lack of an integrated digital infrastructure of the military-industrial complex	There is no single database, product lifecycle management platforms, interaction between enterprises.	Reduced coordination, duplication of processes, information barriers.	Creation of a single digital space for the Ukrainian military-industrial complex based on the state cloud architecture (GovCloud Defense).
Logistical constraints, power outages and infrastructure damage	Transport, energy and telecommunications networks are destroyed.	Delays in production, loss of communications, slowing down of digital operations.	Creation of non-volatile data centers, backup communication channels, use of satellite and Starlink communications.
Human resource shortage in the field of digital technologies	Loss of specialists due to emigration, mobilization, or change of industry.	Reduced ability to support complex systems and develop new solutions.	Implementation of state programs for the return of IT specialists, educational grants and incentives for digital volunteers.
Lack of coordination between state structures, the Armed Forces of Ukraine and the private sector	There is no unified platform for data exchange between defense participants.	Reduced efficiency of innovation, duplication of projects.	Creation of a single defense innovation management system (Defense Innovation Hub), joint project offices for the military-industrial complex and startups.

Source: Compiled by the authors

In the process of digital transformation of the defense-industrial complex of Ukraine in wartime conditions, several systemic barriers were identified that limit the technological, organizational and personnel development of the industry. First of all, it should be noted that the destruction of the production infrastructure of defense enterprises caused the loss of part of the capacities, disruption of logistics chains and complicated the implementation of modern digital solutions.

One of the key challenges remains the lack of a centralized digital policy in the military-industrial complex: initiatives are implemented fragmentarily, standards remain non-unified, and the interaction between state institutions, the private sector and military structures is insufficiently coordinated. This creates an environment in which digital modernization occurs unevenly and requires systemic reforms to ensure the coherence and efficiency of transformation processes.

Priority areas of digitalization of the defense-industrial complex of Ukraine include the integration of production systems, the development of digital twin technologies, ensuring cyber resilience, product life cycle management and the formation of a single digital infrastructure. These guidelines are

enshrined in the Strategy for the Development of the Military-Commercial Industry and Digital Infrastructure of Strategic Industries.

Within the framework of the state policy of modernization of the defense-industrial complex, digital technologies are considered as a key tool for increasing the efficiency, transparency and innovativeness of the industry, ensuring its adaptability to modern challenges and integration into global security standards. In accordance with the provisions of the Defense Industry Development Strategy, approved by Decree of the President of Ukraine No. 372/2021, as well as the draft Digital Infrastructure Strategy, several priority areas of digitalization have been identified [15; 16; 22]:

• integration of production systems when implementing digital platforms that combine PLM (product life cycle management), ERP (resource planning) and MES (production management). This allows for real-time synchronization of design, production and logistics.

• implementation of digital twins by creating virtual models of products and production lines for simulation, testing and optimization of processes, which reduces costs and accelerates the innovation cycle;

• ensuring cybersecurity and information resilience using multi-layered protection systems, including SIEM/SOAR, hardware roots of trust, cryptographic auditing and software lifecycle protection.

• product lifecycle management using digital product passports, PLM and ERP systems for traceability, quality control and compliance with NATO and EU standards.

• a single digital infrastructure through the creation of an integration Core Hub with open APIs, metadata registries and service catalogs, ensuring interoperability between enterprises, government agencies and international partners.

• implementation of cloud and hybrid IT solutions combining local capacities for critical components with certified cloud services for analytics, modelling and data management.

• institutional support for innovation through the creation of competence centers, acceleration programmes, platform-markets of certified solutions and mechanisms for technology transfer from the civil to the defence sector.

The outlined directions form the basis of the roadmap for the digital transformation of Ukraine's defense-industrial complex, aimed at ensuring sustainability, technological autonomy, and integration into global defense cooperation.

At the same time, to intensify these processes, we can propose expanding the spectrum of use of digital technologies in the development of the military-industrial complex of Ukraine, taking into account current trends in the global defense market. This will allow not only to adapt the national system to current challenges, but also to ensure its compliance with international standards and increase competitiveness in the global security environment (Fig. 1).

In the current conditions of a large-scale war against Ukraine, digital technologies are acquiring the status of a strategic resource, which determines not only the operational effectiveness of military operations but also the ability of the state to maintain the defense-industrial potential at the proper level.

The military-industrial complex, in our opinion, is a key element of the national security system, and its digital transformation is a necessary condition for the transition to a new model of defense production – intelligent, flexible and integrated into global technological chains.

The development of digital technologies in the military-industrial complex of Ukraine should ensure increased accuracy, speed and autonomy of production and management processes, improvement of defense planning, logistics and monitoring systems. Of particular importance is the creation of a single information architecture that will allow for the prompt exchange of data between enterprises, scientific institutions and military structures.

The implementation of digital tools from artificial intelligence, big data and digital twins to unmanned systems and cyber defense technologies should be carried out taking into account the principles of technological sovereignty, security and ethical responsibility.

Determining the priority areas of digitalization of the military-industrial complex of Ukraine is a fundamental task of state policy in the field of national security and defense. These areas should become the basis for a comprehensive digital transformation of the defense-industrial system, contribute to the growth of its innovative potential, ensure interoperability with NATO partners and stimulate the development of dual technologies suitable for both military and civilian use.

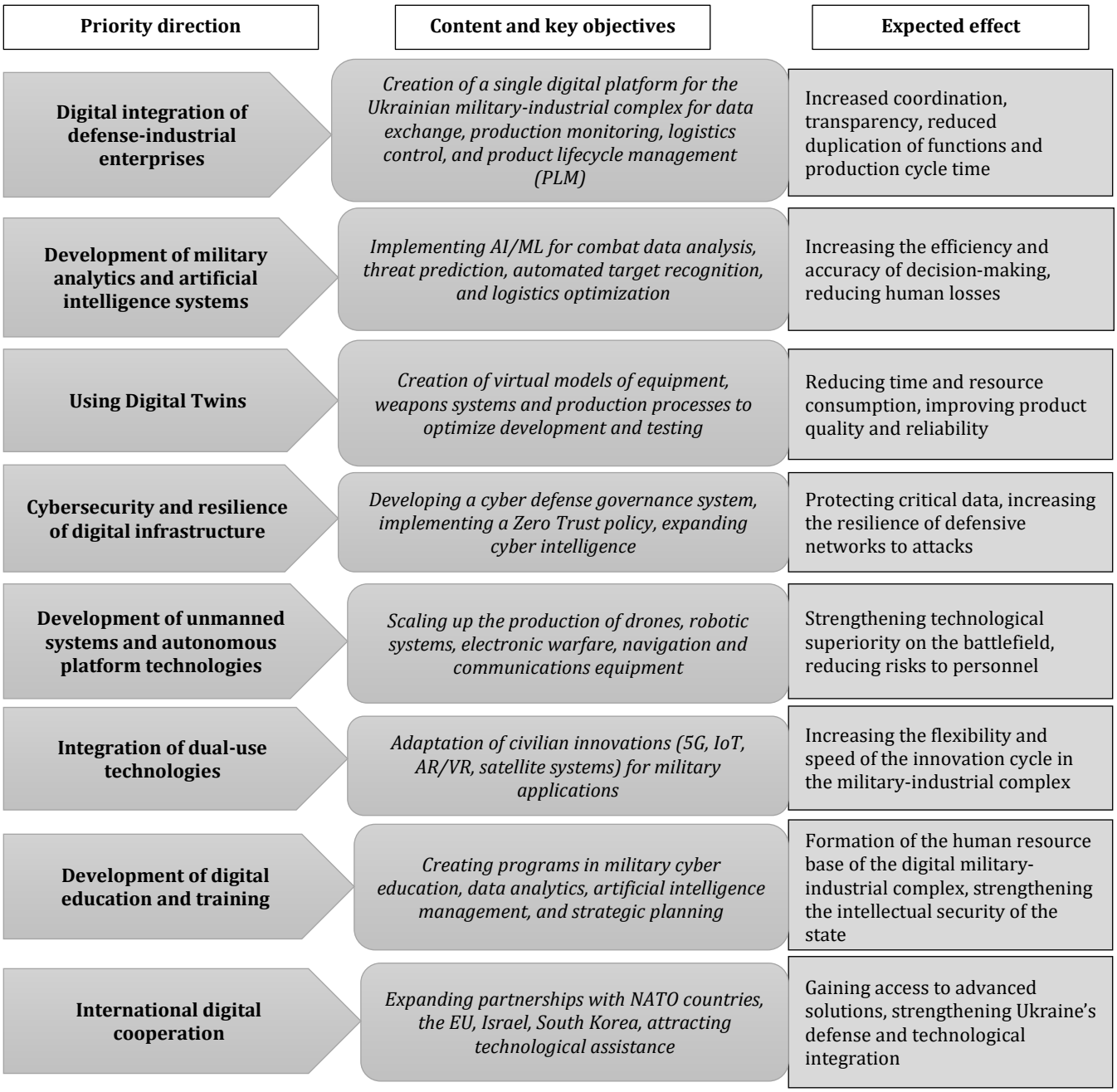

Figure 1. Priority areas of use of digital technologies in the development of the Ukrainian Air Transport Network

Source: Built by the author.

Therefore, the digitalization of the military-industrial complex should be considered not only as a technical upgrade but as a strategic process of rethinking defense production, aimed at increasing the resilience, adaptability, and technological independence of Ukraine.

6. Conclusions

The study confirms that digital technologies have become a key factor in the modernization of the military-industrial complex of Ukraine in 2020–2025. They have ensured the transition from an inflexible state model to an innovation-oriented system with the active participation of the private sector, the integration of artificial intelligence, automated control systems, defense-tech platforms and big data analytics. Digitalization has acted as a multiplier for the growth of defense potential, contributing to technological flexibility, innovation and integration into the modern model of war.

At the same time, several systemic barriers have been identified: the destruction of production infrastructure, the lack of a centralized digital policy, the lack of highly qualified personnel, limited

access to modern technologies and the lack of regulation of intellectual property issues. These factors slow down the pace of transformation and require comprehensive reforms aimed at creating a unified digital strategy, developing human resources and ensuring cyber resilience.

Further exploration in the field of digital transformation of the Ukrainian military-industrial complex should be focused on developing a comprehensive digitalization roadmap, taking into account crisis conditions and international standards and creating a unified information architecture for effective interaction between government structures, the private sector, and military institutions.

References

1. Andrushkiv, B.M., & Petruk, O.M. (2023). Tsyfrovizatsiia oboronno-promyslovoho kompleksu: vyklyky ta ryzyky dlia natsionalnoi bezpeky [Digitalization of the defense-industrial complex: challenges and risks for national security]. *Ekonomika ta derzhava – Economy and State*, (5), 33–38. (in Ukrainian)
2. Avtomatyzovana systema upravlinnia viiskamy [Automated command and control system]. *Novyny veteraniv – Veterans news* (June 12, 2026). https://nova.net.ua/avtomatyzovana-systema-upravlinnia-viiskamy (in Ukrainian)
3. Barbaroux, P. (2021). Defense–Military Innovation: Networks and Dual-use Technological Development. *Innovation Economics, Engineering and Management Handbook 2: Special Themes*, 109–114. https://doi.org/10.1002/9781119832522.ch11
4. Chapman, G., & Yudken, J. (1992). *Briefing Book on the Military-Industrial Complex*. Washington, DC: Council for a Livable World Education Fund.
5. Drony, ShI, kiberataky: yaki uroky zasvoiv svit cherez rik viiny v Ukraini [Drones, AI, cyberattacks: lessons the world learned after a year of war in Ukraine]. *Focus* (February 25, 2023) https://focus.ua/uk/digital/551836-drony-ii-kiberataki-kakie-uroki-izvlek-mir-spustya-god-voyny-v-ukraine (in Ukrainian)
6. Fiott, D. (2025). *Defence Innovation Trends: EDF Snapshot 2021–2024*. https://csds.vub.be/publication/defence-innovation-trends-a-data-snapshot-of-the-european-defence-fund-2021-2024/
7. Loidolt, B., & Ballanco, E. (2018). If We Want Security Force Assistance Missions to Succeed, Give Advisers Control of the Purse Strings. *Modern War Institute War Room*. https://mwi.westpoint.edu/want-security-force-assistance-missions-succeed-give-advisers-control-purse-strings/
8. Mahnken, T. (2021). Defense Innovation and Industrial Mobilization: A Competitive Edge: policy brief. Washington, D.C.: Center for Strategic and Budgetary Assessments. https://csbaonline.org/research
9. Natsionalna prohrama rozvytku viiskovykh komunikatsii na 2022–2025 roky [National Program for the Development of Military Communications for 2022–2025]. *Cabinet of Ministers of Ukraine.* https://www.kmu.gov.ua (in Ukrainian)
10. Nicastro, L. (2024). DARPA and the Future of Defense Innovation. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA889-1.html
11. Pro stvorennia ta funktsionuvannia platformy BRAVE1 [On the Creation and Functioning of the BRAVE1 Platform]. (2023). *Cabinet of Ministers of Ukraine.* https://www.kmu.gov.ua (in Ukrainian)
12. Prohrama "Digital Battlefield" [Digital Battlefield Program]. (2023). *Ministry of Defense of Ukraine*. https://www.mil.gov.ua (in Ukrainian)
13. Prohrama "E-Oborona" dlia tsyfrovoi lohistyky [E-Defense Program for Digital Logistics]. (2023). *Cabinet of Ministers of Ukraine*. https://www.kmu.gov.ua (in Ukrainian)
14. Prohrama rozvytku oboronno-promyslovoho kompleksu Ukrainy na 2022–2025 roky [Program for the Development of the Defense-Industrial Complex of Ukraine for 2022–2025]. (2022). *Cabinet of Ministers of Ukraine.* https://www.kmu.gov.ua (in Ukrainian)
15. Proiekt Stratehii tsyfrovoi infrastruktury stratehichnykh haluzei promyslovosti Ukrainy [Draft Strategy for the Development of Digital Infrastructure of Strategic Industries of Ukraine]. (2023). *Ministry of Strategic Industries of Ukraine*. https://mspu.gov.ua/news/u-minstrategpromi-obgovorili-proyekt-strategiyi-rozvitku-cifrovoyi-infrastrukturi-strategichnih-galuzej-promislovosti-oboronno-promislovogo-kompleksu-ukrayini (in Ukrainian)
16. Prymak, O. (2023). Suchasni problemy zaprovadzhennia tsyfrovizatsii v oboronno-promyslovyi kompleks Ukrainy [Contemporary issues of implementing digitalization in the defense-industrial complex of Ukraine]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public Administration: Concepts, Paradigm, Development, Improvement*, (5), 94–104. (in Ukrainian)

17. Scarazzato, L., & Nicastro, L. (2022). Restructuring the European Defence Industry: Challenges and Innovation Strategies. *Small Wars & Insurgencies*, *33*(2). https://doi.org/10.1080/09592318.2022.2039387
18. Shnukalo, A., Liubarskyi, S., Hangal, A., Shkorupskyi, V., & Yarmolchyk, M. (2024). Tsyfrovi tekhnolohii v systemi naukovo-informatsiinoi diialnosti [Digital technologies in the system of scientific and information activities]. *Military Science*, (2), 161–169. (in Ukrainian)
19. Systema sytuatsiinoi obiznanosti "Delta" [Delta Situational Awareness System]. (2022). *Ministry of Defense of Ukraine*. https://www.mil.gov.ua (in Ukrainian)
20. Systema upravlinnia artyleriiskym vohnem "Kropyva" [Kropyva Artillery Fire Control System]. (2022). *Ministry of Defense of Ukraine.* https://www.mil.gov.ua (in Ukrainian)
21. Ukaz Prezydenta Ukrainy vid 20 serpnia 2021 r. № 372/2021 "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 18 chervnia 2021 roku "Pro Stratehiiu rozvytku oboronno-promyslovoho kompleksu Ukrainy"" [Decree of the President of Ukraine of 20 August 2021 No. 372/2021 "On the Decision of the National Security and Defense Council of Ukraine of June 18, 2021 'On the Strategy for the Development of the Defense-Industrial Complex of Ukraine'"]. *Official Internet Representation of the President of Ukraine.* https://www.president.gov.ua/documents/3722021-39725 (in Ukrainian)
22. Ukaz Prezydenta Ukrainy vid 25.03.2021 № 121/2021 "Pro Stratehiiu voiennoi bezpeky Ukrainy" [Decree of the President of Ukraine of 25 March 2021 No. 121/2021 "On the Military Security Strategy of Ukraine"]. *Official Internet Representation of the President of Ukraine.* https://www.president.gov.ua/documents/1212021-37661 (in Ukrainian)