e-ISSN 3083-6018

SOCIAL DEVELOPMENT: Economic and Legal Issues

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

Strategic Guidelines for the Digital Transformation of the Military-Industrial Complex Worldwide

Andriy Shakhovets [1] *

[1] *National 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: 10.70651/3083-6018/2026.4.23

Received:
19 March 2026
Accepted:
22 April 2026
Published online:
24 April 2026

ABSTRACT

This article explores the strategic dimensions and challenges of digital transformation within the global military-industrial complex (MIC). Digitalization is examined as a decisive factor in the modernization of defense industries, shaping states' competitiveness, technological autonomy, operational efficiency, and resilience in the evolving security environment. The study traces the evolution of military-industrial potential under the influence of global digitalization processes, clarifies the distinctions between the concepts of military-industrial complex, defense-industrial complex, and defense production, and positions military-industrial potential as an analytical category. Particular attention is devoted to the integration of Industry 4.0 components—digital twins, PLM/MES systems, IIoT, artificial intelligence, and cybersecurity—into the operations of leading defense enterprises worldwide. The article advances a conceptual framework for the digital transformation of the military-industrial complex by identifying five interrelated strategic directions. At the institutional level, emphasis is placed on the consolidation of digital sovereignty, the establishment of coherent legal regulation, and the creation of governance mechanisms capable of coordinating state, industry, and research actors. Technological development is understood through the construction of integrated platforms that ensure interoperability and the deployment of advanced digital tools, thereby enabling seamless interaction across production and management systems. Human capital emerges as a critical dimension, requiring the systematic training of digital specialists, the establishment of educational consortia, and the introduction of programs for "digital officers" equipped with strategic and technological competencies. Ethical and security considerations are highlighted as indispensable, encompassing cyber resilience, the responsible use of artificial intelligence, and strict compliance with international law and humanitarian principles. Finally, the financial and economic foundation is addressed through innovation funds, public-private partnership mechanisms, tax incentives, and cluster-based ecosystems that stimulate investment and sustain technological modernization. Taken together, these strategic orientations form an integrated pathway toward a resilient, innovative, and globally competitive defense industry in the digital era. It is argued that the synergy of these directions creates an integrated system capable of ensuring sustainability, innovation, and strategic effectiveness of the defense sector. Future research perspectives include the development of quantitative methodologies to assess the impact of digitalization on military-industrial potential, comparative analysis of international cooperation models in DefenseTech, and formulation of practical recommendations for Ukraine, considering resource constraints and global technological trends.

KEYWORDS

military-industrial complex, digital transformation, military-industrial potential, Industry 4.0, cybersecurity, strategic guidelines.

e-ISSN 3083-6018

СОЦІАЛЬНИЙ РОЗВИТОК: економіко-правові проблеми

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

Стратегічні орієнтири цифрової трансформації військово-промислового комплексу країн світу

Андрій О. Шаховець [1] *

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

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

СТАТТЯ

Дослідницька

DOI: 10.70651/3083-6018/2026.4.23

Отримана: 19.03.2026 р.
Прийнята: 22.04.2026 р.
Опублікована: 24.04.2026 р.

АНОТАЦІЯ

У статті досліджено стратегічні виміри та виклики цифрової трансформації в межах глобального військово-промислового комплексу (ВПК). Цифровізація розглядається як вирішальний чинник модернізації оборонної промисловості, що визначає конкурентоспроможність держав, їхній технологічний суверенітет, операційну ефективність та стійкість у динамічному безпековому середовищі. У дослідженні простежено еволюцію військово-промислового потенціалу під впливом глобальних процесів цифровізації, розмежовано поняття «військово-промисловий комплекс», «оборонно-промисловий комплекс» та «оборонне виробництво», а також позиціоновано «військово-промисловий потенціал» як аналітичну категорію. Особливу увагу приділено інтеграції компонентів Індустрії 4.0 – цифрових двійників, систем PLM/MES, промислового інтернету речей (IIoT), штучного інтелекту та кібербезпеки – в операційну діяльність провідних оборонних підприємств світу. Автором запропоновано концептуальну основу цифрової трансформації військово-промислового комплексу шляхом виокремлення п'яти взаємопов'язаних стратегічних напрямів. На інституційному рівні акцент зроблено на консолідації цифрового суверенітету, розробці узгодженого правового регулювання та створенні механізмів управління, здатних координувати дії держави, промисловості та науково-дослідних суб'єктів. Технологічний розвиток розглядається крізь призму побудови інтегрованих платформ, які забезпечують інтеркалібрування (інтероперабельність) та розгортання передових цифрових інструментів, уможливлюючи безшовну взаємодію між виробничими та управлінськими системами. Людський капітал визначено як критично важливий вимір, що потребує системної підготовки цифрових фахівців, створення освітніх консорціумів та впровадження програм для «цифрових офіцерів» (digital officers), наділених стратегічними та технологічними компетенціями. Етичні аспекти та безпекові міркування виділено як невід'ємні складники, що охоплюють кіберстійкість, відповідальне використання штучного інтелекту та суворе дотримання норм міжнародного права і гуманітарних принципів. Насамкінець, фінансово-економічний фундамент забезпечується через інноваційні фонди, механізми державного-приватного партнерства, податкові стимули та кластерні екосистеми, які стимулюють інвестиції та підтримують безперервну технологічну модернізацію. У сукупності зазначені стратегічні орієнтири формують інтегровану траєкторію розвитку стійкої, інноваційної та глобально конкурентоспроможної оборонної промисловості в цифрову епоху. Доведено, що синергія цих напрямів створює цілісну систему, здатну забезпечити життєздатність, інноваційність та стратегічну ефективність оборонного сектору. Перспективи майбутніх досліджень містять розробку кількісних методологій для оцінювання впливу цифровізації на військово-промисловий потенціал, порівняльний аналіз міжнародних моделей співпраці у сфері DefenseTech, а також формулювання практичних рекомендацій для України з урахуванням ресурсних обмежень та глобальних технологічних трендів.

КЛЮЧОВІ СЛОВА

військово-промисловий комплекс, цифрова трансформація, військово-промисловий потенціал, Industry 4.0, кібербезпека, стратегічні орієнтири.

1. Introduction

The modern military-industrial complex (MIC) is in a phase of profound transformations, which are caused by global security challenges, intensive development of digital technologies and the growing role of innovations in ensuring the defense capability of states. Digitalization of production processes, integration of artificial intelligence, automated control systems and cyber defense are becoming key factors in increasing the efficiency and sustainability of defense infrastructure. At the same time, uneven technological development between countries, limited resources and aggravation of geopolitical conflicts actualize the need to form strategic guidelines for the digital transformation of the MIC.

The problem is to determine the optimal models of digital modernization that would combine scientifically based approaches with practical implementation tools, taking into account the specifics of national economies, the level of technological readiness and international standards of cooperation. Its solution is directly related to important scientific tasks – the development of concepts for integrating digital technologies into production and management processes, modeling risks and development scenarios, as well as practical tasks – increasing defense capabilities, optimizing costs, ensuring technological independence and forming competitive advantages in the global arms market. Thus, the formulation of the problem of digital transformation of the military-industrial complex goes beyond the boundaries of a purely technological discourse and acquires strategic importance, as it determines the trajectories of the development of defense systems in the context of global security and international integration.

2. Literature Review

In the modern scientific discourse, the issue of digital transformation of the military-industrial complex has been reflected in the works of a number of foreign authors. In particular, P. Barbaru substantiates the importance of innovative ecosystems and network forms of interaction for the development of the defense industry. G. Chapman analyzes the relationship between defense industrial policy and technological progress, emphasizing the strategic consequences of such a combination. D. Fiotta focuses on the processes of European defense-industrial integration and the formation of digital autonomy, which is of key importance for ensuring the technological independence of the EU. B. Loidolt considers the strategic aspects of the digitalization of defense industries, emphasizing their role in the formation of new models of competitiveness. T. Mankena [16] examines the impact of breakthrough technologies on military strategy and defense planning, demonstrating how digital innovations change the architecture of security systems. L. Nicastro [19] analyzes the institutional and industrial mechanisms of the development of the defense sector, while L. Scarazzato [23] pays attention to digital value chains and the transformation of production processes in the defense industry. Thus, the scientific achievements of domestic authors, such as Kim T. I., Ukrainets Yu. M. [13], Semenenko O. M., Boyko R. V., Voronchenko I. O., Taran O. V. [24], Pustoviyt R. F. [20-21] form a multidimensional vision of the digital transformation of the military-industrial complex, covering both strategic and institutional, technological and organizational aspects of this process.

Despite the significant contribution of foreign and domestic researchers to the study of the digitalization of defense industries, there are still areas in their works that require deeper study precisely in the context of strategic guidelines. These works lack a holistic vision of the strategic guidelines for the digitalization of the military-industrial complex at the global level, which would take into account the balance between national security and global cooperation.

3. Problem Statement

The purpose of the article is a comprehensive study of the strategic guidelines for the digital transformation of the military-industrial complex of the world, which involves determining the conceptual foundations of the digital modernization of the military-industrial complex in a global dimension, taking into account technological, economic, social and security factors.

4. Methods and Materials

The theoretical and methodological basis of the study is the scientific works of domestic and foreign scientists on the issues of digital transformation of the defense industry, the development of military-industrial potential and the implementation of Industry 4.0 technologies. The research used methods of analysis and synthesis – to generalize modern approaches to the digitalization of the military-industrial complex; the system method – to determine the relationships between technological, institutional and economic components of digital transformation; the comparative method – to study the international experience of digital modernization of defense industries; the generalization method – to form strategic guidelines for the digital development of the military-industrial complex of countries around the world.

5. Results and Discussion

The digital transformation of the military-industrial complex (MIC) of the countries of the world is emerging as one of the key factors in the modernization of defense systems in the 21st century. The rapid development of information technologies, artificial intelligence, automated control systems and cyber defense is leading to fundamental changes in production processes, logistics and strategic planning of defense industries. In these conditions, digitalization is becoming not only a technological trend but also a strategic necessity that determines the competitiveness of states in the global arms market and their ability to effectively respond to new security challenges.

At the same time, the process of digital modernization of the MIC is accompanied by several contradictions: uneven technological development between countries, limited resources, increasing dependence on global suppliers and increased cyber threats. This highlights the need to form strategic guidelines for digital transformation that would ensure a balance between national security, economic efficiency and international integration.

The concept of "military-industrial potential" (MIP) at the intersection of military affairs, economics and politics acquires particular relevance in conditions of armed conflicts, global instability and intensive processes of rearmament of states. Its content is multifaceted and has numerous interpretations that vary depending on the scientific school, country and historical period. In the classical sense, MIP encompasses a set of production, technological, personnel and institutional resources that ensure the state's ability to create, modernize and maintain weapons and military equipment in accordance with the strategic needs of national security.

In modern discourse, MIP is considered not only as a material and technical base of the defense industry, but also as an integrated indicator of the state's ability to effectively combine innovative technologies, economic mechanisms and political decisions in the field of defense. This concept encompasses the strategic guidelines for the development of the defense-industrial complex, the level of its integration into global production and technological chains, as well as the ability to adapt to new challenges – from cyber threats to changing geopolitical balances.

In the Ukrainian context, the MDP is actively used in connection with the modernization of the defense-industrial complex (DIC), import substitution policy, strategic planning and ensuring national security. It acquires particular importance in conditions of military operations, when issues of technological independence, mobilization readiness and efficiency of resource use become decisive for the stability of the state. The MDP of Ukraine is currently considered as a strategic tool not only for ensuring defense capability, but also for integration into international security structures, the formation of competitive positions in the global arms market and the development of an innovative economy.

In the scientific literature, the concept of military-industrial potential (MIP) is considered from different positions – from the economic base of defense capability to an integral indicator of national power. Professor G. Chapman [4], D. Fiott [9] interprets it as the material basis of defense capability, focusing on the production and resource component. This approach clearly outlines economic opportunities, but limits strategic depth, leaving out of consideration intangible factors – scientific and technical potential, human resources and management mechanisms.

Other authors, in particular T. I. Kim and Y. M. Ukrainets, emphasize the economic risks of militarization and global responsibility, considering MIP as a profitable industry dependent on international conflicts. Such a position is important from the point of view of ethics and economic security, but only partially covers institutional and technological aspects [13].

A systemic approach is demonstrated by O. M. Semenenko, R. V. Boyko, I. O. Voronchenko and O. V. Taran, who define the military-economic security as an integral indicator that includes economic, military and political components of national power. This allows us to consider it as a geostrategic factor, but the abstractness of the definition complicates its practical application without clear methods of quantitative measurement [24].

R. F. Pustoviyt proposes the concept of military-economic security as a set of conditions and factors that ensure timely and reliable satisfaction of military-economic needs. This approach brings the military-economic security closer to the practical dimension of defense policy, but requires integration with modern processes of digital transformation [21].

In scientific discourse, the concepts of "military-industrial complex" (MIC), "defense-industrial complex" (DIC) and "defense production" have a common subject area, but differ in the level of generalization and functional content. The military-industrial complex represents a macro-level system of interaction between the state, the army and industry, covering political, economic and institutional mechanisms for implementing military policy. The military-industrial complex has a narrower production-technological and scientific-innovative focus, concentrating on enterprises, design bureaus and infrastructure that ensure the creation and modernization of weapons. Defense production, in turn, is a micro-level practical activity that materializes the potential in specific defense products [3; 15; 21; 25]. Against this background, the concept of "military-industrial potential" (MIP) occupies a special analytical and evaluative place. It is not a structural entity, but reflects the totality of the state's resources and capabilities that ensure the creation and expansion of defense products. MIP integrates the material base of the MIP, institutional mechanisms of the MIP and practical activities of defense production, acting as an indicator of the system's readiness to perform defense tasks.

Through the prism of the topic of digital transformation, it is important to emphasize that the MCP is the most suitable category for strategic analysis. It is this that allows us to assess not only the existing production capacities, but also the system's ability to adapt to new technological challenges – the integration of digital platforms, process automation, the development of innovative ecosystems and the formation of human resources. Thus, the MCP becomes a key indicator of strategic guidelines for the digital modernization of defense industries in a global dimension.

Over the past decades, the military-industrial potential (MCP) of states has undergone significant transformations under the influence of global digitalization. If in the second half of the twentieth century the MCP was determined mainly by production capacities, material and technical base and mobilization resources, today its key characteristics are the level of digital integration, innovative capacity and ability to technological adaptation [3; 16; 24].

In the modern global environment, digital technologies are a determining factor in the formation of the military-industrial potential of states. They ensure its competitiveness, flexibility and ability to quickly implement innovations. Digitalization transforms the defense-industrial sector, making it more efficient, adaptive and strategically sustainable.

It is not only about technological improvement of production processes, but also about creating a new management model, where the key elements of success are the speed of decision-making, transparency of procedures and integration with civilian digital systems. The digital transformation of the defense industry forms a qualitatively new architecture of the military-industrial potential, combining technological innovations with institutional modernization and opening up prospects for strategic development in a global dimension.

The modern development of the defense-industrial complex is determined by the rapid spread of digital technologies, which are becoming a fundamental factor in increasing the efficiency of the production of weapons and military equipment. In the context of global competition and growing security challenges, the digital transformation of the defense-industrial complexes of the world's leading states appears as a strategic necessity. It not only increases the efficiency of production processes but also forms a new management architecture that ensures a flexible response to operational defense needs and adaptation to rapid technological changes.

The introduction of key elements of the Industry 4.0 concept, in particular automation, robotics, the use of big data, artificial intelligence and cyber defense, creates the prerequisites for the formation of new models of combat platforms and technological modernization of defense systems. Digitalization is becoming a determining factor in strategic stability, as it ensures the speed of decision-making, transparency of processes and the integration of defense production structures with civilian digital systems, Table 1.

Table 1. The presence of digital elements in leading defense industry enterprises around the world

Country	Leading companies	Digital elements confirmed in open sources
USA	Lockheed Martin; Boeing Defense; Northrop Grumman	Production and training digital twins, use of PLM, integrated digital factories (MES/smart factories), IIoT, AI analytics; availability of digital factories and digital twin projects.
United Kingdom	BAE Systems	Availability of digital twins, such as platform/vessel models and PLM applications/drawings to digital models, MES pilots.
Germany	Rheinmetall, KMW	Digital twin (production/operational models), integrated technical support services (IRIS®suite – digital lifecycle file), IIoT, integration with ERP; examples of digital services.
France	Dassault Aviation / Dassault Systèmes; Thales	PLM/MBSE and "virtual twins" via the 3DEXPERIENCE platform; digital design/simulation tools (CAD/CAE) are widely used in defense
Israel	Israel Aerospace Industries (IAI); Elbit Systems	PLM integration and project solutions, cases of cooperation with IT partners (PLM/integration projects), digital models/simulations; mentions of PLM → production integration
South Korea	Hanwha; Korea Aerospace Industries (KAI)	Smart factory / digital twin, including Hanwha digital twins in smart factory; KAI use in digital simulation and VR/DT solutions for training and project support
Turkey	ASELSAN, ROKETSAN	Official announcements about digital transformation: implementation of PLM, AI/Big Data, IIoT in product lines
China	COMAC; AVIC (групи гравців авіації)	Digital twin projects for aviation production (COMAC C919 – examples of digital twin/intelligent platforms in collaboration with suppliers), PLM/factory digitalization
Russia	Rostec / United Engine Corporation (UEC)	Investments in HPEC to create digital twins (e.g., a supercomputer for digital engine twins), digital project announcements; development of "digital factories."
Others (Australia, Canada, Japan)	Thales Australia; CAE; Mitsubishi Heavy Industries та ін.	Use of PLM/CAD/CAE, digital twin and MES at different scales; cases at the supplier and research center level.

Source: Formed by the authors based on [1; 2; 5; 6; 8; 14; 18; 22; 26].

A comparative analysis of digital components confirmed in open sources indicates that the world's leading defense-industrial enterprises are actively integrating key elements of the Industry 4.0 concept. Among them are digital twins, PLM systems, MES solutions, IIoT and CAD/CAE platforms. The most comprehensive integration is demonstrated by companies in the USA, Germany, France and South Korea, where digital twins are used not only in production processes, but also in training simulations, technical support and product life cycle management. PLM solutions have become a basic tool for design, modeling and integration with ERP systems, ensuring end-to-end digital coordination of processes. MES systems and the concept of "smart factories" are actively implemented in the USA, Korea, China and Israel, where they support flexible production and adaptation to changing combat requirements [1; 5; 8; 26].

At the same time, countries with a lower level of technological capitalization, such as Turkey and Russia, mostly declare digital transformation, but its scale and depth remain limited. This is confirmed mainly by investment applications and individual projects that do not form a systemic digital model. In general, the digital elements of Industry 4.0 have become critically important for the modernization of defense production, and their implementation serves as an indicator of the technological capacity of the state to ensure national security in conditions of high-tech confrontation. Thus, digitalization directly contributes to the growth of military-industrial potential. A comparative assessment of the integration

of digital technologies into military logistics and troop management in different countries demonstrates a significant asymmetry of development, which is determined by the level of economic potential, the scale of defense investments and the presence of their own technological base (see Table 2).

Table 2. The use of digital solutions in military logistics in different countries of the world

Country / Organization	Digital solutions in military logistics	Digital solutions in troop management	Integration features
США (DoD, DARPA, CENTCOM)	Predictive logistics (AI/ML), autonomous supply platforms, IoT sensors, GCSS-Army	JADC2, tactical clouds, digital maps, AI analytics	High level of integration; effective interdepartmental coordination;
NATO / UK (MOD, BAE Systems)	Smart logistics, ERP integration, digital supply chains	BMS, digital command interfaces, simulation systems	Ensuring interoperability between allies; standardization of protocols
Germany (Bundeswehr, Rheinmetall)	IIoT monitoring, digital maintenance, ERP	FüInfoSys, PLM command modules	Focus on full life cycle management of weapons
Israel (IDF, Elbit Systems)	Automated supply, mobile logistics platforms	C4I systems, digital combat interfaces	Active integration of commercial technologies into the military sphere
South Korea (ROK Armed Forces, Hanwha)	Smart factory – logistics, MES, digital accounting	VR/AR command, mobile systems	Implementation through a powerful defense industry
Ukraine (Armed Forces of Ukraine, Ukroboronprom)	Pilot ERP/IIoT solutions, digital accounting, 3D printing	Mobile command platforms, digital maps, C2 elements	fragmented integration; activation of processes during war

Source: Compiled by the author [7; 8; 10; 11; 12; 17].

Summarizing the results of the analysis, it can be stated that the United States and China are today setting global standards in the field of digital military logistics. NATO countries focus on ensuring interoperability and collective development of technologies, while Israel acts as a kind of laboratory for innovative solutions. Ukraine, in turn, is actively adapting digital technologies in accordance with current military needs, demonstrating an example of practical integration of digitalization in conditions of armed confrontation.

In the near future, it is the synergy of allied integration, artificial intelligence, digital twins and autonomous systems that will determine the quality and speed of military logistics in the leading countries of the world. This combination will become a key strategic reference point that will ensure the effectiveness, adaptability and sustainability of defense systems in the global security environment.

Thus, the digital transformation of defense-industrial complexes is not limited to technological improvement. It forms a qualitatively new model for the development of military-industrial potential, where the key guidelines are innovation, adaptability and the ability to strategically integrate into the global security environment.

In today's conditions of geopolitical instability and the transformation of global security paradigms, the digitalization of the defense-industrial complex is gaining critical importance. It is a key tool for ensuring technological autonomy, operational efficiency and strategic stability of the state. For Ukraine, which is in a protracted military conflict and is carrying out systemic modernization of the security and defense sector, the need to rethink approaches to the digital transformation of the military-industrial complex, taking into account internal resource constraints and external technological trends, is especially relevant.

Despite the presence of individual initiatives in the field of production automation, the introduction of digital management platforms and the use of artificial intelligence elements, the lack of a holistic system of strategic guidelines significantly complicates the formation of a coordinated policy for the digitalization of the industry. This limits the possibilities of integrating the national military-industrial complex into international defense cooperation, reduces its adaptability to crisis scenarios, and hinders the development of the innovation environment.

The digital transformation of the military-industrial complex involves the creation of a multi-level development system in which political, technological, personnel, ethical and economic aspects form a holistic architecture of innovative management. The implementation of digitalization in the defense sector requires a systemic approach based on five interrelated structural directions that form the basis for an effective transition to a digital defense-industrial model (Fig. 1).

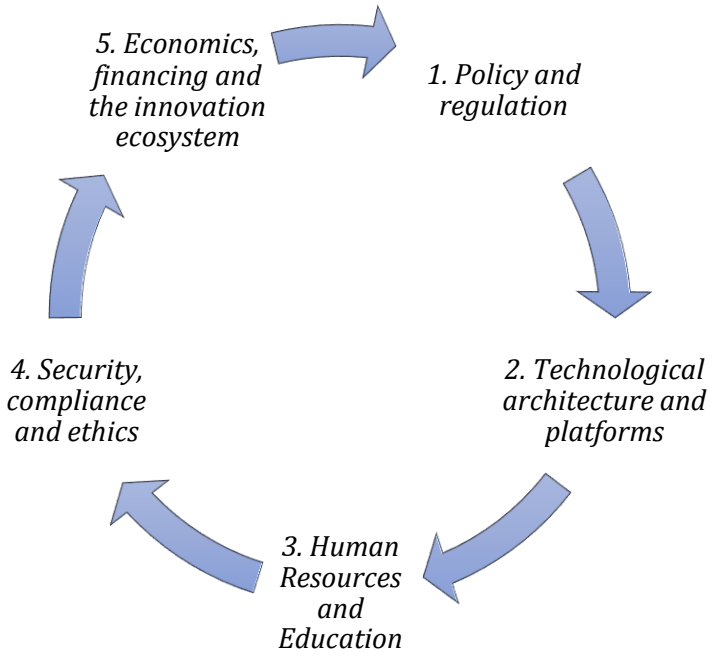

Figure 1. Main structural directions of digitalization in the global military-industrial complex
Source: Built by the author.

The first direction defines the institutional foundations of the digital transformation of the military-industrial complex. It is aimed at forming a state policy of digital sovereignty, legal regulation of data circulation, intellectual property and dual-use technologies. A necessary step is the adoption of the national "Digital Strategy of Defense-Industrial Development", which will establish standards, priorities and mechanisms for interaction between the state, business and scientific institutions. The legislative framework should include norms on cyber protection of defense data, the use of artificial intelligence in military systems and regulations for the export of digital technologies. An important task is to create an interdepartmental coordination body – the Council for the Digital Transformation of the Military-Industrial Complex, which will ensure the consistency of decisions and monitoring of policy effectiveness.

The second direction covers the formation of a unified digital infrastructure of the military-industrial complex. It should be based on a modular architecture, open standards and secure communication protocols. It is proposed to create a national defense-technological platform – an integrated environment for the development, testing and operation of digital solutions, which will ensure interaction between enterprises, scientific institutions and government agencies. The priority areas are the implementation of artificial intelligence, Big Data, quantum computing, digital twins and industrial Internet of Things (IIoT) technologies. The architecture should be built on the principles of "Zero Trust", and API standardization will ensure compatibility between subsystems. The use of cloud and edge solutions will allow the creation of a flexible and scalable ecosystem of digital production. The third direction is aimed at developing the human resource potential of the digital defense industry. The digitalization of the military-industrial complex is impossible without training a new generation of specialists – data analysts, cybersecurity engineers, modeling, system integration and military artificial intelligence specialists. It is advisable to create an educational and scientific consortium of the military-industrial complex, which will unite universities, research institutes and defense enterprises. Educational programs should combine engineering, IT and management competencies, including the ethics of digital technologies. It is recommended to introduce a state program for training "digital officers" – specialists in digital management in the defense sector, who will have the skills of strategic thinking, risk analysis and cybersecurity. The fourth direction defines the principles of creating a secure

digital environment of the military-industrial complex. The main task is to develop a comprehensive cyber defense governance system, combining technical, legal and organizational tools. It is necessary to implement cyber resilience standards, digital risk audits and compliance mechanisms with international norms (NIST, ISO/IEC 27001, Tallinn Manual 2.0). The ethical dimension involves the development of a code of conduct for the responsible use of artificial intelligence in military systems, which defines the limits of technological autonomy and the role of humans in decision-making. It is proposed to create an independent Ethics Committee for Digital Defense Technologies, which will monitor the compliance of developments with the principles of humanity, legality and international law.

The fifth direction forms the financial and economic basis of digital transformation. Its implementation involves the development of innovation and investment mechanisms to support startups, technology clusters and military-industrial complex enterprises. It is advisable to create a State Fund for Digital Defense Transformation, which will finance projects in automation, cyber defense, artificial intelligence and industrial modeling. Public-private partnerships (PPP) should play an important role in attracting venture capital and foreign investors. It is recommended to introduce tax incentives for digital innovations in the military-industrial complex, as well as create dual-purpose regional technology parks – platforms for experimental production and testing of new technologies. Thus, the five structural directions of military-industrial complex digitalization form an integrated system in which political will, technological infrastructure, human resources capacity, ethical responsibility and economic support interact within a single strategy. Their synergistic implementation will allow creating a sustainable, secure and competitive digital defense-industrial complex, which will ensure the strategic autonomy of the state.

In today's conditions of global competition and growing security challenges, the digitalization of the military-industrial complex (MIC) has become a strategic factor that determines the technological autonomy, operational efficiency and stability of states. The introduction of digital technologies in the field of defense production and management ensures not only the modernization of production processes, but also forms a new model of strategic development, where the key guidelines are innovation, integration and cyber resilience.

The experience of leading countries in the world shows that the comprehensive digital transformation of the MIC encompasses institutional, technological, personnel, ethical and financial and economic dimensions. Their synergy creates conditions for the formation of sustainable defense ecosystems capable of quickly adapting to changing combat requirements and global technological trends. At the same time, countries with a lower level of technological capitalization face problems of fragmented digitalization, which limits their integration into international defense cooperation and reduces strategic capabilities.

In this context, recommendations for strengthening structural directions of digitalization of the military-industrial complex aim to outline institutional mechanisms, technological priorities, personnel strategies, ethical standards, and financial instruments that will ensure the formation of a competitive and secure digital defense-industrial complex on a global scale, Fig. 2.

The set of recommendations for the digitalization of the defense-industrial complex should cover key areas of policy, technological architecture, cybersecurity, human capital development, financing and innovation ecosystem, forming a holistic framework for the strategic development of the industry.

In the political dimension, an important task is to introduce unified data classification standards that will determine access levels, storage periods and responsibility for their protection. For the development of public-private partnerships in the field of DefenseTech, it is necessary to create a legal framework that will include standard legal models, intellectual property rules and tax incentives. Export control of digital technologies should be carried out through automated monitoring systems, and the ethical aspects of the use of artificial intelligence in military systems should be regulated in accordance with international norms and humanitarian law.

In the technological dimension, the digitalization of the military-industrial complex should be based on a single integration platform (Core Hub), which will ensure interaction between PLM, ERP and MES systems via API bus, metadata registries and service catalogs. It is advisable to implement a hybrid IT infrastructure that combines local capacities for critical components with certified cloud solutions for analytics. The use of digital twins, MLOps, DevSecOps and DevOps practices will allow to optimize production processes and ensure fast and secure deployment of models. In the field of cybersecurity, it is necessary to create a multi-layered protection system that will cover physical, network, hardware and

software components. The use of SIEM and SOAR systems, regular Red/Blue-team exercises, as well as the hardware roots of trust program will ensure the stability and authenticity of critical elements. It is important to implement secure software lifecycle (secure SDLC) standards and automated export management mechanisms with cryptographic access auditing.

1. Policy and regulation	2. Technological architecture and platforms	3. Human Resources and Education	4. Security, compliance and ethics	5. Economics, financing and the innovation ecosystem
•Create a national "Roadmap for Digitalization of the Military-Industrial Complex" with 5-/10-/15-year goals and responsibilities •Establish uniform standards for classification of military-industrial complex data (access categories, TTL, storage obligations) •Develop a legal framework for PPP in DefenseTech (legal templates, IP rules, tax incentives) •Regulate export controls for digital technologies (including algorithms and H/W) with automated control tools •Incorporate provisions on ethical control of the use of AI in military systems	•Implement a single integration platform (Core Hub) — API bus, metadata registries, service catalog (MVP: PLM↔ERP↔MES integration) •Adopt a hybrid infrastructure model: on-prem for critical H/W + certified (secure) cloud for analytics •Deploy digital twins for key products and production lines •Introduce MLOps and DevSecOps/DevOps practices for accelerated, secure deployment of models •Ensure exchange standards (APIs, data schemas) and compatibility with international standards (NATO/EU, where relevant)	•National training program "Defence Digital Fellows" (bachelor's/master's/retraining): AI, cyber, IIoT, systems engineering •Competence centers (Digital Labs) at universities and defense industry enterprises •Policy for attracting diaspora experts and internships in international DefenseTech clusters •KPI-oriented certification programs for engineers, operators and managers of digital systems	•Implement a multi-layered security model at the state/enterprise level: physical, network, hardware, software •Mandatory SIEM+SOAR in key areas; regular Red/Blue-team exercises •Hardware roots of trust program for critical boards and communication channels •Standards for secure software/software lifecycle (secure SDLC) •Automated export/export license management mechanisms with cryptographic audit of access to code/models	•Introduce targeted R&D funding (matching grants) for DefenseTech startups •Tax incentives for localization of production of critical digital components •Tech Sovereignty Fund for investments in strategic platforms (digital twins, crypto H/W) •Stimulate co-financing of pilots through PPP models and MVP procurement programs •Support the cluster model: hubs (university-incubator-enterprise) with an open API market •Acceleration programs with a focus on the transition from civil innovations to DefenseTech •Platform-market for certified modules/services with a security and compatibility rating

Figure 2. Recommendations for strengthening the main structural directions of digitalization in the global military-industrial complex

Source: Built by the author.

Human capital development involves the creation of a national program "Defense Digital Fellows", which will cover the training and retraining of specialists in the fields of artificial intelligence, cybersecurity, IIoT and systems engineering. Competence centers (Digital Labs) at universities and enterprises will facilitate technology transfer, and the involvement of diaspora experts and internships in international clusters will integrate global experience.

The financial component of digitalization should include targeted R&D funding through the matching grants mechanism for startups, tax incentives for the localization of production of critical

components and the creation of the "Tech Sovereignty" investment fund. Co-financing of pilot projects through public-private partnerships and MVP procurement will contribute to the rapid implementation of innovations.

The innovation ecosystem should develop based on a cluster model that combines universities, incubators and enterprises in the format of open hubs. Acceleration programs should be aimed at transforming civilian innovations into solutions for DefenseTech. The creation of a market platform for certified modules and services with security and compatibility ratings will ensure transparency and competitiveness of digital components. Taken together, these recommendations form a multidimensional framework for the digital transformation of the military-industrial complex, capable of ensuring its sustainability, innovation and strategic effectiveness. In the 21st century, the digitalization of the defense-industrial sector is becoming a key factor in the defense capability, technological autonomy and strategic stability of the state, defining new development guidelines at the intersection of innovation, security and interoperability.

6. Conclusions

The study of the strategic guidelines for the digital transformation of the military-industrial complex (MIC) of the world shows that digitalization has become a key factor in the modernization of defense industries and the formation of military-industrial potential in the 21st century. It determines the competitiveness of states, their ability to achieve technological autonomy, operational efficiency and strategic stability in the face of global security challenges.

The strategic guidelines for the digital transformation of the MI of the world define a new paradigm of the defense economy, where innovation, security and interoperability become key factors for development. Further research should contribute to the formation of a comprehensive model of digital modernization capable of ensuring the stability and competitiveness of states in the global security environment.

References

1. Ukraine deploys digital twins for rebuild effort. (2022). *Build in Digital.* https://buildindigital.com/ukraine-deploys-digital-twins-for-rebuild-effort/
2. Artificial Intelligence Strategy. (2021). *Defense Logistics Agency*. https://lnk.ua/HWgmMS3MX
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. Cyber Defence. (2024). *Brussels: NATO*. https://www.nato.int/cps/en/natohq/topics_78170.htm
6. Defence-Critical Materials in Australia: Strategic Importance. (2025). *Discovery Alert*. https://discoveryalert.com.au/news/defence-critical-materials-australia-strategy-2025
7. Defense Logistics: The Role of Artificial Intelligence. (2022). *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA1234-1.html
8. Defense-Tech Startup Hadrian Raises $260 Million for New Robot Factory. (2025). *WSJ*. https://www.wsj.com/articles/defense-tech-startup-hadrian-raises-260-million-for-new-robot-factory
9. Fiott, D. (2025). Defence Innovation Trends: EDF Snapshot 2021–2024. *CSDS*. https://csds.vub.be/publication/defence-innovation-trends-a-data-snapshot-of-the-european-defence-fund-2021-2024/
10. Future of Army Logistics: Exploiting AI, Overcoming Challenges and Charting the Course Ahead. (2024). *U.S. Army*. https://lnk.ua/p3KgPFEbx
11. Grieves, M., & Vickers, J. (2017). Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In: Kahlen F.-J., Flumerfelt S., Alves A. (Eds.). *Transdisciplinary Perspectives on Complex Systems*. Cham: Springer.
12. Global Combat Support System – Army (GCSS-Army). (2022). *U.S. Army*. https://www.army.mil/article/252994/gcss_army_enables_data_driven_decisions

13. Kim, T. I., & Ukrainets, Y. M. (2022). Viiskovo-promyslovyi kompleks u suchasnii svitovii ekonomitsi: peredumovy, faktory, tendentsii rozvytku [Military-industrial complex in the modern world economy: prerequisites, factors, development trends]. *Ekonomika ta suspilstvo – Economy and Society*, (39). https://doi.org/10.32782/2524-0072/2022-39-33 (in Ukrainian)
14. Logistics Under Threat: Future Scenarios and Technology Need. (2023). *Defense Advanced Research Projects Agency (DARPA).* https://www.darpa.mil/news-events/2023-logistics
15. 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/
16. 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
17. Military Technology Trends 2025. (2025). *StartUs Insights*. https://www.startus-insights.com/innovators-guide/military-technology-trends/
18. Networked Combat and the Future of Military Logistics. (2023). *Center for Strategic and International Studies (CSIS).* https://www.csis.org/analysis/networked-combat-and-future-military-logistics
19. Nicastro, L. (2024). DARPA and the Future of Defense Innovation. *RAND Corporation*. https://www.rand.org/pubs/research_reports/RRA889-1.html
20. Pustoviit, R. F. (2021). Teoretyko-metodolohichni zasady zabezpechennia voienno-ekonomichnoi bezpeky Ukrainy [Theoretical and methodological principles of ensuring the military-economic security of Ukraine]. *Naukovyi visnyk Natsionalnoho universytetu oborony Ukrainy – Scientific Bulletin of the National Defense University of Ukraine, 3*(60), 21–27. (in Ukrainian)
21. Pustoviyt, R. F. (2016). Viiskovo-ekonomichna bezpeka derzhavy [Military-economic security of the state]. *Ekonomika ta derzhava – Economy and State*, (7), 23–28. (in Ukrainian)
22. Russia: statistics. (2024). *Data Commons Place Explorer*. https://lnk.ua/LNJcCmCEE
23. 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
24. Semenenko, O. M., Boiko, R. V., Voronchenko, I. O., & Taran, O. V. (2022). Otsiniuvannia rivnia voienno-ekonomichnoi bezpeky krain svitu ta Ukrainy za rezultatamy analizu dynamiky yikh voienno-ekonomichnykh pokaznykiv rozvytku (2012–2021 rr.) [Assessment of the level of military-economic security of countries of the world and Ukraine based on the results of the analysis of the dynamics of their military-economic development indicators (2012–2021)]. *Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen Natsionalnoho universytetu oborony Ukrainy imeni Ivana Cherniakhovskoho*, *2*(75), 76–85. (in Ukrainian)
25. Semenenko, O., Voronchenko, I., Moskalenko, I., Ponomarenko, S., Saienko, S., & Borysenko, I. (2021). Analiz ta otsinka vplyvu voienno-ekonomichnykh faktoriv na stan rozvytku Zbroinykh syl Ukrainy ta riven yii voiennoekonomichnoi bezpeky [Analysis and assessment of the impact of military-economic factors on the state of development of the Armed Forces of Ukraine and the level of its military-economic security]. *Journal of Scientific Papers "Social Development and Security"*, *11*(3), 45–57. (in Ukrainian)
26. Supply Chain Disruptions Drive Revenue Declines. (2023). *Defense Industry Europe.* https://defence-industry.eu/supply-chain-disruptions-drive-revenue-declines-for-lockheed-martin-and-rtx/