Electronic scientific and practical journal

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

#33 (2025)
October '25

WWW.SMART-SCM.ORG
ISSN 2708-3195
DOI.ORG/10.46783/SMART-SCM/2025-33

ISSN 2708-3195

Electronic scientific and practical collection
INTELLECTUALIZATION OF LOGISTICS
AND SUPPLY CHAIN MANAGEMENT

Electronic scientific and practical publication in economic sciences

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): **Order of the Ministry of Education and Culture of Ukraine dated October 10, 2022 No. 894 (Appendix 2)**

Field of science: Economic.
Specialties: C1 (051) – Economics; D3 (073) – Management

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2025-33

The electronic magazine is included in the international scientometric databases:
Index Copernicus, Google Scholar

Released 6 times a year

№ 33 (2025)
October 2025

Kyiv - 2025

Founder: Viold Limited Liability Company

The electronic scientific and practical journal is registered in international scientometric data bases, repositories and search engines. The main characteristic of the edition is the index of scientometric data bases, which reflects the importance and effectiveness of scientific publications using indicators such as quotation index, h-index and factor impact (the number of quotations within two years after publishing).

In 2020, the International Center for Periodicals (ISSN International Center, Paris) included the Electronic Scientific and Practical Edition "Intellectualization of logistics and Supply Chain Management" in the international register of periodicals and provided it with a numerical code of international identification: ISSN 2708-3195 (Online).

Recommended for dissemination on the Internet by the Academic Council of the Department of Logistics NAU (No. 7 of February 26, 2020). Released 6 times a year. Editions references are required. The view of the editorial board does not always coincide with that of the authors.

Electronic scientifically and practical journal "Intellectualization of logistics and Supply Chain Management" included in the list of scientific publications of Ukraine in the field of economic sciences (category "B"): ***Order of the Ministry of Education and Culture of Ukraine dated October 10, 2022 No. 894 (Appendix 2)***

Field of science: Economic.

Specialties: C1 (051) – Economics; D3 (073) – Management

t.me/smart_scm
facebook.com/Smart.SCM.org
twitter.com/ScmSmart

DOI: https://doi.org/10.46783/smart-scm/2025-33
e-mail: support@smart-scm.org

тел.: (063) 593-30-41
https://smart-scm.org

Contents

DOI: https://doi.org/10.46783/smart-scm/2025-33-2

UDC 658.7:355.45:005.21:005.342
JEL Classification: L64, M11, D81, R41, O32.
Received: 28 August 2025

Hryhorak M.Yu. Doctor of Economics, Associate Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0002-5023-8602
Researcher ID – AAK-2963-2021
Scopus author id: – 57208222758
E-Mail: hryhorak.mariia@lll.kpi.ua

Marchuk V.Ye. Doctor of Technical Sciences, Professor, Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0003-0140-5416
Researcher ID – S-6514-2018
Scopus author id: – 57212323045
E-Mail: v.marchuk.kpi@gmail.com

Harmash O.M. PhD in Economics, Associate Professor, Associate Professor of the Department of International Business and Logistics, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0003-4324-4411
Researcher ID – I-4542-2018
Scopus author id: – 57218381499
E-Mail: o.harmash.kpi@gmail.com

ENHANCING THE RESILIENCE, ADAPTABILITY, AND ANTIFRAGILITY OF DEFENSE INDUSTRY SUPPLY CHAINS UNDER CONDITIONS OF HIGH TURBULENCE

Mariia Hryhorak, Volodymyr Marchuk, Oleh Harmash. "Enhancing the resilience, adaptability, and antifragility of defense industry supply chains under conditions of high turbulence". *The article substantiates the theoretical and methodological foundations and develops practical approaches to enhancing the resilience, adaptability, and antifragility of supply chains within Ukraine's defense industry under conditions of high environmental turbulence. The specific nature of defense industry supply chains is defined as complex socio-technical systems operating under the influence of geopolitical risks, restricted access to critical resources and technologies, cyber threats, and strict regulatory requirements. The study systematizes the factors affecting the resilience, adaptability, and viability of defense supply chains and identifies the key threats, barriers, and drivers of their development. The essence of the concepts of resilience, adaptability, and antifragility – which* *together constitute the foundation of supply chain viability – is revealed, and the rationale for their integrated application in defense industry management is provided. A system of managerial measures is proposed to foster flexible organizational structures, promote partnership-based interaction among business ecosystem participants, and implement modern digital technologies (IoT, Big Data, AI, blockchain, digital twins) that enhance the ability of supply chains to rapidly respond, recover, and transform during crises. The practical significance of the study lies in formulating scientifically grounded recommendations for Ukraine's defense enterprises to build viable, adaptive, and antifragile supply chains capable of ensuring the continuity of defense production, strengthening national security, and maintaining economic stability amid wartime and global instability.*

Keywords*:* supply chains, defense industry, resilience, adaptability, antifragility, viability, digital technologies, risk management

Марія Григорак, Володимир Марчук, Олег Гармаш. «Підвищення стійкості, адаптивності та антикрихкості ланцюгів постачання підприємств оборонно-промислового комплексу в умовах високої турбулентності». *У статті обґрунтовано теоретико-методичні засади та розроблено практичні підходи до підвищення стійкості, адаптивності та антикрихкості ланцюгів постачання підприємств оборонно-промислового комплексу (ОПК) України в умовах високої турбулентності зовнішнього середовища. Визначено специфіку ланцюгів постачання ОПК як складних інтегрованих соціо-технічних систем, що функціонують під впливом геополітичних ризиків, обмежень доступу до ресурсів і технологій, кіберзагроз та жорстких регуляторних вимог. У роботі систематизовано чинники, які впливають на стійкість, адаптивність та життєздатність оборонних ланцюгів постачання, виокремлено ключові загрози, бар'єри та драйвери їх розвитку. Розкрито сутність концепцій стійкості, адаптивності та антикрихкості, що утворюють основу життєздатності систем постачання, та обґрунтовано доцільність їхнього інтегрованого застосування в управлінні ОПК. Запропоновано систему управлінських заходів, спрямованих на формування гнучких організаційних структур, розвиток партнерської взаємодії учасників бізнес-екосистем і впровадження сучасних цифрових технологій (IoT, Big Data, AI, блокчейн, цифрові двійники), які підвищують здатність ланцюгів постачання до швидкого реагування, відновлення та трансформації під час кризових ситуацій. Практичне значення дослідження полягає у формуванні науково обґрунтованих рекомендацій для підприємств ОПК України щодо побудови життєздатних, адаптивних і антикрихких ланцюгів постачання, здатних забезпечити безперервність оборонного виробництва, зміцнення національної безпеки та стійкість економіки в умовах війни та глобальної нестабільності.*

Ключові слова: ланцюги постачання, оборонно-промисловий комплекс, стійкість, адаптивність, антикрихкість, життєздатність, цифрові технології, управління ризиками.

Introduction. The contemporary operating environment of enterprises within the defense-industrial complex (DIC) is characterized by an unprecedented level of turbulence driven by both global and regional challenges. The armed aggression against Ukraine, large-scale destruction of industrial and transport infrastructure, disruptions in the supply of critical resources, intensifying international competition, and stringent sanctions have created a complex environment in which DIC enterprises must ensure the continuity of production and the fulfillment of state defense contracts. Under such conditions, effective supply chain management becomes not only an essential component of economic activity but also a critical factor of national security.

The supply chains of defense-industrial enterprises possess a number of specific characteristics, including a high degree of integration with international suppliers, dependence on imported components, the necessity to comply with strict standards of quality and confidentiality, as well as constraints associated with secrecy regimes and export control regulations. Simultaneously, warfare and geopolitical instability significantly increase the vulnerability of these supply chains, leading to supply disruptions, rising material costs, loss of suppliers, and, in some cases, a complete breakdown of logistical connections.

In this regard, the formation of resilient, adaptive, and antifragile supply chains acquires strategic importance for defense-industrial enterprises. In this context, resilience should be understood as the ability of the supply chain to maintain its functionality under crisis conditions, while adaptiveness refers to its capacity to promptly respond to environmental changes, reconfigure logistical and production processes, engage alternative suppliers, and integrate new technologies.

It should be emphasized that existing scientific approaches to supply chain management are primarily focused on civilian industries and do not fully consider the specific features of the defense-industrial sector, in particular, the increased role of state regulation, the strategic sensitivity of products, and the necessity of accounting for military and political risks. This situation creates a scientific gap that requires comprehensive research and the development of new models and managerial solutions aimed at ensuring the resilience and adaptiveness of defense-industrial supply chains under conditions of high turbulence.

Therefore, the study of methods for enhancing the resilience and adaptability of supply chains within the defense-industrial complex is of exceptional relevance, both for improving the economic efficiency of the sector and for strengthening the overall defense capability of the state.

Literature Review. The issues of resilience, adaptability, and fragility of supply chains in recent years have attracted increasing attention in global academic literature due to the growing uncertainty and turbulence of the business environment. This is driven both by escalating geopolitical risks and by the rapid development of technologies that are transforming logistics processes.

In foundational research by Ponomarov and Holcomb (2009) [1], supply chain resilience is defined as the system's ability to withstand disruptions, adapt to them, and recover while maintaining its essential functions. The authors emphasize the interconnection between supply chain elements and identify flexibility, redundancy, and adaptability as key components of resilience. These ideas were further developed by Petty et al., who proposed practical tools for assessing an organization's readiness for disruptions [2]. Resilience is an essential attribute of a supply chain for short-term survival and a critical capability for long-term adaptation and prosperity. A particular emphasis is placed on a proactive approach to risk management, which involves identifying potential threats, planning mitigation measures, and preparing recovery scenarios.

The study by Pires Ribeiro and Barbosa-Povoa (2018) [3] broadened the concept of resilience by including the supply chain's ability not only to recover from crises but also to maintain stable operations at acceptable costs and within reasonable timeframes. Melnyk et al. (2010) provided an even broader perspective on the future of supply chains, which must balance efficiency, security, sustainability, resilience, and innovativeness according to customer needs and external challenges.

Further development of supply chain resilience theory is associated with the works of various authors who integrated multiple perspectives. In particular, Dmitry Ivanov substantially expanded the theoretical and methodological foundations by proposing a comprehensive three-dimensional model for assessing supply chain resilience that encompasses product, process, technological, and social aspects [4]. He also emphasized that resilience should be considered in conjunction with adaptability and the system's transformational capacity – an especially relevant perspective under prolonged crises such as pandemics or armed conflicts [5].

As disruptions and uncertainty have become central themes in supply chain literature [6], researchers [7] have shifted their focus to two dominant strategies – redundancy and flexibility – proposed as means to mitigate the impact of disruptions. They identified four broad conceptual strategies – insurance, acceleration, strategic adaptive capability, and reconfiguration – each uniquely serving to reduce the likelihood and scale of disruptions within supply chains. Other scholars [8–10] have combined different aspects of resilience discussed in the literature using quantitative methods in the design or redesign of supply chains.

At the same time, contemporary literature recognizes that the traditional engineering-based interpretation of resilience is insufficient. Engineering resilience aims at optimality and structural safety and is measured by the speed of returning to equilibrium (recovery time) and resistance to disturbances (survival time). Researchers are increasingly moving toward the concept of socio-ecological resilience, which considers environmental dynamics, uncertainty, and the need for continuous transformation of supply chains [9, 10]. Socio-ecological resilience allows for experimentation and adaptive design since supply chains must evolve over time. This requires managers to foster adaptability and transformability, thereby anticipating and influencing events occurring beyond the immediate supply chain. The same idea is supported by other scholars [11], who argue that maintaining and developing resilience requires accounting for a wide spectrum of social and environmental changes. Purposeful transformation of the system is necessary for it to continue delivering what holds fundamental value for society.

Summarizing theoretical research on resilience in supply chains based on a systematic review of the literature, it can be concluded that resilience is a multidimensional and interdisciplinary concept. It has evolved from generating reactive strategies to cope with disruptive events toward the development of proactive pre- and post-disruption strategies. Currently, the domain of supply chain resilience encompasses several capabilities: prevention, resistance, response, recovery, and market adaptation. Moreover, resilience includes the ability for cumulative learning and continuous improvement, becoming a strategic capability for enhancing competitiveness – an important reason for its inclusion in modern supply chain management frameworks [12].

Against this background, a new concept – antifragility – has emerged. It interprets disruptions and crises not only as threats but also as opportunities for strengthening, learning, and development of systems. The term antifragility was introduced by Nassim Nicholas Taleb in his 2012 book Antifragile: Things That Gain from Disorder. Taleb highlighted that in complex systems there exist not only resilient or fragile structures but also those that do not merely withstand stress and shocks but grow stronger and evolve under their influence. This qualitatively distinguishes antifragility from resilience, which merely denotes the ability to preserve functionality or return to the original state after a disruption [13].

One of the leading researchers integrating the concepts of resilience and antifragility in supply chains is Dmitry Ivanov. In his works, he proposed combining antifragility with resilience theory and developed dynamic models demonstrating how supply chains can reconfigure and strengthen after disruptions. He also introduced the concept of viability as a logical continuation of antifragility [14, 15].

Considering the complexity, multi-tiered nature, and geographic dispersion of modern supply chains, traditional approaches to assessing their resilience and antifragility – focused solely on internal processes or individual organizations – are no longer adequate. Supply chains increasingly function within broader business ecosystems, where their resilience and capacity for recovery depend not only on internal reserves but also on the nature of interactions among various stakeholders – manufacturers, suppliers, logistics operators, government institutions, research organizations, and the private sector. Therefore, it is appropriate to assess the resilience and antifragility of supply chains through the lens of these interactions – considering the level of partnership, readiness for collaboration, information exchange, technology sharing, and resource coordination [16]. Such an approach allows for a more precise identification of system vulnerabilities while fostering the development of long-term, trust-based relationships among participants, thereby enhancing the ecosystem's ability to adapt, recover swiftly after crises, and transform in response to new challenges.

In the context of the defense-industrial complex (DIC), this issue becomes particularly significant. Supply chains within the DIC are, on the one hand, highly complex, multi-layered, and technologically intensive; on the other hand, they are critically important for ensuring national security, defense resilience, and the state's strategic autonomy. A seminal paper [17] presented the results of a discussion titled "Research Directions in Defense Logistics." Participants of that discussion drew several important conclusions: supply chain management is a critical success factor not only for industrial and commercial enterprises but also for military operations; although there remains a gap between civilian and military research, there exists an opportunity to leverage existing knowledge and expertise to recognize that competition for defense contracts increasingly occurs not between individual firms but between resilient, adaptive, and interconnected supply chains.

In recent academic publications, it is increasingly emphasized that the successful functioning of defense-industrial enterprises and their ability to fulfill defense orders directly depend on the efficiency, resilience, and flexibility of their supply chains (Ekström [18]; Hilletofth & Skoglund, 2020, 2023 [19–21]). A study of the Swedish defense-industrial complex demonstrated that under military conditions, an optimal approach involves combining the principles of just-in-time, just-in-case, and just-enough. Such a synthesis enables achieving a balance between efficiency and resilience under uncertainty and high disruption risk. Highlighting the importance of responsiveness, recovery, and planning in military supply chains, other authors [22] underscored the need for continuous improvement of logistics strategies and assessment tools to enable military organizations to overcome disruptions effectively and sustain operational efficiency. In the context of global turbulence, the importance of risk management within the defense industry is increasing, particularly given its dependence on foreign supplies [23].

In the studies by Sani et al. (2023) [24–26] and Cabrera et al. (2023) [27], it is substantiated that military supply chains face a set of unique challenges, including:

– excessive dependence on a limited pool of suppliers of critical materials and components;

– high regulatory and technical complexity;

– the need to ensure both informational and physical security at all stages of the supply process;

– constraints on geographical diversification due to strategic and political factors.

It is also worth noting that:

– the application of the concept of antifragility to military supply chains remains at an early stage of theoretical development;

– the integration of digital technologies – such as blockchain, digital twins, and artificial intelligence – aimed at enhancing the resilience and adaptability of defense supply chains requires more in-depth research;

– the interconnection between the resilience of defense-industrial supply chains and sustainable development concepts, which are gaining increasing traction in the EU's defense-industrial sector (notably within Horizon Europe programs), remains insufficiently explored.

At the current stage of the development of theory and practice in defense-industrial supply chain management, there is a noticeable disproportion between quantitative and qualitative approaches to assessing their efficiency, resilience, and antifragility. Most academic studies in this area focus primarily on qualitative analysis, the construction of theoretical models, or conceptual frameworks [28–29], which, although of significant theoretical value, remain distant from the practical needs of supply chain participants. Meanwhile, practical diagnostic tools, quantitative assessment methods, and comparative analyses of resilience, adaptability, and antifragility levels in defense supply chains remain underdeveloped and insufficiently tested in real-world industrial contexts.

Particular attention should be paid to the issue of interaction between defense-industrial enterprises and private sector companies. This dimension is critically important for ensuring the flexibility, innovativeness, and technological competitiveness of defense-industrial supply chains. However, mechanisms of such interaction – legal regulation, information exchange, standardization of requirements, and the development of partnership-based cooperation models – remain inadequately studied, creating additional risks for the efficiency and resilience of defense supply systems.

Summarizing the above, it should be emphasized that the modern military supply network must be capable of promptly adapting to changes in the external environment, requirements, and threats; recovering quickly from disruptions; and maintaining a high level of resilience under uncertainty. To achieve this, it is necessary – already at the design stage of such a network – to clearly define the properties, functional principles, and managerial mechanisms that will enhance its viability, taking into account both internal structural characteristics and external factors of interaction with the private sector.

Purpose of the Article. The purpose of this article is to substantiate the theoretical foundations and propose practical approaches to enhancing the resilience, adaptability, and antifragility of the supply chains of Ukraine's defense-industrial complex (DIC) through the lens of partnership-based interactions among participants of business ecosystems and the integration of modern digital technologies under conditions of global turbulence and military threats.

Research Objectives:

1. To clarify the essence and specific characteristics of defense-industrial supply chains as complex integrated systems.
2. To systematize the challenges, threats, barriers, and drivers of the DIC supply chain development, taking into account the factors of resilience, adaptability, and antifragility.
3. To substantiate the feasibility of applying the concept of business ecosystem interaction for the assessment and enhancement of the viability of DIC supply chains.
4. To determine the role of modern digital technologies in ensuring the resilience, adaptability, and antifragility of supply chains.
5. To formulate practical recommendations for improving the efficiency and viability of Ukraine's DIC supply chains under wartime conditions and global instability.

Research Methodology. The study employs a comprehensive interdisciplinary approach that integrates systems analysis, elements of the theories of resilience, adaptability, and antifragility, the concept of business ecosystems, and modern supply chain management frameworks. The research utilizes content analysis of scientific publications, comparative analysis of existing approaches to assessing resilience, adaptability, and antifragility in supply chains, expert evaluation of current threats and challenges, as well as structural and logical generalization to develop practical recommendations.

Particular attention is devoted to the specific operational features of Ukraine's defense supply chains under armed conflict conditions and to the application of digital technologies aimed at enhancing their viability and sustainability.

Presentation of the main results. Supply chain management represents one of the key components of modern management, ensuring the coordination and integration of all processes related to the movement of materials, information, and financial resources from the supplier to the end consumer. Under conditions of increasing uncertainty and turbulence in the external environment, the concepts of resilience, adaptability, and antifragility of supply chains acquire particular significance – especially within the defense-industrial complex (DIC).

In scientific and applied literature, the term "defense-industrial supply chain" is often used without a precise definition of its specific characteristics and structure, which complicates both theoretical research and the practical development of strategies aimed at enhancing the resilience, adaptability, and antifragility of such systems. Therefore, it is necessary to clarify this concept.

A defense-industrial supply chain (DIC supply chain) is a complex, integrated system of interconnected organizations, processes, and flows that ensure the development, production, delivery, technical maintenance, and disposal of defense-oriented products, services, and technologies, with the ultimate goal of meeting the needs of national security and defense. Unlike traditional commercial supply chains, DIC supply chains are characterized by a heightened level of strategic importance, stringent requirements for security, confidentiality, technological sophistication, and regulatory oversight.

They possess a unique configuration that includes both state and private sector actors, dual-use elements, and specialized logistical and informational solutions (Fig. 1). Furthermore, such supply chains are inextricably linked with national security and defense systems, which imposes additional requirements for their reliability and their ability to recover rapidly after external or internal disruptive impacts.

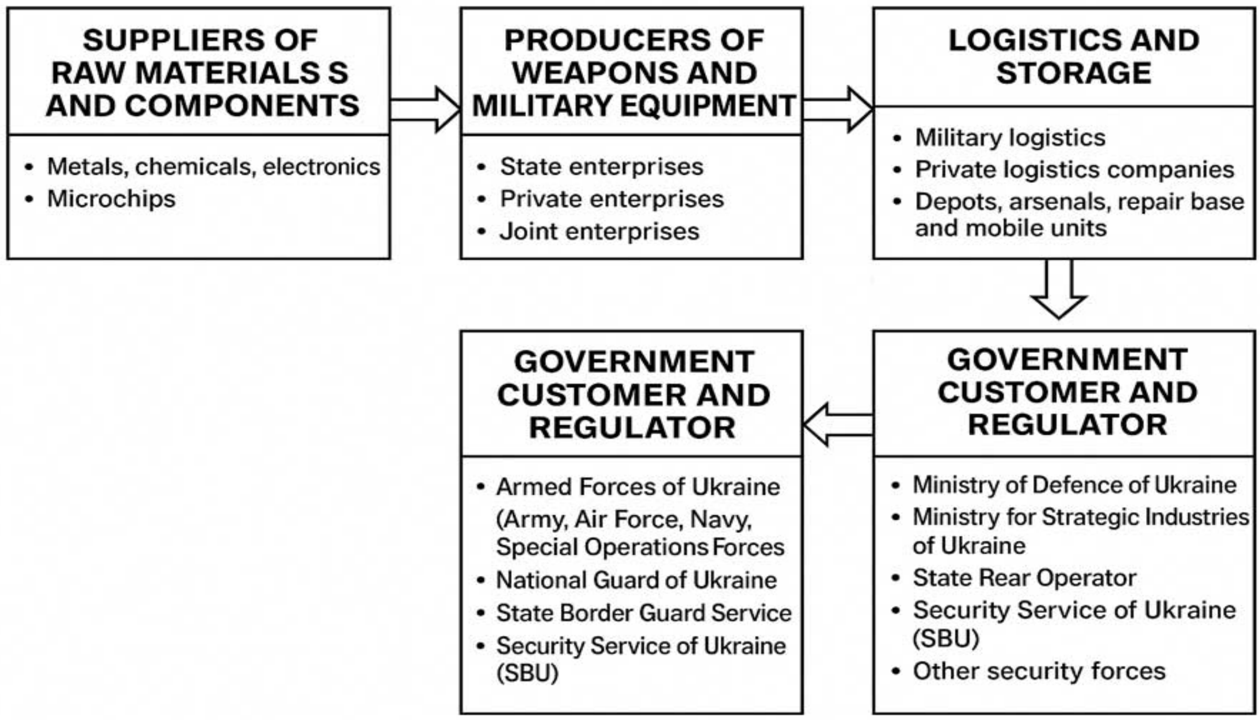

Figure 1 – General configuration of defense-industrial supply chains
Source: Developed by the authors

The configuration of the defense-industrial supply chain (DIC supply chain) comprises five principal blocks. The first block, "Suppliers of raw materials and components," constitutes the foundation of the entire chain. Without high-quality and uninterrupted supplies of materials and components, the production of weapons and military equipment (WME) is impossible. Within this block, various types of linkages operate – horizontal, vertical, and import-based. Horizontal linkages characterize interactions among different domestic suppliers that coordinate volumes and delivery schedules of materials of various purposes. Vertical linkages form between suppliers at different tiers, jointly ensuring the supply of finished assemblies, modules, and components. Import linkages reflect the dependence of certain domestic suppliers on foreign materials or technologies, which creates additional operational risks for the chain.

This block also maintains direct contractual relationships with WME manufacturers for the supply of raw materials, semi-finished products, and components. Manufacturers provide technical specifications and quality requirements for supplied items. Furthermore, the relationship with the state customer – primarily the Ministry of Defence – plays a decisive role in setting priorities for the development of national suppliers, attracting investment, and establishing certification and standardization requirements for materials.

The "Manufacturers of Weapons and Military Equipment" block comprises plants and enterprises that transform raw materials, semi-finished products, and components into finished WME. This block sustains internal linkages among enterprises within the state conglomerate (e.g., Ukroboronprom), private manufacturers, state and private research and development institutions, design bureaus, and contractors executing specific orders for components, assemblies, or services. External functions include continuous monitoring of the quality and conformity of supplied materials and components to technical requirements; management of logistics and storage of finished products; and organization of transportation to the customer.

Key external functions of this block also encompass fulfillment of the provisions of the State Defence Order (SDO); reporting on the progress and outcomes of its implementation; participation in tender and competitive procedures; receipt and allocation of funding from the state customer; and obtaining feedback from end users – most notably via the Ministry of Defence of Ukraine – regarding the operational effectiveness of WME under combat conditions. Such feedback is critically important for rapid product modernization, elimination of identified deficiencies, and enhancement of the combat effectiveness of systems.

The "Logistics and Storage" block is responsible for organizing the movement of products from manufacturers to end users and for ensuring appropriate preservation of weapons, equipment, components, and spare parts at all stages of the supply chain. Primary functions of this block include coordination with various modes of transport (road, rail, air) for efficient cargo movement; interaction among different types of warehouses – central, regional, and mobile (field); inventory management; ensuring the security of stored items and compliance with storage conditions; provisioning of spare parts, tools, and equipment for maintenance and repair; transfer of damaged equipment to repair and refurbishment facilities; and the implementation and use of modern logistics information systems for monitoring stock levels, movements, and locations of materiel.

The block's external linkages cover coordination with WME manufacturers for receipt of products into warehouses and organization of their onward transportation; execution of orders from the state customer (Ministry of Defence of Ukraine) regarding movement, allocation, and prioritization of weaponry and equipment deliveries in line with the needs of the Armed Forces of Ukraine; direct delivery of WME, ammunition, and material-technical supplies to military units, training ranges, and forward positions; route planning and provision of security for transport columns and logistical convoys; and coordination of the security of particularly sensitive or hazardous cargoes with relevant security services and specialized agencies.

The "State Customer and Regulator" block plays a central role in determining what, how much, and at what price must be produced to meet the needs of the security and defence sector. It also shapes the legal, financial, and organizational environment necessary for the effective operation of the DIC. Core functions include close coordination with the General Staff of the Armed Forces for defining volumes, nomenclature, and specifications of required WME on the basis of combat experience, threat analysis, and forecasts; coordination of the formation of the State Defence Order (SDO) and state programs for DIC development; interaction with the Ministry of Defence to optimize procurement procedures with particular emphasis on transparency in the acquisition of non-lethal materiel, logistic support items, and equipment; regulation of issues related to international trafficking of arms, technologies, and licensed export/import; and resolution of complex interagency and strategic tasks for the development of the DIC.

External activities of this block include concluding contracts with WME manufacturers; securing financing and effecting payments for completed work; oversight of SDO execution, technical supervision, and acceptance of finished products; formulation and approval of product and component quality requirements; issuing directives on the allocation and distribution of weapons and military equipment and coordinating logistical operations; receiving requests from military units and analyzing weapon performance in combat to inform future orders, modernization programs, and import substitution initiatives; and engagement with international partners on matters of military-technical assistance, joint production, cooperation in research and development, and technology transfer.

The "End Users" block – primarily the Armed Forces of Ukraine and other security services – comprises the direct users of WME, whose practical experience is invaluable for product improvement. Principal functions of this block include supplying combat experience, tactical practices, and lessons learned from real-world employment of WME; generating requests for specific types of armament tailored to the tasks of particular units and service branches; coordinating with rear services for receipt of WME, ammunition, spare parts, fuel, and other material-technical provisions; and providing maintenance and light repairs of equipment directly within combat units or at forward positions.

This block also maintains active external interactions, notably: receipt of WME and material-technical resources from warehouses or via direct delivery to positions; provision of feedback via the Ministry of Defence or directly to designers, engineers, and manufacturers regarding field requirements, remarks, and urgent needs; participation in the formulation of modernization requirements based on assessments of effectiveness, reliability, ergonomics, and adaptability to combat conditions; and submission of reports and recommendations to the state customer that form the basis for adjustments to future State Defence Orders and technical specifications (see Fig. 2).

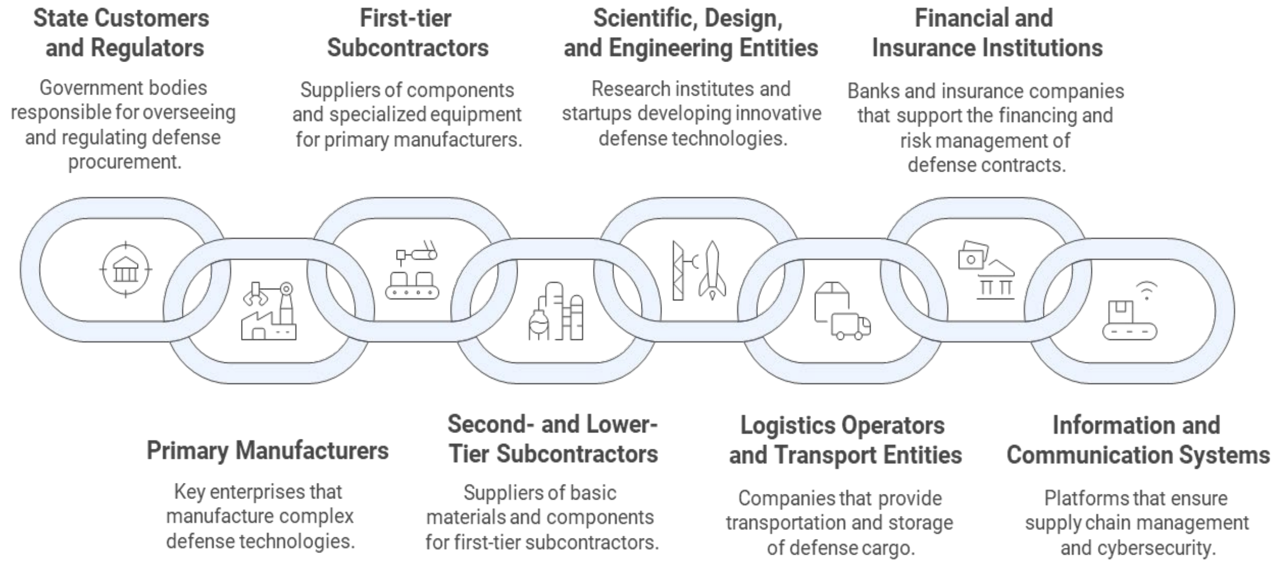

Figure 2 – Structure of the Supply Chain in the Defense-Industrial Complex
Source: Developed by the authors

Thus, feedback from end users is critically important for the closure and overall effectiveness of the entire supply chain within the defense-industrial complex (DIC). Consequently, the defense-industrial ecosystem represents a multilevel system of actors that interact in the processes of creating, supplying, and maintaining military and dual-use technologies. Its functioning is ensured by a network of state, industrial, scientific, logistical, and financial institutions, each performing defined functions in shaping the nation's defense capabilities and maintaining technological sovereignty, namely:

1. State Customers and Regulators:

– Ministries of Defense;

– Security and intelligence agencies;

– Defense procurement agencies;

– Certification and standardization authorities;

– International defense alliances (where cooperation exists).

2. Prime Contractors:

– Key enterprises of the defense industry;

– System integrators;

– Developers of complex technological solutions (aviation, armored vehicles, missile systems, IT systems, etc.).

3. Tier 1 Suppliers:

– Suppliers of components, assemblies, and specialized equipment;

– Dual-use enterprises.

4. Tier 2 and Lower-Tier Suppliers (Tier 2, Tier 3…):

– Manufacturers of basic materials, parts, and components;

– Suppliers of raw materials, rare-earth metals, and electronics.

5. Scientific, Design, and Engineering Institutions:

– State and private research institutes;

– Design bureaus;

– Innovative startups.

6. Logistics Operators and Transport Structures:

– Specialized carriers of defense cargo;

– Warehouses and dual-purpose logistics hubs;

– Multimodal transport companies with appropriate permits.

7. Financial and Insurance Institutions:

– Banks providing financing for defense contracts;

– Insurance companies covering risks associated with supply and production.

8. Information and Communication Systems:

– Digital supply chain management platforms;

– Data protection and cybersecurity systems.

Overall, the configuration of a DIC supply chain is multilevel, high-tech, and often exhibits a networked or hybrid structure, encompassing:

– Vertically integrated structures – leading enterprises that control substantial portions of the chain (e.g., from design to final assembly and testing);

– Cooperative clusters – networks of enterprises concentrated in strategic regions engaged in joint development and production;

– Global or regional supply chains – involving international suppliers of raw materials, technologies, or components (particularly for high-tech products);

– Closed critical segments – chain segments fully controlled by the state or strategic enterprises to safeguard against external threats;

– Dual-circuit supply chains – separating civilian and military circuits to enhance flexibility and enable rapid capacity mobilization in crises.

Thus, defense-industrial supply chains possess a set of unique characteristics that fundamentally distinguish them from analogous systems in the civilian sector. This specificity arises from the high strategic importance of defense products, the complexity of production processes, and the strict requirements for security, quality, and confidentiality.

First, DIC products are typically technologically sophisticated and unique, requiring the participation of highly specialized suppliers of components and materials. Such suppliers are often monopolistic or form a limited group of contractors, which increases dependency risks and contributes to supply chain fragility.

Second, state regulation plays a dominant role in DIC supply chains, encompassing stringent standards for quality and certification, as well as control over compliance with secrecy and security regimes. This restricts flexibility and the ability to rapidly substitute suppliers, while also complicating integration with international supply chains.

Third, the DIC operates in an environment of high external turbulence – geopolitical conflicts, sanctions, import and export restrictions, and the risks of warfare directly affect resource availability and supply stability. These conditions elevate the requirements for supply chain resilience and adaptability.

Fourth, ensuring continuity of production and adherence to strict timelines for the execution of state defense orders constitutes a critical task. Any disruption in supply can have far-reaching consequences for both enterprises and national security.

Moreover, DIC supply chains are characterized by a high degree of integration among enterprises of different levels – from component developers and manufacturers to final assemblers and military customers. This necessitates effective coordination, information exchange, and mutual trust among participants – factors often complicated by secrecy and regulatory constraints.

Therefore, the distinctive nature of defense-industrial supply chains lies in the combination of high technological complexity, strict regulatory oversight, significant vulnerability to external risks, and the imperative to ensure maximum levels of resilience and adaptability. The management of such supply chains requires specialized approaches that account for both the strategic importance of defense products and the particularities of the contemporary geopolitical environment.

Effective management of defense-industrial supply chains (DIC supply chains) under contemporary conditions is impossible without the integration of the concepts of resilience, adaptability, and antifragility, which collectively form the foundation of the viability of such supply chains as integrated socio-technical systems.

The viability of a DIC supply chain should be understood as the system's ability to ensure the continuity of its key functions, to respond rapidly to internal and external environmental changes, to effectively counteract disruptive influences, and to leverage crises as opportunities for transformation and structural reinforcement. Table 1 presents the authors' conceptual interpretation of the key characteristics defining resilience, adaptability, fragility, and viability of defense-industrial supply chains.

Table 1. Comparative Analysis of the Key Characteristics of Resilience, Adaptability, Fragility, and Viability in Defense-Industrial Supply Chains

The Concept	The Essence of the Concept	Form of Response to Disruptions	Management Focus	Significance for the Defense Industry
Resilience	Ability to withstand disruptions and recover rapidly	Return to the previous or an acceptable state	Continuity planning, reserves, and recovery strategies	Critical need to maintain uninterrupted functioning during crises
Adaptiveness	Ability to modify structure and processes in accordance with new conditions	Flexible reorganization, process modification, and engagement of new partners	Structural flexibility, link adaptation, and configuration changes	Ability to respond to new challenges (sanctions, changes in suppliers and markets)
Antifragility	Ability to become stronger after disruptions and crises	Utilization of crises as catalysts for growth and development	Promotion of learning, innovation, and structural transformation	Strengthening of competitive advantages and resilience to future shocks
Viability	System's ability to maintain functionality and development in the long term	Balance between efficiency, resilience, adaptability, and innovativeness	Systemic strategic management and integration of approaches	Ensuring long-term national and economic security

Source: Generalized by the authors based on [15-17, 22, 24]

Management of the viability of defense-industrial supply chains is based on a set of interrelated principles that reflect the integration of approaches to resilience, adaptability, and antifragility. Foremost among these is the principle of security and criticality priority, which entails the identification of bottlenecks, critical suppliers, and essential resources, as well as ensuring their protection against physical, economic, and cyber threats. Equally important is the principle of structural and informational transparency, which requires the establishment of a network of interactions among supply chain participants based on reliable communication systems that enable real-time monitoring of the condition of key elements of the chain and potential risks.

Given the need to ensure adaptability, a critical aspect is the principle of flexibility and modularity, which implies the creation of capabilities for rapid reconfiguration of production, diversification of supply sources, and logistics routes. This principle is complemented by the principle of decentralization and redundancy, aimed at minimizing dependence on a single supplier or node, maintaining alternative supply options, and distributing critical capacities geographically.

The concept of antifragility necessitates the implementation of the principle of learning and evolutionary development, which refers to the ability of the supply chain not only to recover from crises but also to accumulate experience, strengthen its internal structure, and enhance management efficiency under the influence of stress factors.

In this context, the principle of integrated risk management acquires strategic importance, implying a systemic approach to the identification, analysis, and neutralization of both anticipated and unforeseen threats across all levels of supply chain functioning (Fig. 3).

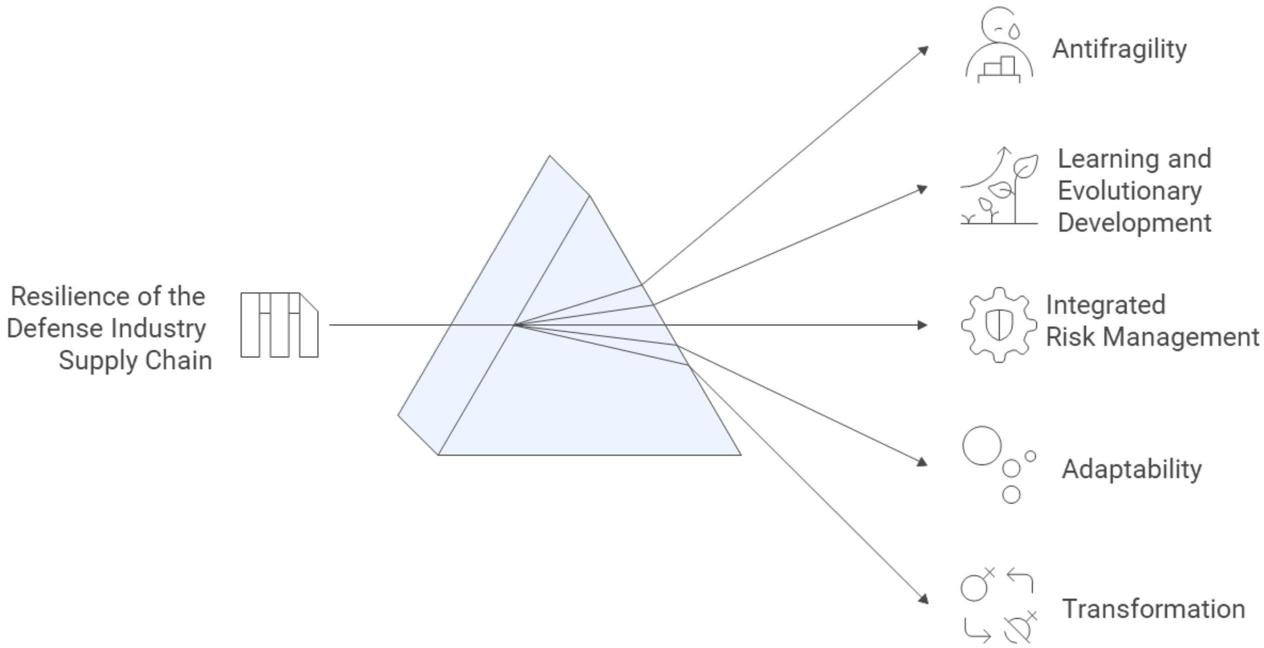

Figure 3 – Structure of the Elements of Resilience in the Defense-Industrial Supply Chain
Source: Developed by the authors

Thus, the viability of a defense-industrial supply chain as an integrated system results from the comprehensive implementation of principles that ensure its resilience to disruptive influences, its adaptability to environmental changes, and its capacity for effective transformation under crisis conditions. Ensuring such viability is a prerequisite for the sustainable functioning of the defense-industrial complex (DIC), as well as for enhancing national security and the strategic autonomy of the state.

Management of DIC supply chains is characterized by a set of specific challenges and threats that significantly affect their resilience and fragility. Among the key threats is geopolitical instability, manifested in armed conflicts, sanctions, and political isolation. These factors restrict access to critical resources, thereby reducing overall supply chain resilience and increasing the risk of supply disruptions and functional breakdowns. A particularly serious issue is the high dependence on the import of critical materials and technologies, especially from unstable or unfriendly regions, which introduces additional vulnerabilities and amplifies systemic fragility in the event of interruptions in international deliveries.

Another major threat lies in cyberattacks and other information-related risks, which can compromise the operation of digital supply chain management platforms, leading to reduced process transparency, loss of coordination control, and, consequently, a decline in overall system resilience. Disruptions in global transport and logistics networks caused by crises or emergencies create physical barriers to material flows, further increasing fragility and diminishing the supply chain's ability to respond rapidly to changes.

In addition to external challenges, the development and functioning of DIC supply chains are influenced by a number of internal barriers. A large bureaucratic apparatus and the complexity of state procurement procedures hinder decision-making agility and innovation implementation, thereby reducing the system's flexibility and adaptability. A shortage of qualified personnel in production, logistics, and innovation limits modernization potential and managerial efficiency, further exacerbating system fragility. Technological obsolescence of equipment and limited access to financing impose additional obstacles to ensuring production continuity and supply chain resilience.

At the same time, there are important drivers of development that contribute to strengthening resilience and reducing fragility in DIC supply chains. Notably, production localization and supplier diversification help decrease dependence on external sources, thereby improving the system's flexibility and reliability. The development of innovative technologies, digitalization of management processes, and enhanced cybersecurity improve transparency, coordination efficiency, and responsiveness to threats.

An equally vital component is integration into international cooperative programs and standardization, which expand technological capabilities and enhance overall resilience through access to shared resources and partner networks. State support—in the form of import substitution policies, incentives for scientific research, and investment in production capacity development—creates the necessary conditions for establishing a viable and adaptive supply system.

Table 2. Challenges, Threats, Barriers, and Development Drivers of Defense-Industrial Supply Chains from the Perspective of Resilience and Fragility

Characteristics	Content	Possible Implications for the Resilience and Fragility of Defense Industry Supply Chains
Challenges and Threats		
Geopolitical Instability	Armed Conflicts, Sanctions, Trade Restrictions, and Political Isolation	Reduced resilience due to limited access to resources; increased fragility caused by supply disruptions and chain breaks
High Technological Complexity and Limited Number of Suppliers	The Production of Defense Industry Products Often Depends on Unique Technological Components Supplied by a Limited Number of or Even Monopolistic Companies.	This creates vulnerability through risk concentration and makes supply chains fragile to technical failures, material shortages, or price fluctuations.

Dependence on Imports	Critical Materials, Technologies, and Components Originating from Unfriendly or Unstable Regions	Increased fragility due to the risk of supply blockades; reduced resilience of the production process
Need for Strict Quality and Safety Control	The requirements for quality, reliability, and safety of products in the defense sector are extremely strict, which limits the possibilities of replacing suppliers and implementing new technologies without lengthy certification and verification procedures.	This creates additional barriers to the rapid adaptation of supply chains.
Increasing Turbulence of the Market Environment	Demand fluctuations, changes in state defense orders, financial constraints, and other factors	Reduced ability of supply chains to adapt quickly
Cyberattacks and Information Threats	Interference with digital platforms, data leaks, and management paralysis	Decreased informational and managerial resilience; increased fragility of management and coordination systems
Environmental and Social Requirements	Modern requirements for sustainability, environmental safety, and social responsibility, which often conflict with other priorities such as speed or cost	Increased fragility of supply chains and the need to adapt to environmental and social requirements
Disruptions in Global Logistics	Interruptions in international routes and shortage of transportation capacities	Increased fragility of physical flows; reduced resilience in the supply of components and resources
Development Barriers		
Bureaucratic Constraints	Complexity and Duration of Public Procurement, Certification, and Licensing Procedures	Reduced flexibility and adaptability; increased fragility due to delays in implementing new solutions
Shortage of Qualified Personnel	Insufficient Number of Specialists in the Fields of Production, Innovation, and Defense Industry Logistics	Decreased operational resilience; increased fragility resulting from human factors and decision-making errors
Technological Obsolescence	High Level of Equipment Wear and Limited Technological Capabilities	Increased production fragility; reduced resilience to technical failures and accidents
Limited Access to Financing	Insufficient Investment in the Modernization and Development of Defense Industry Supply Chains	Reduced resilience of innovative development; increased fragility due to the lack of resources for diversification and protection
Development Drivers		
Localization and Diversification	Development of Domestic Production, Engagement of New Suppliers and Regional Clusters	Increased resilience through reduced external dependence; decreased fragility due to alternative sources of supply
Development of Innovation and Digitalization	Implementation of Advanced Technologies, Digital Management Platforms, and Cybersecurity Measures	Strengthening of management and coordination resilience; reduced fragility through transparency and control
International Cooperation and Standardization	Integration into International Programs, Harmonization of Requirements, and Joint Defense Projects	Enhanced resilience through expanded partnerships; reduced fragility through shared access to technologies and resources
State Support and Incentives	Import Substitution Policies, Tax Incentives, and Support for Research and Development	Strengthening the resilience of domestic production potential; reducing fragility through strategic planning

Source: Generalized by the authors based on [8, 14-16, 21]

Therefore, the successful management of defense-industrial supply chains (DIC supply chains) requires a systemic approach that accounts for the impact of both external challenges and threats, as well as internal barriers, while simultaneously leveraging development drivers to enhance resilience and reduce fragility within the system. Only through such an integrated approach can the viability of the supply chain be ensured – an essential foundation for the defense capability and strategic autonomy of the state.

Figure 4 summarizes the authors' proposed set of key management measures aimed at strengthening the resilience, adaptability, and antifragility of defense-industrial supply chains.

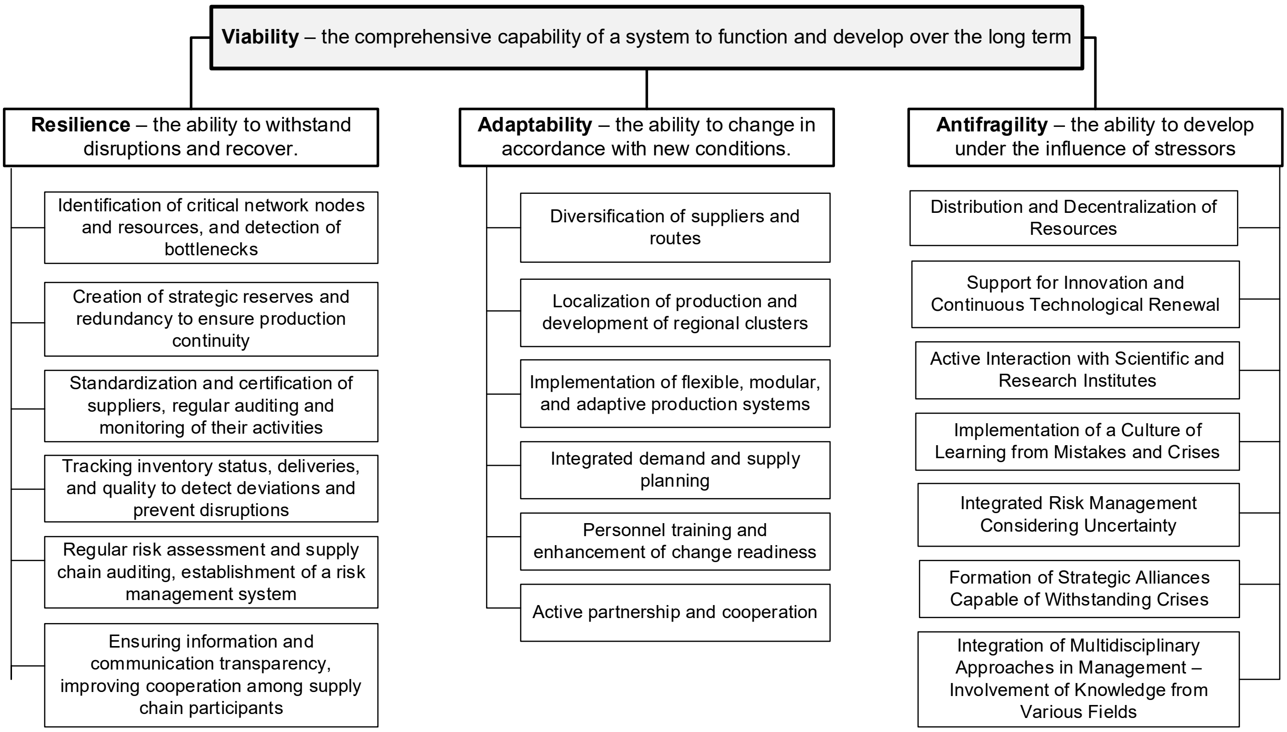

Figure 4 – System of Managerial Measures for Enhancing the Resilience, Adaptability, and Antifragility of Defense-Industrial Supply Chains

Source: Developed by the authors

Thus, ensuring the resilience of defense-industrial supply chains requires the implementation of a comprehensive set of measures that allow them to maintain continuous operation even under adverse conditions. Foremost among these is the identification of critical nodes and resources within the supply chain, enabling a focused allocation of efforts toward the most vulnerable points of the system. The formation of strategic reserves of materials and components ensures the continuity of production in the event of supply disruptions. A well-organized inventory management system helps anticipate demand fluctuations and guarantees the availability of critical materials. This approach enables effective resource management, optimizes production capacities, and maximizes output during peak demand periods. Regular monitoring and quality control of supplies, together with the standardization of supplier requirements, help prevent the use of substandard products that may cause operational failures. The development of business continuity plans and personnel training allows for rapid and coordinated responses to emergencies.

Equally important is the cybersecurity of information systems supporting supply chain management, as threats in the digital domain can paralyze coordination and control. The optimization of logistics processes, regular risk audits, and ensuring information transparency among participants further enhance system resilience, creating a robust foundation for stable performance. To strengthen the adaptability of supply chains, measures must be implemented to ensure flexibility and rapid system reconfiguration in response to changing conditions. Defense industry contractors face considerable challenges in ensuring timely deliveries and maintaining high product quality. Diversification of suppliers and logistics routes minimizes the risks associated with disruptions along a single direction or from an individual supplier. Localization of production and the formation of regional clusters reduce dependency on external factors and shorten delivery times.

Flexible production systems, capable of rapidly modifying product assortments or output volumes, enable prompt responses to market needs and operational challenges. The digitalization of management processes – through the use of data analytics and predictive systems – supports effective, real-time decision-making. Conducting scenario-based exercises and decentralizing management authority increase responsiveness to localized problems. Early warning systems and active promotion of innovation facilitate timely adaptation of supply chains to emerging challenges.

Finally, partnership and cooperation among supply chain participants establish a network of mutual support that strengthens adaptive capacity. Cultivating collaboration and building trust within defense-industrial supply chains ensure the stable supply of high-quality products, thereby reinforcing the broader foundation of the national defense industry.

Considering that antifragility is the ability of a supply chain not only to withstand stressors but to become stronger as a result of them, the development of antifragility requires the implementation of a culture of learning from errors and crises, with a systematic analysis of all failures aimed at continuous improvement. Flexible transformation strategies enable rapid reconfiguration of the supply chain in response to unforeseen events. The continuous introduction of innovations and technological upgrades enhances both competitiveness and system endurance. Integrated risk management, which accounts for uncertainty and radical change, allows preparation for a wide range of potential scenarios. The development of partnership networks, collaboration with scientific institutions, and the establishment of feedback systems ensure a constant exchange of knowledge and resources, thereby strengthening antifragility. Furthermore, the development of human capital focused on innovation and adaptability builds teams capable of operating effectively under uncertainty. Scenario-based training and a multidisciplinary approach to management foster the formation of a holistic, viable, and self-developing supply chain system.

Thus, a comprehensive approach to supply chain management that integrates measures for enhancing resilience, adaptability, and antifragility is crucial for ensuring their viability, especially under conditions of instability and continuous change. Implementing these managerial measures requires a transformation of the technological decision-making base, as traditional approaches are limited in speed, transparency, and coordination of managerial efforts. The absence of integrated systems and unified standards leads to isolated operation of individual departments and contractors, complicating synchronization of actions, generating conflicts, and diminishing overall supply chain efficiency.

First and foremost, it should be emphasized that to increase the resilience, adaptability, and antifragility of defense-industrial supply chains, flexible management structures are essential. Traditional hierarchical models – characterized by excessive bureaucracy and multiple levels of control – impede rapid decision-making and hinder coordination among supply chain participants. Consequently, modern agile organizational structures are shifting away from vertically isolated models toward horizontal systems that minimize bureaucracy and delegate authority directly to those closest to operational processes.

A horizontal organizational structure with broad spans of control and fewer hierarchical layers dismantles traditional organizational barriers, stimulates cross-functional collaboration, and accelerates decision-making and responsiveness to change. This is particularly critical for defense-industrial supply chains, where timing and precision are of paramount importance. A key element of such a structure is the team-based management model – a network of small, autonomous, cross-functional teams with clearly defined client-oriented accountability. These teams bring together specialists from diverse fields, empowered to make decisions that balance individual initiative with collective coordination. Such an approach fosters innovation and rapid response to emerging challenges and opportunities – an especially relevant factor within the defense industry context.

Moreover, the mission-oriented focus of these teams enables them to concentrate on meeting the needs of both internal and external clients, fostering shared responsibility for results and reinforcing a collective sense of purpose. This alignment leads to high task efficiency and coordinated action across all supply chain participants. Equally important is the leadership role, which supports transformation and the cultivation of agile thinking, sets the tone for implementing innovative practices, and creates an environment that promotes adaptability and proactivity (Fig. 5).

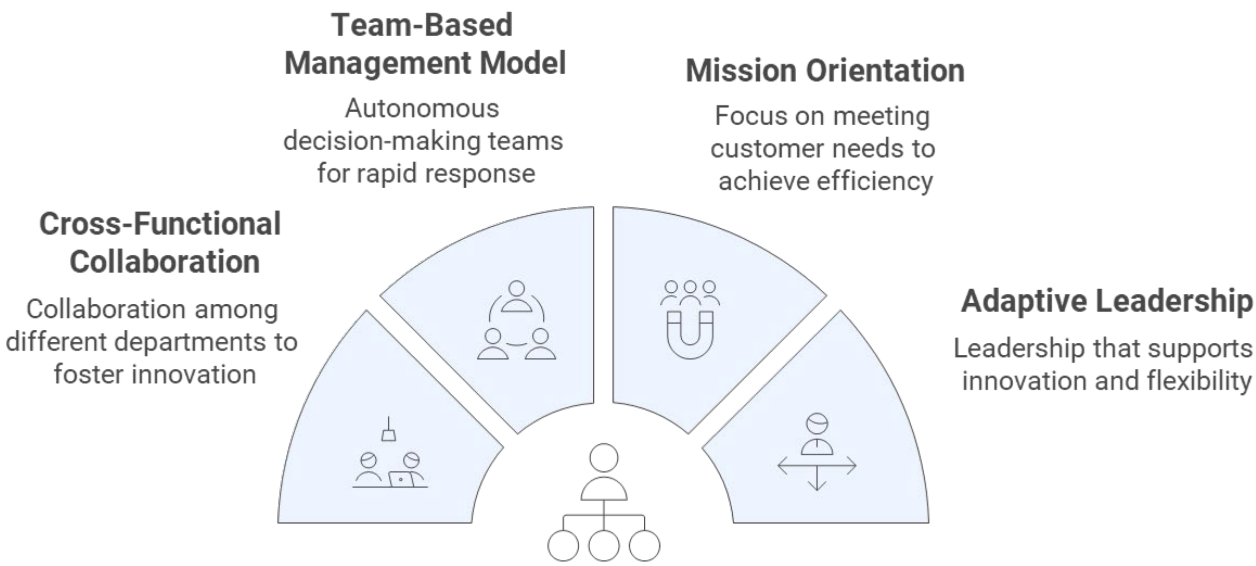

Figure 5 – Structural Support for Innovation
Source: Developed by the authors

Flexible structures with decentralization and a team-based approach require robust technological support to ensure effective coordination, information exchange, and real-time decision-making. Modern digital technologies provide this support by enabling the integration of heterogeneous data, process automation, large-scale information analysis, and risk forecasting. They create a unified information environment that fosters transparency and interaction among supply chain participants, regardless of their geographical distribution or functional specialization.

Without modern digital solutions, agile organizational models cannot achieve their full efficiency, as it is technology that transforms individual actions into coordinated, rapid, and adaptive processes.

Table 3 illustrates how key digital tools – the Internet of Things (IoT), Big Data, Artificial Intelligence (AI), Blockchain, Cloud Computing, and Digital Management Platforms – contribute to enhancing the resilience, adaptability, and antifragility of defense-industrial supply chains.

Table 3. The Role of Digital Technologies in Enhancing the Resilience, Adaptability, and Antifragility of Defense-Industrial Supply Chains

Digital Technology	Enhancing Resilience	Enhancing Adaptability	Enhancing Antifragility
Internet of Things (IoT)	• Continuous monitoring of equipment and vehicle condition for timely maintenance (predictive maintenance). • Control of temperature, humidity, and storage conditions for critical materials. • Rapid detection and localization of problems to minimize downtime.	• Dynamic adjustment of delivery routes based on real-time traffic and environmental data. • Flexible inventory management in real time. • Support for operational interaction among supply chain participants.	• Sensor data analysis to predict and prevent failures. • Development of recovery scenarios after incidents. • System learning from collected data to enhance resilience.
Big Data	• Identification of supply and consumption patterns to prevent shortages. • Risk analysis related to external factors (political instability, climate change). • Monitoring compliance with regulatory requirements.	• Accurate demand forecasting and detection of market trend shifts. • Identification of potential bottlenecks in the supply chain. • Support for adaptive production and procurement planning.	• Analysis of crisis events to develop best practices. • Modeling of scenario developments to improve preparedness. • Detection of vulnerabilities and weak links for further strengthening.
Artificial Intelligence (AI)	• Automatic detection of anomalies in processes and prediction of potential disruptions. • Optimization of routes and inventories to reduce risks. • Decision support in complex operational conditions.	• Automation of planning processes considering internal and external changes. • Development of adaptive management strategies based on data analytics. • Identification of new opportunities for supply chain optimization.	• Continuous learning of the system based on environmental changes. • Development and implementation of resilience and transformation strategies. • Decision-making support in crisis situations through simulations.
Blockchain	• Guarantee of data transparency and immutability for material origin and transactions. • Reduction of fraud and error risks. • Strengthening of trust among supply chain participants.	• Facilitation of fast and secure transactions between parties. • Greater flexibility in contract and agreement adjustments. • Automation of procedures via smart contracts.	• Decentralized data storage increases resistance to external attacks. • Ensures business continuity even in case of localized disruptions. • Enhances data reliability and security under crisis conditions.
Cloud Computing	• Scalable resources for storage and processing of critical data. • Ensuring uninterrupted access to information. • Fast data recovery after system failures.	• Flexible access to information resources from any location. • Support for team mobility and fast data exchange. • Easy integration of new services and applications.	• Data backup and disaster recovery mechanisms. • Automatic resource scaling in response to changing loads. • Strengthening the overall viability of the infrastructure.
Digital Management Platforms	• Centralized risk and monitoring management in real time. • Improved process transparency and control. • Integration of different systems for unified supply chain visibility.	• Coordination of actions among different participants via a unified platform. • Support for rapid information exchange and joint decision-making.	• Continuous process improvement based on analytics and feedback. • Support for innovative approaches and development strategies.

		• Flexible planning and adaptation to external changes.	• Ensuring sustainability of transformation processes.

Source: Generalized by the authors based on [4, 5, 10, 21-24]

Summarizing the data presented in the table, it should be noted that Internet of Things (IoT) technologies enable continuous data collection from equipment, transport, and warehouses, allowing for the prompt detection of potential malfunctions and rapid response, thereby enhancing system resilience. At the same time, IoT facilitates flexible management of routes and inventories, which strengthens adaptability, while also accumulating data for forecasting and process improvement – an essential component of antifragility.

Big Data technologies make it possible to analyze large volumes of information to identify risks, forecast demand, and detect weak links within the supply chain. This enhances resilience through early warning of threats, strengthens adaptability by enabling rapid plan adjustments, and contributes to antifragility through systematic learning from crisis situations.

Artificial Intelligence (AI) automates anomaly detection, optimizes resource allocation, and supports decision-making under complex conditions. As a result, AI contributes to risk reduction and improved efficiency (resilience), rapid reconfiguration of processes (adaptability), and in-depth analysis for post-stress system development (antifragility).

Blockchain technology ensures the transparency and security of transactions, protects against fraud, and increases trust among supply chain participants – key factors for resilience. It also supports rapid and secure coordination of actions (adaptability) and creates a decentralized system resistant to external attacks (antifragility).

Cloud computing guarantees scalability and resource availability, maintaining operational continuity and facilitating rapid recovery after disruptions, thereby enhancing resilience. Flexible access and service integration strengthen adaptability, while backup mechanisms and automatic scaling sustain the system's viability and antifragility under crisis conditions.

Digital management platforms integrate heterogeneous data and processes, enabling real-time risk monitoring and effective decision-making (resilience), coordination of actions and rapid adaptation to change (adaptability), and continuous process improvement through innovation support (antifragility).

Thus, the comprehensive implementation of these digital technologies provides the foundation for building viable defense-industrial supply chains capable of functioning effectively and evolving under conditions of persistent challenges and continuous transformation.

Conclusions. Based on the results of the conducted research, the essence of defense-industrial supply chains (DIC supply chains) has been clarified as complex integrated systems operating under conditions of high uncertainty, multiple threats, and severe constraints characteristic of both the global environment and the internal realities of Ukraine during wartime. The study substantiates the relevance of applying the concept of supply chain viability to the DIC, which synthesizes approaches to ensuring their resilience, adaptability, and antifragility.

The research systematized the main challenges, threats, barriers, and drivers influencing the development of such supply chains from the standpoint of their impact on system resilience and fragility. It was established that the key factors shaping viable defense-industrial supply chains include the diversification of suppliers and logistics routes, the development of horizontal interaction among business ecosystem participants, and the extensive use of modern digital technologies.

The necessity of abandoning traditional hierarchical and centralized models of managing DIC supply chains was separately justified in favor of flexible, decentralized organizational structures that combine autonomy, partnership, and an integrated digital environment.

To enhance the resilience, adaptability, and antifragility of Ukraine's defense-industrial supply chains under conditions of global turbulence and armed conflict, a comprehensive approach must be applied, integrating organizational, technological, and managerial measures.

In particular, it is advisable to diversify suppliers and transportation routes, thereby reducing dependence on individual countries and critical logistical nodes. It is equally important to develop horizontal partnerships among defense enterprises, the private sector, research institutions, and international companies to establish a robust and sustainable business ecosystem.

The implementation of modern digital technologies – including the Internet of Things (IoT), Artificial Intelligence (AI), Blockchain, and cloud-based platforms – will enhance transparency, flexibility, and decision-making speed.

A critically important task is the development of local production of strategically significant components, the strengthening of information security, the implementation of risk monitoring systems, and the regular training of personnel in crisis management principles. The combined effect of these measures will enable Ukraine's defense-industrial supply chains not only to effectively withstand external challenges but also to evolve and improve even under difficult and unstable conditions.

Further research should focus on the quantitative modeling of resilience, adaptability, and antifragility parameters of DIC supply chains, using practical assessment tools tailored to the realities of Ukraine. A promising direction lies in the development of diagnostic methodologies for evaluating the interaction between DIC enterprises and the private sector within business ecosystems, as well as the study of the effectiveness of specific digital technologies (such as Artificial Intelligence, Blockchain, and digital management platforms) in strengthening supply chain viability.

Special attention should also be devoted to the formation of regulatory and organizational frameworks that would enable the implementation of flexible management models for defense supply chains during both wartime and post-war reconstruction periods.

References

1. Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. The International Journal of Logistics Management, 20(1), 124-143.
2. Pettit, T. J., Fiksel, J., & Croxton, K. L. (2010). Ensuring supply chain resilience: Development and implementation of an assessment tool. Journal of Business Logistics, 31(1), 1-21.
3. Pires Ribeiro, J., & Barbosa-Povoa, A. (2018). Supply chain resilience: Definitions and quantitative modelling approaches – A literature review. Computers & Industrial Engineering, 115, 109–122. DOI: https://doi.org/10.1016/j.cie.2017.11.006
4. Antonio Padovano & Dmitry Ivanov (2025): Towards resilient and viable supply chains: a multidimensional model and empirical analysis, International Journal of Production Research, DOI: 10.1080/00207543.2025.2470350
5. Dmitry Ivanov (2024) Two views of supply chain resilience, International Journal of Production Research, 62:11, 4031-4045, DOI: 10.1080/00207543.2023.2253328
6. Supply Chain Resilience: Adapting To Global Disruptions and Uncertainty Dr. Arjita Mishra, Nidhi Gupta, Gautam Kumar Jha. International Journal of Innovative Research in

Engineering Volume 5, Issue 2 (March-April 2024), PP: 189-196. URL: https://www.doi.org/10.59256/ijire.20240502025 ISSN No: 2582-8746

7. Mackay, J., Munoz, A., & Pepper, M. (2020). Conceptualising redundancy and flexibility towards supply chain robustness and resilience. Journal of Risk Research, 23(12), 1541–1561. https://doi.org/10.1080/13669877.2019.1694964

8. Maharjan, R., & Kato, H. (2022). Resilient supply chain network design: A systematic literature review. Transport Reviews, 42(6), 739–761. DOI: https://doi.org/10.1080/01441647.2022.2080773

9. Wieland, A., & Durach, C. F. (2021). Two perspectives on supply chain resilience. Journal of Business Logistics, 42(3), 315–322. DOI: https://doi.org/10.1111/jbl.12271

10. Zavala-Alcívar, A., Verdecho, M. J., & Alfaro-Saiz, J. J. (2023). Supply chain resilience: a conceptual evolution analysis. Dirección y Organización, 5-17.

11. Nikookar, E., Stevenson, M., & Varsei, M. (2023). Building an antifragile supply chain: A capability blueprint for resilience and post-disruption growth. Journal of Supply Chain Management, 1–19. https://doi.org/10.1111/ jscm.12313

12. Zavala-Alcívar, A., Verdecho, M. J., & Alfaro-Saiz, J. J. (2023). Supply chain resilience: a conceptual evolution analysis. Dirección y Organización, 5-17.

13. Lotfi, R., Mehrjardi, M. S., MohajerAnsari, P., Zolfaqari, F., & Afshar, M. (2023). Antifragile, sustainable, and agile supply chain network design by considering resiliency, robustness, risk, and environmental requirements. Environmental Science and Pollution Research, 30(48), 106442-106459.

14. Ivanov D. (2024). Transformation of supply chain resilience research through the COVID-19 pandemic. International Journal of Production Research, 62(23), 8217-8238. Ivanov, D. (2025). When is the supply chain resilient? Customer and operational perspectives. International Journal of Production Research, 1–16. DOI: https://doi.org/10.1080/00207543.2025.2454331

15. Ivanov, D. (2025). No risk, no fun? A bioinspired adaptation-based framework for supply chain resilience in Industry 5.0. International Journal of Production Research, 1-21.

16. Ramezani, J., & Camarinha-Matos, L. M. (2020). Approaches for resilience and antifragility in collaborative business ecosystems. Technological forecasting and social change, 151, 119846.

17. Zsidisin, G. A., Bresler, A., Hazen, B., Snider, K. F., & Wilkerson, T. H. (2020). Research in defence logistics: Where are we and where are we going? Journal of Defense Analytics and Logistics, 4(1), 3–17. https://doi.org/10.1108/JDAL-07-2019-0012

18. Ekström, T. (2025). Supply Chain Resilience – An Empirical Exploration of Barriers and Enablers in Military Settings. Scandinavian Journal of Military Studies, 8(1), pp. 119–136. DOI: https://doi.org/10.31374/sjms.350

19. Melnyk, S., Narasimhan, R., & DeCampos, H. (2014). Supply chain design: Issues, challenges, frameworks and solutions. International Journal of Production Research, 52(7), 1887–1896. https://doi.org/10.1080/00207543.2013.787175

20. Rebecca Lucas, Thomas Ekström, Paola Fusaro, Elizabeth Hastings Roer, Lucia Retter. Toward Defense Supply Chain Disruption Management. A Research Agenda for Defense Supply Chain Resilience. https://www.rand.org/pubs/research_reports/RRA2504-1.html

21. Roland Hellberg, David Sprängare, Olov Candell, Claes Carpenfelt, Kristian Lundberg, Per Samuelsson, Imoh Antai, Per Andersson & Lars Backlund (07 May 2025): Performance constraints in defence industry supply chains: evidence from case studies, Defence and Peace Economics, DOI: 10.1080/10242694.2025.2500362

22. Elvemo, L. (2025). Supply Chain Resilience in Military Operations: A Case Study Exploring Command and Control. Scandinavian Journal of Military Studies, 8(1), pp. 178–199. DOI: https://doi. org/10.31374/sjms.356

23. Korkmaz, G. (2024). Supply chain risks and management strategies in the defense industry. Journal of Defense Resources Management (JoDRM), 15(1), 35-60.

24. Sani, S., Schaefer, D., & Milisavljevic-Syed, J. (2022). Strategies for Achieving Pre-emptive Resilience in Military Supply Chains. Procedia CIRP, 107, 1526–1532. DOI: https://doi.org/10.1016/j.procir.2022.05.186

25. Sania S., Schaeferb D., Milisavljevic-Syeda J. Strategies for Achieving Pre-emptive Resilience in Military Supply Chains. Procedia CIRP 107 (2022) 1526–1532

26. Gürtlich, G., Lampl, S. (2022). Resilience and Military Supply Chain Management. In: Kummer, S., Wakolbinger, T., Novoszel, L., Geske, A.M. (eds) Supply Chain Resilience. Springer Series in Supply Chain Management, vol 17. Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-95401-7_29

27. Cabrera, B., Santa, R., Tegethoff, T., Morante, D., & Ferrer, M. (2023). Supply chain resilience in the Colombian defense sector before and during the COVID-19 pandemic: A comparative study. PLOS ONE, 18(3), e0282793. https://doi.org/10.1371/journal.pone.0282793

28. Antai, I., & Hellberg, R. (2025). Surge complexities in defense industry supply chains: evidence from multiple case studies. The International Journal of Logistics Management, 36(7), 242-261.

29. Loska, D., Genchev, S., Rich, N., & Malik, T. (2024). Defense supply chain collaboration: an exploratory study and empirical framework. Journal of Defense Analytics and Logistics, 8(1), 2-37.

30. Hubarieva, I. O., Harmash, O. M., Trushkina, N. V., Shkrygun, Yu. O., Patlachuk, T. V. (2024). Digital transformation of enterprise' logistics activities: bibliometric and trend analysis. Intellectualization of logistics and Supply Chain Management [Online], 28, 47-70. https://doi.org/10.46783/smart-scm/2024-28-5.

31. Harmash, O., Hubarieva, I., Harmash, T., Trushkina, N. (2024). Relationship between the concepts of "digital transformation" and "industry 5.0": bibliometric analysis. Intellectualization of logistics and Supply Chain Management [Online], 24, 89-106. https://doi.org/10.46783/smart-scm/2024-24-10.

32. Global Risks Report (2024). World Economic Forum. URL: https://www.weforum.org/publications/global-risks-report-2024/

33. Hryhorak M.Y., Harmash O.M., Popkowski T. Artificial intelligence in supply chain management: opportunities and threats for professional competence. Intellectualization of logistics and Supply Chain Management. [Online], vol.19, pp.24-44, DOI: https://doi.org/10.46783/smart-scm/2023-19-3.