Electronic scientific and practical journal

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

#38(2026)
August '26

WWW.SMART-SCM.ORG
ISSN 2708-3195
DOI.ORG/10.46783/SMART-SCM/2026-38

ISSN 2708-3195
9772708319005

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 June 11, 2026 No. 928 (Appendix 13 item 205).**

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)
D3 – Management
D5 – Marketing

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2026-38

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

Released 6 times a year

№ 38 (2026)
August 2026

Kyiv - 2026

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 June 11, 2026 No. 928 (Appendix 13 item 205).***

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations); D3 – Management; D5 – Marketing

DOI: https://doi.org/10.46783/smart-scm/2026-38
e-mail: support@smart-scm.org
facebook.com/Smart.SCM.org
тел.: (063) 593-30-41
https://smart-scm.org

Contents

INTRODUCTION

We are happy to invite you to get acquainted with the first issue of the new scientific and practical publication "Intellectualization of Logistics and Supply Chain Management".

We strongly believe that the launch of this magazine indicates the objective need to rethink a wide range of issues related to the development of theory and practice in logistics and supply chain management, awareness of the need to unite the scientific community and logistics practitioners, dissemination of modern knowledge and best practices for innovative development of the logistics services market.

The first issue of the magazine is published at a difficult time. The global coronavirus pandemic and the deep economic crisis have significantly worsened business activity in the world. Currently, global supply chains are collapsing, international trade is declining, and competition between global and regional logistics operators is intensifying. The most common thesis is that the world will never be the same again. Industry experts predict the emergence of new, more flexible and adaptive supply chain management strategies and approaches to logistics business process management. The trend towards collaborations, cooperation and unification of services is emerging, comprehensive proposals for clients are being developed. There is increasing talk about the need to build bimodal supply chains, which involves the development of different decision-making scenarios: the traditional approach - cost-effective efficiency, low risk, high predictability; a new approach "second mode" - rapid recognition of opportunities, adaptability, willingness to solve unexpected problems and look for new opportunities.

Radical transformations of the global and national markets for logistics services require appropriate scientific support. Logistics science has a special role to play in this process. Initiating the emergence of a new journal, we decided to focus on its coverage of problematic aspects of the formation and development of logistics systems at the micro, mezo and macro levels, supply chain management, digitization of logistics, methods and tools for optimizing processes in logistics and supply chains, sociopsychology relations and network interaction of enterprises using cloud technologies, artificial intelligence, e-learning, neural business process management systems, etc.

Therefore, we invite scientists, researchers and business representatives, as well as our colleagues from abroad, to cooperate and present the results of scientific research, to discus and debate on them, to work together to develop the scientific theory of logistics and promote mutual intellectual enrichment.

We hope that the new scientific publication will become a theoretical guide for young researchers and representatives of other fields.

HRYHORAK Mariia
Chief Editor

DOI: https://doi.org/10.46783/smart-scm/2026-38-1

UDC 658.7:005.51:004.8
JEL Classification: M11, L91, O33, A14.

Received: 2026-06-21
Accepted: 2026-07-29
Published: 2026-08-30

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@edu.kpi.ua

Karpun O.V. PhD (Economics), Associate Professor, Associate Professor of Department of International Business and Logistics, National Technical University of Ukraine «Igor Sikorsky Kyiv Polytechnic Institute» (Ukraine)

ORCID – 0000-0003-2058-9070
Researcher ID – S-6428-2018
Scopus author id: – 60001156100
E-Mail: karpun.olha@edu.kpi.ua

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT: CONCEPTUAL FRAMEWORK, RESEARCH AGENDA, AND THE ROLE OF A SCIENTIFIC JOURNAL

Mariia Hryhorak, Olga Karpun. «Intellectualization of logistics and supply chain management: conceptual framework, research agenda, and the role of a scientific journal». *The rapid growth of research in digital logistics, artificial intelligence, autonomous systems, resilience, and circular supply chains exacerbates the fragmentation of logistics knowledge and complicates the explanation of modern logistics systems as holistic socio-technical ecosystems. The purpose of this article is to substantiate the intellectualization of logistics and supply chain management as an integrative conceptual framework and an open research agenda. The methodological foundation includes a targeted conceptual literature review, comparative analysis of related concepts, theoretical synthesis, and logical modeling. The article systematizes contemporary directions in logistics research, identifies their integrative gap, and differentiates intellectualization as a process, an intelligent logistics system as an analytical system type, a conceptual framework as an analytical tool, and a research agenda as a domain for further inquiry. The unit of analysis and the boundaries of the proposed framework are specifically clarified. A mechanistic-process model of intellectualization is proposed, in which human intelligence, organizational memory and learning capacity, inter-organizational collective intelligence, and artificial intelligence – through knowledge sharing, coordination, organizational learning, and human oversight of algorithmic decisions – are transformed into adaptive capabilities of the logistics system. Boundary conditions and risks of intellectualization are identified, including algorithmic opacity, poor data quality, platform dependency, cyber risks, and the loss of human expertise. Four theoretical propositions regarding*

causal relationships within the logistics system are formulated, along with a separate methodological proposition on changing the unit of analysis and an institutional proposition on the journal's role. The scientific contribution lies in distinguishing intellectualization from digitalization and AI, constructing a testable system of propositions, and shaping the Research Agenda. A limitation of the study is its theoretical and conceptual nature, which requires further operationalization and empirical testing.

***Keywords**:* Intellectualization, Logistics, Supply Chain Management, Research Agenda, Conceptual Research, Conceptual Framework, Integrative Research Program, Digital Transformation, Open Science

Марія Григорак, Ольга Карпунь. «Інтелектуалізація логістики та управління ланцюгами постачання: концептуальна рамка, дослідницький порядок денний і роль наукового журналу». *Стрімке зростання досліджень цифрової логістики, штучного інтелекту, автономних систем, резильєнтності та циркулярних ланцюгів постачання посилює фрагментацію логістичного знання й ускладнює пояснення сучасних логістичних систем як цілісних соціотехнічних екосистем. Метою статті є обґрунтування інтелектуалізації логістики та управління ланцюгами постачання як інтегративної концептуальної рамки й відкритої дослідницької програми. Методологічною основою є цільовий концептуальний огляд літератури, порівняльний аналіз суміжних понять, теоретичний синтез і логічне моделювання. У статті систематизовано сучасні напрями логістичних досліджень, визначено їхню інтегративну прогалину, розмежовано інтелектуалізацію як процес, інтелектуальну логістичну систему як аналітичний тип системи, концептуальну рамку як інструмент аналізу та дослідницьку програму як простір подальших питань. Окремо уточнено одиницю аналізу й межі застосування запропонованої рамки. Запропоновано механістично-процесну модель інтелектуалізації, у якій людський інтелект, організаційна пам'ять і здатність до навчання, міжорганізаційний колективний інтелект і штучний інтелект через обмін знаннями, координацію, організаційне навчання та людський контроль алгоритмічних рішень перетворюються на адаптивні здатності логістичної системи. Визначено обмежувальні умови та ризики інтелектуалізації, зокрема непрозорість алгоритмів, низьку якість даних, платформну залежність, кіберризики та втрату людської експертизи. Сформульовано чотири теоретичні положення про причинні зв'язки в логістичній системі, окреме методологічне положення про зміну одиниці аналізу та інституційне положення про роль журналу. Науковий внесок полягає у відмежуванні інтелектуалізації від цифровізації та AI, побудові перевірюваної системи положень і формуванні Research Agenda. Обмеженням є теоретико-концептуальний характер дослідження, що потребує подальшої операціоналізації та емпіричної перевірки.*

Ключові слова: Інтелектуалізація, логістика, управління ланцюгами поставок, дослідницький порядок денний, концептуальні дослідження, концептуальна основа, інтегративна дослідницька програма, цифрова трансформація, відкрита наука

1. Introduction. The beginning of the 21st century has become a period of profound transformation in logistics and supply chain management. Globalization, digitalization, the rapid development of artificial intelligence, platform business models, autonomous transport systems, the Internet of Things, and digital twin technologies are fundamentally changing the principles of designing, operating, and developing logistics systems [2-6; 11-18]. Concurrently, the world faces unprecedented challenges – geopolitical instability, military conflicts, pandemics, climate change, and energy and food security crises. Under these conditions, logistics increasingly exhibits the characteristics of a complex adaptive socio-technical system, in which a decisive role is played not only by material flows, but also by

data, knowledge, interaction, trust, and the capacity for rapid collective decision-making.

These changes naturally impact the evolution of logistics science. In recent years, there has been a significant surge in research devoted to digital transformation, artificial intelligence applications, big data analytics, the circular economy, sustainable supply chains, humanitarian logistics, digital trade corridors, and other prominent fields [5-10; 19-35]. However, the vast majority of publications focus on addressing narrow applied problems or examining specific technological solutions. Considerably less attention is paid to comprehending fundamental shifts within logistics science itself, as well as developing new theoretical constructs, conceptual frameworks, and integrative research agendas.

Signs of methodological fragmentation are gradually accumulating within the academic community. Individual research streams evolve with extreme intensity, yet frequently remain isolated from one another, utilizing disparate conceptual approaches, terminologies, and research traditions. Consequently, a paradoxical situation arises: while the volume of scientific knowledge grows exponentially, the need for its integration and conceptual re-evaluation becomes increasingly acute. Therefore, alongside empirical studies, conceptual articles capable of shaping new research avenues, explaining systemic shifts, and proposing new scientific frameworks for their interpretation acquire paramount importance.

Against this backdrop, the concept of intellectualization of logistics and supply chain management becomes increasingly relevant. In this article, it is viewed not as a synonym for digitalization or the implementation of isolated artificial intelligence technologies, but as a qualitatively new stage of logistics development. This stage is characterized by the integration of human intelligence, organizational memory and learning capacity, inter-organizational collective intelligence, and artificial intelligence, as well as the widespread utilization of data and knowledge, the development of adaptive management mechanisms, interdisciplinary research, and the formation of new theoretical models for operating complex logistics systems.

In this context, the role of scientific journals is evolving as well. While traditionally serving primarily to disseminate findings of completed studies, modern academic periodicals are increasingly becoming active participants in shaping the scientific agenda, fostering international research networks, and initiating new scholarly debates. It is precisely through editorial policy, special issues, conceptual publications, methodological papers, and open academic discussions that they can significantly influence the development trajectory of specific scientific fields.

The re-confirmation of the status of the journal "Intellectualization of Logistics and Supply Chain Management" as a Category "B" professional scientific publication represents an important milestone in its development. At the same time, the editorial board considers this event not as the conclusion of a certain stage, but as a rationale for re-conceptualizing the journal's mission in both national and international academic spaces. The natural next step must be to strengthen the journal's role as an international platform for advancing conceptual research, establishing new scientific domains, and integrating interdisciplinary knowledge in logistics and supply chain management.

By genre, this article is a programmatic conceptual publication formatted as an editorial perspective. It does not claim the status of a finalized theory or a proven scientific paradigm. Its purpose is different: to propose an integrative conceptual framework and an open research agenda within which various avenues of contemporary logistics science can be understood as interconnected manifestations of a broader

intellectualization process. This genre selection also determines the nature of the argumentation: the article combines conceptual synthesis, problem statement, the formulation of an authorial framework, and the outlining of an open research agenda [27; 36-38].

The objective of this article is to substantiate the intellectualization of logistics and supply chain management as a process of developing logistics system capabilities, build an integrative conceptual framework for its analysis, identify key methodological challenges of modern logistics science, and outline the journal's role as an academic platform for the development, critical discussion, and subsequent operationalization of the corresponding research agenda.

Accordingly, the article answers the following research questions: how can the intellectualization of logistics be conceptualized as a process of developing logistics system capabilities without equating it with digitalization, automation, or AI; through what core mechanism are sources of intelligence transformed into adaptive capabilities and systemic outcomes; how does the proposed framework differ from the related concepts of digital, smart, autonomous, cognitive, knowledge-based, and resilient logistics; how can a scientific journal support the formation and validation of conceptual frameworks; and what research clusters, questions, units of analysis, theoretical lenses, and methods should constitute an open Research Agenda for the intellectualization of logistics.

The scientific contribution of the article consists of four interconnected outcomes. First, the intellectualization of logistics is substantiated as an integrative conceptual framework that is not reducible to digitalization, automation, or the application of artificial intelligence. Second, four key categories are differentiated: intellectualization as a capability development process, an intelligent logistics system as an analytical system type, a conceptual framework as an analytical tool, and a research agenda as a domain for further inquiry. Third, a mechanistic-process model of intellectualization is proposed, and propositions are grouped by level: theoretical propositions on causal relationships in the logistics system, a methodological proposition regarding the unit of analysis, and an institutional proposition regarding the journal's role. Fourth, a structured Research Agenda is established, translating the journal's thematic priorities into a system of research problems, questions, units of analysis, theoretical lenses, and methods.

2. Conceptual Research Methodology. This article is executed as a theoretical and conceptual study aimed not at empirical hypothesis testing, but at constructing an integrative framework for comprehending the current stage of logistics and supply chain management development. The methodological foundation of the study comprises a targeted conceptual literature review, a comparative analysis of key concepts, theoretical synthesis, and logical modeling. This approach aligns with the genre of a programmatic conceptual paper: it enables not only the synthesis of existing research streams, but also the proposal of an open research agenda for further scientific debate.

The subject of analysis includes contemporary concepts of digital, intelligent, cognitive, autonomous, adaptive, and resilient logistics, as well as studies that view supply chains as complex socio-technical, network, and ecosystem structures [1-25; 39; 40]. Particular attention is given to works analyzing artificial intelligence, big data, digital twins, the Internet of Things, autonomous logistics systems, circular logistics, humanitarian logistics, knowledge management, resilience, and digital trade and logistics corridors [5-18; 26-35; 39; 40]. These research streams are viewed not as isolated thematic domains, but as sources of concepts

and mechanisms necessary to construct an integrative concept of intellectualization.

The literature selection logic was grounded in the principles of a targeted conceptual review rather than a systematic meta-analysis. The source base was formed by selecting peer-reviewed articles, conceptual reviews, programmatic publications, and highly methodologically relevant works indexed in international scientometric databases and academic search engines. The primary time horizon encompassed publications from 2019–2026, as this period witnessed the intensive evolution of research on digital logistics transformation, Industry 4.0, artificial intelligence, and supply chain resilience. Classical works in logistics and supply chain management were utilized as a theoretical baseline for comparing previous and contemporary stages of the discipline's development.

The search, thematic selection, and verification of sources were conducted on July 24, 2026. The source base was drawn from the academic search engines Scopus, Web of Science, and Google Scholar, as well as from publisher portals including Elsevier, Emerald, Taylor & Francis, Springer, Wiley, IEEE, MDPI, and relevant institutional repositories. Bibliographic metadata for the final corpus – specifically DOIs, author names, article titles, journals, publication years, volumes, issue numbers, and page ranges – were additionally verified via Crossref. The search horizon primarily covered 2019–2026 publications; classical works were included only when necessary to explain the theoretical origins of specific concepts or conceptual research methodology. The initial working pool was built as a targeted rather than exhaustive bibliometric sample, incorporating publications directly addressing digitalization, artificial intelligence, resilience, circularity, humanitarian logistics, complex adaptive systems, knowledge management, and theory-building in supply chain management. Following thematic filtering, duplicate removal, and DOI verification, 40 sources were included in the conceptual analysis [1-40].

The search was conducted using the following English search strings and their combinations: digital logistics; intelligent logistics; smart logistics; cognitive logistics; autonomous logistics; artificial intelligence in logistics; artificial intelligence supply chain resilience; digital twin logistics supply chain systems; digital supply chain management industry 4.0 logistics review; supply chain resilience digitalization systematic literature review; adaptive supply chains; circular supply chain digital technologies; humanitarian logistics digital technology resilience; logistics ecosystems; knowledge management supply chain digital transformation; conceptual research supply chain management; research agenda supply chain management; theory building in supply chain management. Sources were included if they met at least one of the following criteria: proposed a new concept or conceptual model; synthesized the evolution of a distinct research stream; explained mechanisms of logistics system transformation; exhibited an interdisciplinary character; or contained methodological propositions relevant to formulating a research agenda. Excluded from the analysis were sources lacking DOIs or complete metadata, duplicates, preprints, non-peer-reviewed materials, publications with retraction notices, purely technical papers disconnected from logistics or SCM, and articles that duplicated already represented approaches without offering new concepts, mechanisms, or explanatory logic.

Because the study was conducted as a targeted conceptual review rather than a systematic bibliometric analysis or meta-analysis, the total volume of initial search hits per database was not treated as evidentiary statistics for the article. The study's working log documented the final corpus of 40 sources included in the conceptual analysis, along with the procedure for their thematic and bibliographic verification. The initial

record counts in Scopus, Web of Science, and Google Scholar, the number of duplicates, and the count of sources post-screening were not presented as established facts, as an exhaustive bibliometric search log per database was not retained. This limitation reduces the search phase's replicability, yet it does not preclude utilizing the assembled corpus for programmatic conceptual synthesis.

Source coding was performed manually using a thematic-conceptual scheme. For each source, the following were recorded: research stream, central concept, main object of analysis, unit of analysis, dominant explanatory logic, role of technology, role of humans, role of knowledge, adaptation or coordination mechanisms, and conceptual boundaries of the approach. Following initial coding, concepts and mechanisms were cross-compared across streams, enabling the identification of recurrent semantic clusters: knowledge creation and utilization, analytical decision support, organizational learning, human-algorithm interaction, trust, inter-organizational coordination, self-organization, adaptation, and evolutionary system change. These clusters formed the foundation for the subsequent articulation of the five dimensions of intellectualization and the mechanistic-process model.

Material synthesis proceeded through several sequential stages. First, the main streams of contemporary logistics transformation were identified: digitalization, artificial intelligence, autonomy, resilience, circularity, humanitarian logistics, ecosystems, and knowledge management. Next, the conceptual boundaries of each stream and the recurrent mechanisms through which distinct forms of intelligence are converted into systemic capability were determined: knowledge sharing, coordination, organizational learning, and human oversight of algorithmic decisions. On this basis, four categories were differentiated: intellectualization as a capability development process, an intelligent logistics system as an analytical system type, a conceptual framework as an analytical tool, and a research agenda as a set of questions for further testing. Subsequently, the mechanistic-process model was constructed, and an open research agenda was formulated.

The sequence of building the conceptual framework is summarized in Figure 1. It encompasses the search and thematic selection of sources, grouping of research streams, analysis of their conceptual boundaries, identification of recurrent mechanisms, differentiation of key categories, model construction, formulation of propositions, and specification of the research agenda.

As shown in Figure 1, the proposed conceptual framework was formed not through an arbitrary combination of current concepts, but as a result of a sequential conceptual synthesis. The transition from building the source base and structuring research streams to constructing the model and formulating theoretical propositions ensures the internal consistency of the framework and creates a foundation for its further operationalization and empirical testing.

The quality of the proposed concept was evaluated against six criteria. The first criterion is distinctiveness from existing concepts: the analysis verified whether intellectualization duplicates digitalization, automation, artificial intelligence implementation, or knowledge management, and whether it explains their relationship within a broader systemic logic. For this purpose, its conceptual boundaries were compared with digital logistics, smart logistics, Logistics 4.0/5.0, AI logistics, as well as cognitive, autonomous, knowledge-based, resilient, and complex adaptive logistics. The second criterion is logical consistency: elements of the concept were cross-examined to identify potential internal contradictions. The third criterion is explanatory power: the framework's ability to interpret various

avenues of contemporary logistics research as manifestations of a common process was assessed. The fourth criterion is operationalizability: the suitability of the proposed dimensions for subsequent conversion into variables, indicators, research questions, or hypotheses was analyzed. The fifth criterion is boundary conditions definition: it was clarified that the concept applies primarily to complex socio-technical logistics systems in which knowledge, data, technology, interaction, and adaptability become key drivers of development. The sixth criterion is generativity: the concept's capacity to establish a basis for new research programs, testable questions, and interdisciplinary discussions was evaluated.

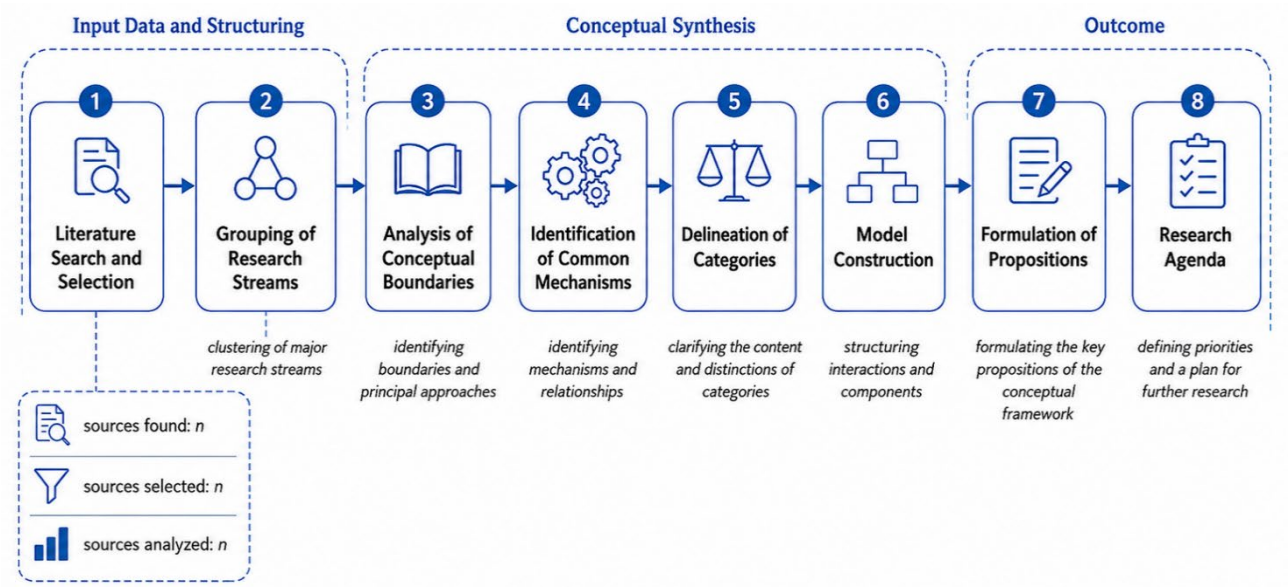


Figure 1 – Methodological Logic for Constructing the Conceptual Framework
Source: developed by the author.

Thus, the methodology of the article combines conceptual analysis, theoretical synthesis, and programmatic research agenda setting. This clearly distinguishes the presented material from an essayistic exposition: the conclusions of the article are grounded not on a free interpretation of isolated trends, but on a rigorous procedure of identifying scientific streams, analyzing their boundaries, determining common mechanisms, building an integrative framework, and outlining criteria for its further validation.

3. From Digital Logistics to Intelligent Socio-Technical Systems

Over the past three decades, logistics and supply chain management have matured as an independent, interdisciplinary scientific domain combining advances in economics, management, engineering, information technology, systems analysis, and operations research. Throughout this period, academic research has significantly expanded its subject field: from optimizing transport and warehousing processes to managing global value chains, digital platforms, risks, resilience, and supply chain sustainability.

Since the second decade of the 21st century, scientific discourse has increasingly shifted toward digital transformation [2-4]. Scholars have focused on Industry 4.0 technologies, the Internet of Things, artificial intelligence, big data, blockchain, digital twins, autonomous transport systems, warehouse robotics, and digital trade platforms [3-6; 11-18]. Concurrently, avenues in humanitarian logistics, the circular economy, green logistics, cybersecurity of logistics systems, risk management, resilience

building, and post-crisis recovery have actively evolved [19-35].

While these streams have broadened the scope of logistics science, they have simultaneously amplified its fragmentation. A significant portion of research remains technologically or empirically focused: attention is concentrated on isolated digital solutions, algorithms, optimization models, disruption response scenarios, or specific flow types. Considerably less developed is the question of how these avenues interact within a complex adaptive socio-technical logistics system.

To systematize these trends, Table 1 summarizes the primary streams of contemporary logistics research. While the table is not the output of an exhaustive bibliometric analysis of the entire field, it captures the key conceptual boundaries of the streams most frequently highlighted in recent review, conceptual, and empirical works [1-35; 39; 40].

Table 1. Main streams of contemporary logistics research and their integrative gap

Stream	Research Focus	Dominant Logic	Integrative Gap	What Intellectualization Adds
Digital Logistics and Supply Chain 4.0	Data, platforms, digital capabilities	Process automation and visibility	Human, social, and evolutionary dimensions	Connects technology with knowledge, learning, and interaction [2–4; 39; 40]
AI in Logistics and SCM	Algorithmic solutions, forecasting, optimization	Decision support or automation	Accountability, trust, human expertise	Views AI as part of hybrid intelligence [1; 5–10]
Digital Twins	Virtual models of processes and supply chains	Monitoring, simulation, stress-testing	Organizational learning and social coordination	Integrates digital models into the knowledge and feedback cycle [11–18]
Resilience and Viability	Disruption response and recovery	Adaptation, reserves, scenario-based management	Crisis experience accumulation and learning	Explains resilience as an emergent outcome of capabilities [19–25]
Circular and Sustainable Logistics	Closed-loop flows, sustainability, resource cycles	Ecological efficiency	Collective decision-making and digital coordination	Combines sustainability with inter-organizational intelligence [26–31]
Humanitarian Logistics	Crisis and humanitarian supply chains	Rapid response, transparency, trust	Long-term crisis memory and AI ethics	Links response mechanisms with social and cognitive dimensions [32–35]
Business Ecosystems	Platforms, partnerships, co-creation of value	Orchestration of autonomous actors	Cognitive and technological network architecture	Uncovers inter-organizational collective intelligence [35; 39; 40]

Sourse: compiled by the authors based on [2-40].

The presented synthesis demonstrates that each of the examined streams possesses its own research focus, dominant logic, and typical unit of analysis. While this ensures the depth of specialized research, it simultaneously creates a risk of conceptual isolation. The integrative gap lies in the insufficient explanation of how digital technologies, knowledge, organizational learning, trust, adaptation, and collective interaction together form a new quality of the logistics system.

4. Conceptual Boundaries of Logistics Intellectualization

The current stage of logistics development is characterized by changes not

only in technologies, but in the very nature of logistics systems themselves. While previous stages of evolution were primarily associated with improving the management efficiency of material, financial, and information flows, today the capacity of systems to create, integrate, utilize, and reproduce knowledge is increasingly becoming the defining driver of development. Within this article, it is precisely this qualitative transformation that is examined as the intellectualization of logistics and supply chain management.

In contemporary scientific literature, the concept of intellectualization is most frequently linked to the digital transformation of logistics, the implementation of artificial intelligence, big data technologies, the Internet of Things, digital platforms, robotics, and other information and communication technologies [2-10; 14; 40]. Undeniably, these processes are crucial components of modern logistics system evolution. However, in our view, equating intellectualization exclusively with technological innovations substantially narrows the scope of this concept.

Technologies in and of themselves do not create an intelligent logistics system. They merely expand the capacities of humans, organizations, and networks regarding information processing, decision-making, and operational coordination. The decisive factor is not the presence of isolated digital tools, but the system's ability to learn, adapt to changes, accumulate knowledge, form new behavioral patterns, and ensure the effective interaction of a large number of autonomous participants. For this reason, intelligence should be viewed not as a property of an individual human or software algorithm, but as an emergent property of a logistics system that arises from the interaction of its elements.

This understanding reflects the natural evolution of logistics as a scientific discipline. While classical logistics focused on material flow management, and the supply chain management concept integrated material, information, and financial flows within a unified network, the current stage of development is characterized by a transition to managing knowledge, adaptability, interaction, and the collective capacity of logistics systems to learn and make decisions. Thus, intellectualization does not contradict previous concepts, but logically extends their evolution, elevating the subject of study to a new level of complexity.

Concurrently, the nature of logistics systems themselves is changing. They are increasingly exhibiting the characteristics of complex adaptive socio-technical ecosystems, in which humans, organizations, digital platforms, artificial intelligence algorithms, autonomous hardware assets, regulatory institutions, and global networks of knowledge creation and exchange interact. The behavior of such systems is determined not only by the optimization of individual processes, but also by mechanisms of self-organization, co-evolution, trust, inter-organizational coordination, and continuous adaptation to external shifts.

Under these conditions, the essence of management undergoes a fundamental change. Its subject becomes not merely material or information flows, but primarily the processes of knowledge creation, integration, sharing, capability development, trust building, decision-making support, and ensuring the capacity of logistics systems for self-learning and self-development. It is these characteristics that determine the competitiveness, resilience, and long-term efficiency of modern business ecosystems.

In this context, it is appropriate to differentiate four interconnected, yet distinct categories:

– Intellectualization of logistics and supply chain management is the process of developing the capabilities of logistics systems to create, integrate, utilize, and reproduce knowledge, make informed decisions, adapt, self-organize, and engage in collective interaction. This refers not merely to the adoption of digital technologies or artificial intelligence algorithms, but to the

formation of a new operational quality of the system, in which knowledge, data, competencies, trust, and coordination become key drivers of development.

– An intelligent logistics system is an analytical system type of logistics system in which the capabilities for knowledge creation, learning, coordination, and adaptation have acquired a stable organizational, technological, and social form. Such a system functions as a complex adaptive socio-technical ecosystem whose development is sustained by the synergy of human intelligence, organizational memory and learning capacity, inter-organizational collective intelligence, and artificial intelligence.

– The conceptual framework of intellectualization is a scientific analytical tool that allows describing, comparing, and explaining the technological, cognitive, organizational, social, and evolutionary dimensions of logistics systems development. Its purpose is not to replace existing concepts of digitalization, automation, resilience, or knowledge management, but to explain their interrelationship within a broader systemic logic.

– The research agenda of intellectualization is a set of open questions, avenues, and hypotheses for further conceptual, empirical, and applied studies. It defines which aspects of the proposed framework require operationalization, empirical testing, critical refinement, and interdisciplinary discussion.

Thus, in this article, intellectualization is not equated with an analytical system type, a methodological framework, or a list of future topics. It is a process; an intelligent logistics system is an analytical type used to describe the stable form of this process; the conceptual framework is a method for its scientific analysis; and the research agenda is the direction for the further development of this analysis.

To substantiate scientific novelty, it is essential to show not only a positive definition of intellectualization, but also its distinction from related concepts already utilized in contemporary logistics literature. Digital logistics, smart logistics, Logistics 4.0/5.0, AI logistics, cognitive logistics, autonomous logistics, knowledge-based supply chain management, digital supply chain, resilience, and the concept of complex adaptive systems explain important, yet partial aspects of logistics transformation [1-25; 36-40]. The proposed framework (Table 2) does not deny these approaches, but clarifies their boundaries and integrates them into a broader logic of developing logistics system capabilities.

Table 2 – Conceptual boundaries of logistics intellectualization

Concept	What It Explains Best	Typical Boundary of Explanation	Unit of Analysis	How Intellectualization Differs
Digital Logistics / Digital Supply Chain	Data, platforms, flow integration	Weaker at explaining learning, trust, and self-organization	Process, enterprise, supply chain	Demonstrates how digital integration becomes a system's capability to learn
Smart Logistics / Logistics 4.0	Automation, sensors, cyber-physical systems	Tends toward technological determinism	Technical system, operation, supply chain	Treats technology as infrastructure rather than the essence of intellectualization
Logistics 5.0	Human-centricity, sustainability, responsibility	Does not always explain the mechanism of human, organizational, and AI interaction	Organization, supply chain, community	Specifies the logic of hybrid intelligence and human oversight
AI and Autonomous Logistics	Algorithmic decision-making,	May ignore accountability, context,	Task, function, autonomous asset	Treats AI as one of the sources of distributed intelligence

	forecasting, autonomous action	and inter-organizational coordination		
Knowledge-Based SCM	Knowledge, competencies, organizational learning	Less fully incorporates digital infrastructure and algorithmic models	Organization, supply chain, partner network	Combines knowledge with technology, trust, and evolutionary adaptation
Supply Chain Resilience	Disruption response, recovery, viability	Frequently focuses on crises rather than continuous system learning	Supply chain, network, crisis event	Explains resilience as an emergent outcome of interacting capabilities
Complex Adaptive Supply Systems	Emergence, self-organization, co-evolution	Remains a overly broad systemic lens	Network, ecosystem	Operationalizes complexity through sources of intelligence, mechanisms, and dimensions

Source: developed by the author.

The presented comparison demonstrates that the scientific novelty of the proposed framework lies not in introducing yet another term for digital transformation, but in integrating the partial explanations that already exist across related concepts. Digital logistics and the digital supply chain effectively explain the role of data and platforms, yet reveal weaker explanations regarding the mechanisms of learning, trust, and social interaction. AI logistics concentrates on algorithmic decision support, but does not always account for organizational accountability and the hybrid nature of intelligence. Resilience explains responses to disruptions, yet requires a broader link to knowledge accumulation and the evolutionary development of the system. The concept of complex adaptive systems provides an overarching logic of self-organization, whereas intellectualization specifies it for logistics through sources of intelligence, transformation dimensions, and systemic outcomes.

5. Mechanistic-Process Model of Logistics Intellectualization

To prevent the proposed model from turning into a broad listing of sources, dimensions, and outcomes, it must be subordinated to a single central theoretical core. In this article, this core is formulated as follows: human intelligence, organizational memory and learning capacity, inter-organizational collective intelligence, and artificial intelligence – through mechanisms of knowledge sharing, coordination, organizational learning, and human oversight of algorithmic decisions – are transformed into adaptive capabilities of the logistics system. Consequently, intellectualization is explained not as the mere presence of numerous modern technologies or competencies, but as a process of converting distributed sources of intelligence into a system's capacity to learn, align actions, respond to disruptions, and update its own decision-making models.

The logic of the model is processual in nature: sources of intelligence transition into integration mechanisms; integration mechanisms shape adaptive capabilities across five dimensions; mature capabilities manifest in systemic outcomes; operational experience, feedback, and the consequences of implemented decisions update knowledge, coordination rules, and algorithmic models. As a result, the model demonstrates not only the components of intellectualization, but also the sequence of transformations, mediation, and cyclical learning within the system.

The generalized logic of transforming distributed sources of intelligence into adaptive capabilities and systemic outcomes of a logistics system is presented in Figure 2. The model reflects not only the components of intellectualization, but also the causal

sequence of their interaction: sources of intelligence are integrated through knowledge sharing, analytical support, coordination, organizational learning, trust building, and human oversight of algorithmic decisions; these mechanisms shape system capabilities across cognitive, technological, organizational, social, and evolutionary dimensions, which under appropriate conditions leads to enhanced decision quality, adaptability, resilience, flexibility, sustainability, and value co-creation.

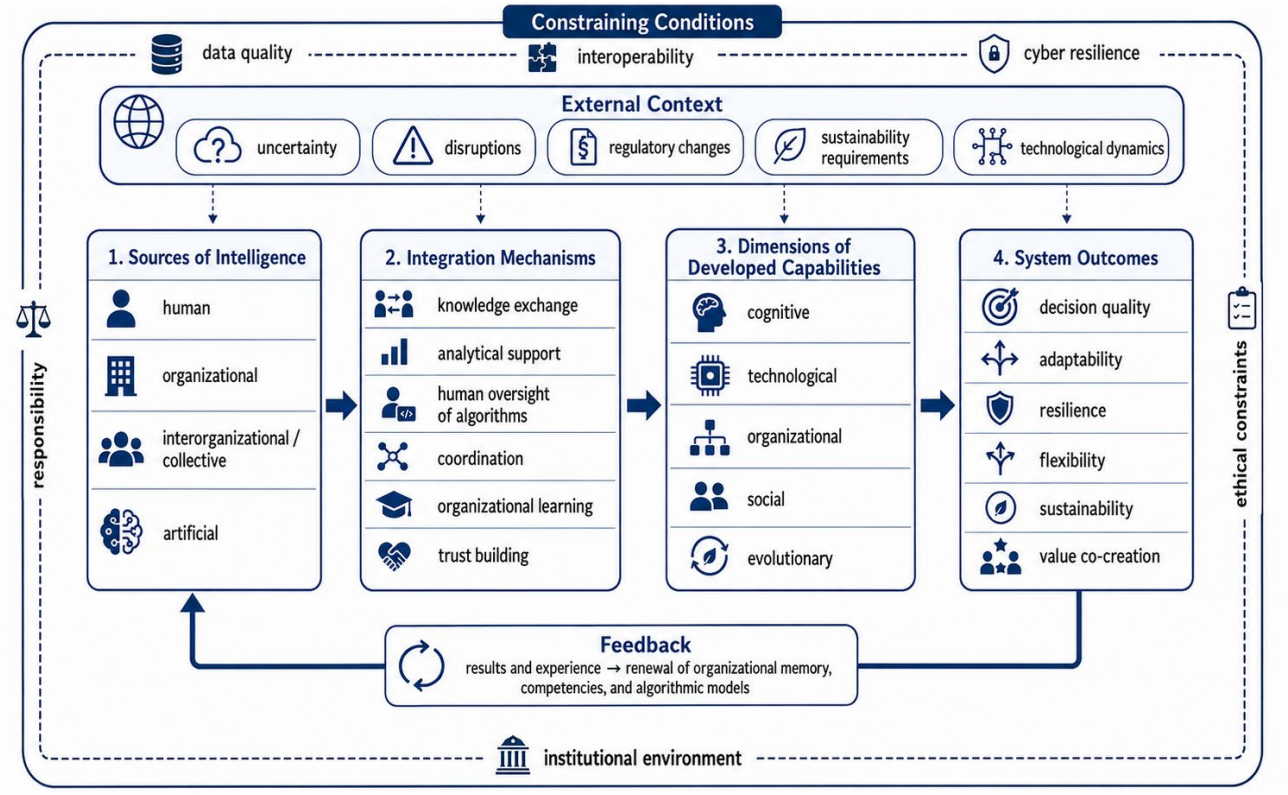


Figure 2 – Mechanistic model of logistics system intellectualization
Source: developed by the author.

As shown in Figure 2, the mere presence of human expertise, organizational memory, inter-organizational collective intelligence, or artificial intelligence technologies does not ensure the intellectualization of a logistics system. The decisive factor is the functioning of integration mechanisms that convert distributed knowledge, experience, data, and algorithmic recommendations into coordinated decisions and adaptive system behavior. Therefore, integration mechanisms constitute the central explanatory link of the proposed conceptual framework.

The model also demonstrates that systemic outcomes are not a guaranteed consequence of digitalization. Their formation depends on boundary conditions, including data quality, system interoperability, cyber resilience, accountability definition, ethical constraints, and the institutional environment. If these conditions are not met, digital technologies may fail to enhance system adaptability, instead scaling errors, increasing dependency on technological infrastructure, and creating new organizational and cybernetic risks.

Feedback completes the processual loop of intellectualization. Data on decision outcomes, experience in disruption response, identified errors, and emerging practices must flow back into the system in the form of updated organizational memory, competencies, coordination procedures, and algorithmic models. In this manner,

intellectualization emerges not as a one-off technological transformation, but as a cyclical process of learning and development within the logistics system.

The first link of the model is sources of intelligence. They answer the question of whose or what intelligence is leveraged in the development of the logistics system. These include:

– Human intelligence, associated with professional knowledge, experience, expertise, and managerial accountability.

– Organizational memory and learning capacity, manifested in accumulated procedures, culture, knowledge, response rules, and the organization's ability to convert experience into new managerial practices.

– Inter-organizational collective intelligence, i.e., the ability of autonomous network participants to co-create knowledge, align decisions, and adapt behavior.

– Artificial intelligence, implemented through algorithms, analytical systems, digital agents, digital twins, and autonomous technologies.

The second link is integration mechanisms. They perform the core explanatory function of the model by demonstrating under what conditions distinct sources of intelligence cease to be isolated resources and begin to form systemic capability. Knowledge sharing ensures the transfer of experience, data, and practical interpretations among humans, organizations, and digital systems. Coordination aligns the decisions of autonomous or semi-autonomous supply chain participants. Organizational learning transforms isolated disruption responses into stable rules, procedures, competencies, and updated behavioral models. Human oversight of algorithmic decisions guarantees accountability, explainability, and the adjustment of automated recommendations in situations of high uncertainty. Trust in this model is viewed as a prerequisite for effective knowledge sharing and a mechanism for inter-organizational coordination, rather than an independent systemic outcome.

The third link is mature capabilities across the five dimensions of intellectualization:

– The cognitive dimension reflects the capacity to create, accumulate, integrate, and utilize knowledge.

– The technological dimension captures the ability to employ digital platforms, AI, digital twins, the Internet of Things, robotic systems, and big data analytics as the infrastructure for intelligent management.

– The organizational dimension characterizes not a source of intelligence, but the transformation of structures, roles, decision rights, coordination procedures, and interaction models among autonomous actors.

– The social dimension reflects the capacity to sustain trust, collaboration, leadership, human capital development, and collective decision-making.

– The evolutionary dimension characterizes the capacity for self-organization, innovative development, co-evolution, and continuous adaptation under conditions of high uncertainty.

Thus, organizational memory and learning capacity act as a source of intelligence, whereas the organizational dimension describes the domain of structural and managerial system transformation.

The fourth link is systemic outcomes. The immediate integral outcome of intellectualization is the adaptive capability of the logistics system – that is, the capacity to modify decisions, routes, roles, procedures, partnerships, and resource deployment models in response to shifting conditions. Through this capability, broader systemic outcomes can take shape: decision quality, resilience, sustainability, flexibility, and value co-creation. At the same time, these outcomes are not guaranteed by products of digitalization or AI implementation. They emerge only when sources of intelligence are integrated through the specified mechanisms and anchored within the corresponding

cognitive, technological, organizational, social, and evolutionary capabilities.

This structuring aligns the distinct elements of the authorial concept within a single unified model and mitigates the risk of excessive combinatorics. Sources of intelligence do not substitute for the dimensions of intellectualization, but explain the origin of knowledge, experience, decisions, and algorithmic recommendations. Integration mechanisms are not an additive list of factors, but represent a causal bridge between distributed intelligence and the adaptive capability of the system. Dimensions are not types of intelligence, but delineate the domains in which this capability is anchored. Systemic outcomes are not an automatic consequence of digitalization, but arise provided that integration mechanisms genuinely convert individual resources into coordinated logistics system behavior.

Figure 2 establishes the sequence: "sources of intelligence → integration mechanisms → capabilities across five dimensions → systemic outcomes → experience and feedback → knowledge and model updates". This mode of presentation is essential for a conceptual article: it demonstrates causality, mediation, boundary conditions, and cyclical system learning, rather than offering a static list of components.

From a methodological standpoint, the mechanistic-process model enables the integration of a wide spectrum of contemporary research streams into a single conceptual framework [1-40]. Digital twins, artificial intelligence, big data, the Internet of Things, blockchain, autonomous transport, digital trade and logistics corridors, circular and humanitarian logistics, resilience management, business ecosystems, and other avenues cease to be treated as isolated objects of study. They emerge as diverse sources, infrastructures, or contexts for intelligence integration, the impact of which depends on whether knowledge sharing, coordination, organizational learning, human oversight of algorithmic decisions, and feedback loops are effectively secured.

In this lies the strategic value of the proposed concept. It is not intellectualization itself, but the conceptual framework of its analysis that unites the findings of different scientific schools, refines the conceptual apparatus, and creates a methodological foundation for subsequent conceptual and empirical studies in logistics and supply chain management. Within this article, the authors deliberately refrain from proclaiming intellectualization a new scientific paradigm; such status can only be recognized through broader adoption of this problem-formulation approach, explanatory logic, and method selection within the scientific community. Therefore, the research agenda of intellectualization is presented as an open set of propositions and questions requiring further operationalization, critical discussion, and empirical validation.

5.1. Propositions for Further Testing

To prevent the proposed model from remaining merely a descriptive framework, it must be translated into propositions suitable for subsequent operationalization (Table 3). These propositions operate across different levels: theoretical propositions describe causal and mediated relationships within the logistics system; the methodological proposition clarifies the unit of analysis; and the institutional proposition addresses the journal's role in shaping the research field (and is presented separately in Section 7). This division prevents the conflation of systemic theory, research methodology, and editorial policy.

The presented theoretical propositions serve two key functions. First, they render the conceptual framework open to academic debate: each proposition can be supported, refined, or contested in subsequent research. Second, they transform the general model of intellectualization into a set of testable relationships between sources of intelligence,

integration mechanisms, transformation dimensions, and systemic outcomes.

Table 3 – Theoretical propositions of the conceptual framework of logistics intellectualization

Proposition	Content	Direction of Testing
1. Complementarity of Dimensions	Intellectualization is determined not by the maximum development of a single dimension, but by the alignment of cognitive, technological, organizational, social, and evolutionary dimensions.	Comparison of balanced versus technology-dominant profiles of logistics systems.
2. Mediated Impact of AI	Artificial intelligence enhances adaptability only through data quality, organizational learning, and human oversight of algorithmic decisions.	Testing the mediating effect of data, learning, and human-in-the-loop mechanisms.
3. Emergent Nature of Resilience	Resilience is an emergent outcome of interacting technological, social, and organizational capabilities, rather than a direct consequence of digitalization.	Comparison of digital sophistication with actual recovery speed and adaptability.
4. Integration of Distributed Intelligence	Human, organizational, inter-organizational, and artificial intelligence are converted into adaptive capabilities through knowledge sharing, coordination, learning, and oversight.	Analysis of the role of integration mechanisms between sources of intelligence and systemic outcomes.

Source: developed by the author.

The methodological proposition of this article asserts that intellectualization alters the primary unit of analysis in logistics science: shifting from an individual process or enterprise to a supply chain, network, and socio-technical ecosystem. This proposition does not describe an internal causal mechanism within the logistics system, but specifies the level at which such a system should be investigated. It can be tested by comparing the explanatory power of models operating at different scales: functional, organizational, network, and ecosystemic.

5.2. Boundary Conditions and Risks of Intellectualization

The mechanistic-process model of intellectualization does not assume an automatic transition from digitalization or AI implementation to adaptability, resilience, sustainability, and value creation. On the contrary, its explanatory strength also lies in revealing when the expected positive effect may fail to materialize. If sources of intelligence are not integrated through effective knowledge sharing, coordination, organizational learning, and human oversight of algorithmic decisions, intellectualization can introduce new vulnerabilities or scale existing errors.

Consequently, intellectualization must be viewed not as a linearly positive process, but as an ambivalent transformation of a complex socio-technical system. It can enhance adaptability only in the presence of sufficient data quality, transparent algorithmic procedures, distributed accountability, cyber resilience, system interoperability, preservation of human expertise, and balanced data access rules. In the absence of these conditions, the very same technologies and organizational mechanisms can amplify algorithmic opacity, platform lock-in, data power concentration, cyber risks, automated erroneous decisions, local optimization at the expense of the system, and the environmental costs of digital infrastructure.

The most critical boundary conditions include data quality and availability, algorithmic transparency, meaningful human oversight, digital system interoperability, cyber resilience, equitable data access rules, and the organizational capacity to retain critical expertise. Lacking these,

intellectualization may weaken rather than strengthen the system: scaling faulty decisions, diluting accountability, deepening platform lock-in, generating cascading digital vulnerabilities, reinforcing localized optimization to the detriment of the network, or increasing the environmental footprint of digital infrastructure.

Thus, the intellectualization model must not only explain the desired developmental trajectory of logistics systems, but also define its boundaries. This distinction is vital for subsequent operationalization: future empirical studies must test not only the direct or mediated positive impacts of intellectualization, but also the conditions under which these effects diminish, reverse direction, or yield unintended consequences. For this reason, risks, constraints, and negative scenarios are not external add-ons to the concept, but an integral part of its theoretical architecture.

6. Research Agenda

The rapid transformation of the global economy, business process digitalization, geopolitical instability, climate challenges, and accelerated technological progress impose fundamentally new demands on logistics science. Under these conditions, establishing a long-term academic research agenda – which consolidates the efforts of the scholarly community around the most promising and socially significant issues – becomes just as critical as analyzing current operational processes.

The editorial board of the journal operates on the premise that modern logistics is undergoing a transition from predominantly functional flow management to the governance of complex adaptive socio-technical systems. Therefore, a Research Agenda cannot be limited to a mere list of thematic priorities. It must capture unresolved scientific problems, formulate research questions, define units of analysis, propose theoretical lenses, guide authors on appropriate methodologies, and outline the type of scientific contribution expected from future submissions.

To this end, the journal's research avenues are presented as a system of research clusters (Table 4). Each cluster directly connects to the mechanistic-process model of intellectualization proposed in this article: sources of intelligence specify which actors or systems generate knowledge, decisions, and algorithmic recommendations; integration mechanisms explain the bridge from isolated resources to adaptive capabilities; intellectualization dimensions delineate the domains where these capabilities become embedded; and systemic outcomes define the expected effects to be conceptually explained or empirically tested.

The established research agenda is not a simple inventory of thematic topics, but a system of interconnected research clusters. To reflect its internal logic, the clusters are structured across three levels: sources and mechanisms of intelligence; systemic properties and domains of application; and methodological research support. The architecture of the research agenda is presented in Figure 3.

As shown in Figure 3, the first level unites clusters that investigate the sources and mechanisms for building the intellectual capabilities of a logistics system: hybrid intelligence, autonomous systems, digital trust, knowledge, and human capital. These avenues explain which actors, technologies, and mechanisms create knowledge, shape decisions, enable human-algorithm interaction, and support inter-organizational coordination.

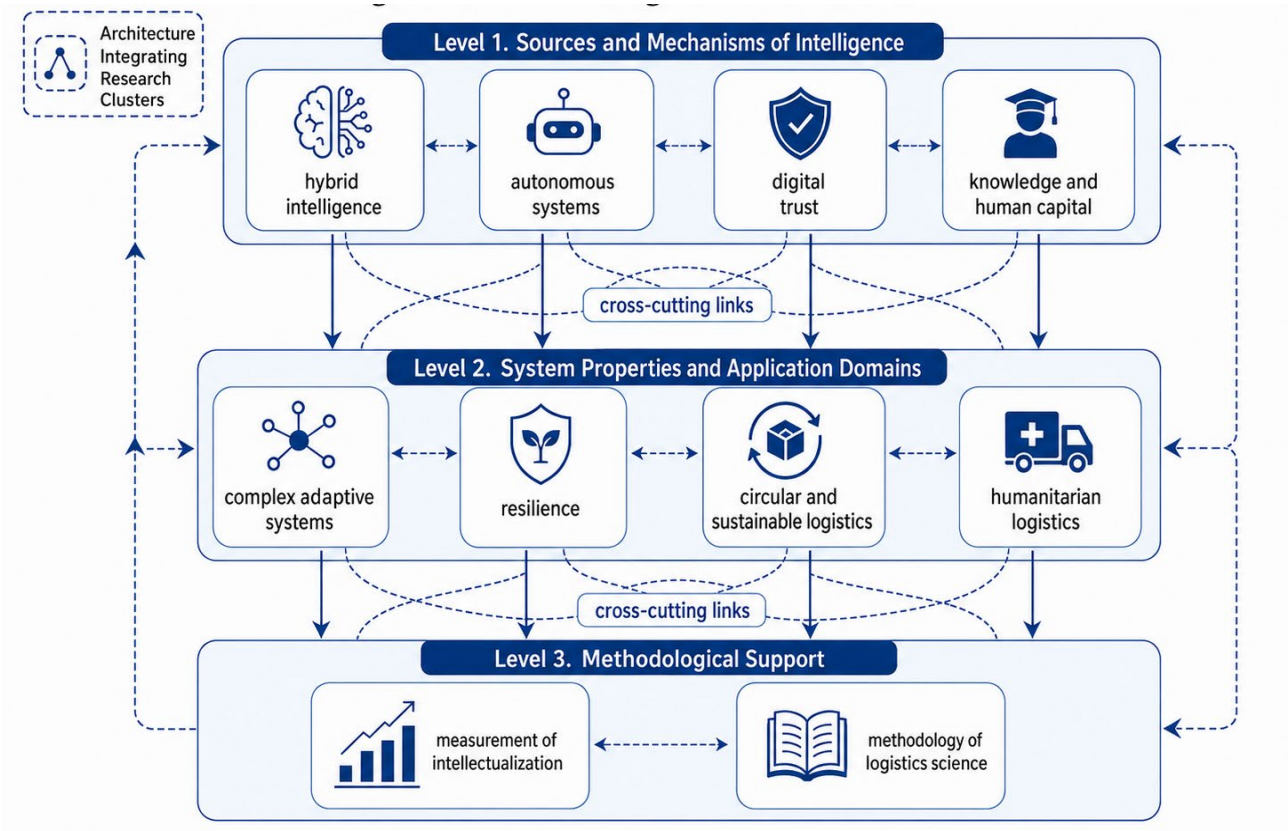


Figure 3 – Research agenda architecture
Source: developed by the author.

The second level encompasses systemic properties and practical application domains of intellectualization: complex adaptive systems, resilience, circular and sustainable logistics, and humanitarian logistics. Within these clusters, research focuses on how the combination of human, organizational, inter-organizational, and technological capabilities influences logistics system adaptation, performance under disruption, resource flow sustainability, and societal resilience.

The third level provides the methodological support for the research program, covering the measurement of intellectualization and the methodological development of logistics science. It ensures concept operationalization, indicator development, unit-of-analysis selection, theoretical proposition testing, and cross-comparison of findings across studies. At the same time, the boundaries between levels remain flexible: cross-cutting linkages demonstrate that each thematic cluster requires an appropriate methodological toolkit, while empirical insights should continuously feed back into refining concepts, models, and research methods.

Figure 3 illustrates the overarching architecture and interdependence of the research clusters. Their substantive breakdown – unresolved problems, core research questions, units of analysis, plausible theoretical lenses, recommended methodologies, and expected types of scientific contribution – is detailed in Table 4.

The presented Research Agenda transforms the journal's thematic profile into an instrument of scientific orientation. Its core logic lies not in establishing an exhaustive list of topics, but in helping authors navigate from a general subject to a research problem, from a problem to a question, and from a question to an appropriate unit of analysis, theoretical lens, and testing methodology. It is precisely this transition that renders the editorial policy not only thematic, but also methodological.

Table 4 – The journal's Research Agenda as a system of research clusters

Cluster	Unresolved Problem	Core Question	Unit of Analysis & Methods	Expected Contribution
Hybrid Intelligence	Allocation of decisions among human, organization, network, and AI	When does a hybrid decision outperform a purely human or algorithmic one?	Team, process, network; experiments, case studies, agent-based modelling	Accountability distribution models; empirical evidence
Autonomous Systems	Boundaries of control and accountability of autonomous agents	How does autonomization transform the management of logistics operations?	Operation, warehouse, route; design science, simulations, digital twins	Governance architectures; autonomy metrics
Complex Adaptive Systems	Transition from local decisions to systemic properties	How do local rules shape network adaptability or vulnerability?	Chain, ecosystem; network analysis, system dynamics	Explanatory models; testable hypotheses
Resilience	Transforming crisis experience into long-term capability	Which mechanisms build resilience following disruptions?	Chain, critical infrastructure; longitudinal studies, case studies	Adaptation models; assessment methodologies
Digital Trust	Data sharing among autonomous actors	Which rules ensure trust without excessive centralization?	Platform, corridor; comparative case studies, design science	Trust architectures; interoperability criteria
Circular and Sustainable Logistics	Aligning sustainability, closed-loop flows, and digital coordination	How does collective intelligence impact circular flows?	Flow network, ecosystem; LCA, modelling, case studies	Integrative models; sustainability metrics
Humanitarian Logistics	Balancing speed, fairness, transparency, and trust	How to coordinate humanitarian supply chains under extreme uncertainty?	Community, humanitarian chain; action research, scenario planning, network analysis	Applied coordination models; policy recommendations
Knowledge and Human Capital	Transition from individual expertise to systemic capability	How do learning and competencies drive supply chain adaptation?	Specialist, team, organization; surveys, interviews, SEM	Measurement scales; competency models
Methodology of Intellectualization	Risk of substituting intellectualization with digitalization metrics	Which indicators reflect the capacity to learn and adapt?	System, chain, ecosystem; Delphi method, scale validation, bibliometrics	Concept operationalization; research agendas

Source: developed by the author.

The identified clusters are not isolated. For instance, studies on hybrid intelligence are directly linked to digital trust, autonomous systems, knowledge management, and the methodology of measuring intellectualization. Research on resilience intersects with humanitarian logistics, complex adaptive systems, and the circular recovery of material flows. Therefore, the journal's mission extends beyond accepting manuscripts on individual topics to supporting works that build inter-cluster bridges and generate a cumulative scientific contribution.

Principles of Building the Editorial Portfolio

The established priorities do not imply restricting the journal's thematic scope. On the contrary, they form an open framework

for advancing scientific inquiry. The editorial team seeks to support works that:

1. Formulate a clear unresolved problem, rather than merely describing a trendy topic.
2. Offer research questions, hypotheses, or conceptual propositions open to debate or empirical testing.
3. Define the unit of analysis and the boundary conditions for the applicability of conclusions.
4. Combine a theoretical lens with methodologies suited for conceptual or empirical validation.
5. Generate a scientific contribution across one or several levels: empirical evidence, methods, models, concepts, theories, or research agendas.
6. Adhere to the principles of open science, reproducibility of results, and international academic collaboration.

Thus, the journal's Research Agenda serves not as a closed list of subjects, but as an open research platform. Its purpose is to cultivate an intellectual domain where current logistics trends are transformed into scientific problems, testable questions, methodologically sound research designs, and cumulative contributions to the field of logistics science.

7. The Academic Journal as an Institutional Mechanism for Field Development

Scientific progress is driven not only by the emergence of new research findings, but also by the presence of institutions capable of facilitating their critical reflection, integration, and continuous development. Traditionally, the academic journal has served as one such core institution. However, amid the rapid growth of scientific information, deepening interdisciplinarity, and the globalization of scholarly communication, its role is shifting significantly.

In the context of establishing the field of logistics intellectualization, a journal can fulfill five interconnected functions:

– Representative function. Ensures the quality of academic communication, rigorous double-blind peer review, and the international visibility of research findings.

– Integrative function. Unites diverse disciplines, methodologies, and research traditions.

– Concept-forming function. Supports publications that construct new concepts, models, typologies, and theoretical propositions.

– Foresight function. Identifies emerging research problems, organizes special issues, and shapes the Research Agenda.

– Platform function. Builds an open intellectual ecosystem that connects authors, reviewers, editors, early-career researchers, practitioners, and international partners.

The influence of an academic journal on the development of a research field extends beyond selecting and disseminating individual papers. Through editorial policy, peer review standards, special thematic issues, support for conceptual papers, research agenda setting, and the expansion of academic networks, the journal shapes which types of scientific contribution gain recognition, which questions become subjects of future research, and how a shared scientific language is formulated. The generalized mechanism of this impact is illustrated in Figure 4.

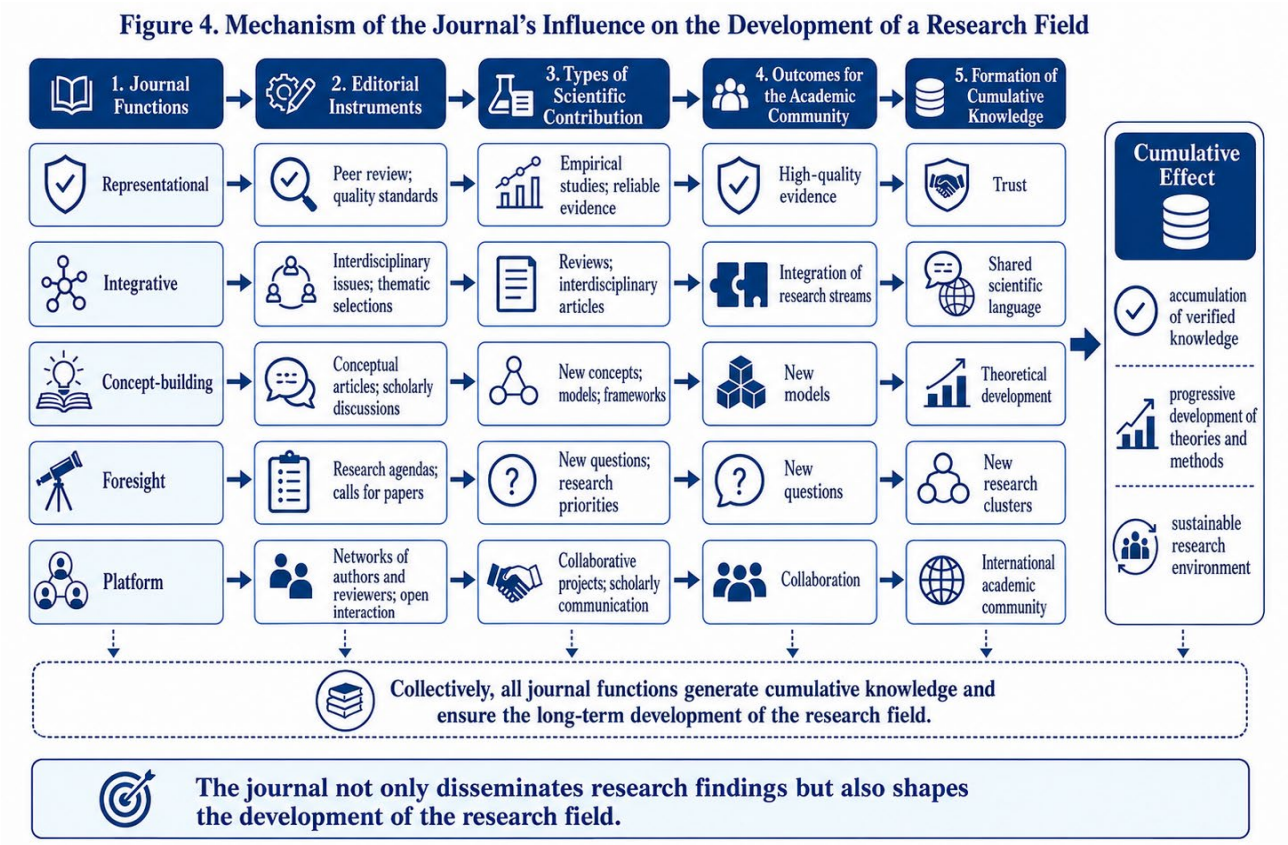


Figure 4 – Mechanism of the Journal`s influence on the development of a research field
Source: developed by the author.

As shown in Figure 4, each function of the journal is operationalized through a specific set of editorial instruments and fosters corresponding types of scientific contribution. The representative function, enforced via peer review and quality standards, supports the generation of reliable empirical evidence and reinforces trust in published findings. The integrative function, executed through interdisciplinary issues, thematic collections, and review papers, facilitates the convergence of research streams and the formulation of a shared scientific language. The concept-forming function creates space for novel concepts, models, and theoretical frameworks, whereas the foresight function translates emerging problems into new research questions, priorities, and thematic clusters. The platform function enables interaction among authors, reviewers, and institutions, sustaining collaborative projects, professional communication, and the growth of the international academic community.

The interplay of these functions yields not a mere sum of discrete publications, but the gradual accumulation of knowledge. Cumulative knowledge arises when new studies build upon prior findings, refine concepts, test models, compare methodologies, and uncover new research questions. Within this logic, the journal operates not merely as a channel of academic communication, but as an institutional mechanism supporting the consistent advancement of theory, methodology, and the research community.

At the same time, the presented diagram is conceptual rather than empirically proven. It depicts a hypothesized mechanism of journal impact that warrants further validation through the analysis of publication thematic structures, citation patterns, interdisciplinary linkages, co-authorship networks, and the emergence of new

research clusters. This provides grounds to treat the institutional role of the journal as a distinct avenue for future inquiry, rather than an established fact.

Thus, the journal's functions, editorial instruments, and supported types of scientific contribution constitute an interconnected institutional loop. Its performance is measured not by the volume of published material, but by the publication's capacity to ensure evidence quality, knowledge integration, concept development, question generation, and the sustainability of academic engagement.

The institutional proposition of this article asserts that an academic journal influences the development of a research field not only through manuscript selection, but also by defining the admissible types of scientific contribution, interdisciplinary linkages, and open research questions. This proposition belongs not to the operational theory of logistics systems, but to the domain of academic field institutionalization. It can be tested through the analysis of publication thematic structures, the proportion of conceptual and methodological papers, citation interdisciplinarity, co-authorship networks, special thematic issues, and the volume of articles building upon the published Research Agenda.

Editorial instruments for implementing these functions may include special issues, invited conceptual papers, perspective papers, methodological debates, literature reviews with explicitly defined research gaps, methodological transparency requirements, open data support where feasible, the publication of research agendas, and the encouragement of interdisciplinary peer review. Such instruments enable the journal to shape not only publication topics, but also the types of scientific contribution recognized as meaningful for field advancement.

The role of the journal is appropriately framed not around a "quality pyramid," but across distinct levels of abstraction in scientific contribution. Empirical evidence provides the factual foundation; methods and tools enhance research reproducibility; models explain underlying mechanisms; concepts and frameworks refine scientific terminology; and theories alongside research programs shape the long-term agenda. None of these levels is inherently "superior" in quality: theoretical generalizations require validation, while empirical findings derive scientific weight through validity, transparency, and cumulative integration into broader scholarly discourse.

The anticipated outcomes of this institutional role encompass not simply an increase in publication output, but an enhancement in evidence quality, the development of a shared research language, the emergence of novel conceptual frameworks, the strengthening of international research networks, and the accumulation of knowledge in the field of logistics intellectualization. In this process, open science acts not as a decorative principle, but as a prerequisite for trust – safeguarding methodological transparency, responsible data usage, ethical peer review, and the verifiability of research results.

8. Discussion

The proposed framework holds merit only if it explains more than existing concepts of digital transformation in logistics. Compared to Logistics 4.0, its explanatory advantage lies not in an expanded roster of technologies, but in a distinct research query. Logistics 4.0 primarily addresses how digital, cyber-physical, platform, and analytical solutions reconfigure operations, processes, and supply chain integration [1-6; 11-18]. Intellectualization, by contrast, asks under what conditions these solutions are converted into a system's capacity to learn, coordinate, adapt, and make responsible decisions. Therefore, a digital twin, a predictive algorithm, or a data-sharing platform does not in itself constitute evidence of intellectualization. These tools become elements of intellectualization only when

embedded within mechanisms of knowledge creation, organizational learning, human oversight, inter-organizational trust, and feedback loops.

Compared to Logistics 5.0, the proposed framework clarifies the precise interaction among human-centricity, sustainability, technological advancement, and adaptability. Logistics 5.0 importantly shifts focus from purely technocratic automation toward human agency, social responsibility, and sustainable development [19-25]. However, human-centricity alone does not fully explain how human expertise interacts with organizational memory, algorithmic models, and the collective knowledge of the network. The intellectualization framework introduces a mechanistic explanation to this relationship: human intelligence does not merely "remain at the center," but fulfills functions of interpretation, critical oversight, contextualization of algorithmic recommendations, and accountable decision-making under uncertainty. In this sense, intellectualization does not compete with Logistics 5.0, but provides a more precise language for describing the hybrid intelligence of logistics systems.

The relationship between intellectualization and knowledge-based supply chain management warrants distinct delineation. Knowledge-based supply chain management has long emphasized the value of knowledge, competencies, learning, and inter-organizational experience sharing [27; 36-38]. The intellectualization framework does not refute this tradition, but extends it along at least three vectors. First, knowledge is viewed not merely as an organizational or network resource, but as an emergent property resulting from the interaction of human, organizational, inter-organizational, and artificial forms of intelligence. Second, the focus expands beyond knowledge accumulation to encompass its algorithmic representation, automated updating, explainability, and governance. Third, knowledge is linked to the evolutionary adaptation of the system: the critical metric becomes not the mere existence of a knowledge base or skill set, but the system's capacity to modify its behavioral rules in response to disruptions, errors, and novel environmental signals.

Regarding complex adaptive systems (CAS) theory, the proposed framework occupies an intermediate position between a general system metaphor and an operationalized model of logistics transformation. CAS theory effectively explains self-organization, non-linearity, emergence, and co-evolution, yet often remains at a high level of abstraction. Intellectualization operationalizes these concepts for logistics through sources of intelligence, integration mechanisms, five transformation dimensions, and systemic outcomes. Its contribution lies not in replacing complexity theory, but in demonstrating which specific socio-technical mechanisms can convert localized actor decisions, digital signals, algorithmic recommendations, and organizational experience into adaptive supply chain or ecosystem capabilities.

The most debatable proposition within the framework is the complementarity of dimensions. It posits that a high level of technological development cannot compensate for deficiencies in organizational learning, trust, or human oversight. This is a strong, non-trivial proposition. In certain contexts, the technological dimension may indeed exert a dominant influence – such as in standardized operations with high data quality and low environmental uncertainty. In other contexts – particularly during crises, wartime disruptions, information scarcity, or interactions among autonomous actors – technological superiority can be neutralized by a lack of coordination and trust. Thus, complementarity should be treated not as an axiom, but as a hypothesis sensitive to the type of logistics system, the level of uncertainty, and the nature of actor interdependence.

The proposition regarding the mediated impact of artificial intelligence is similarly open to debate. The proposed framework assumes that AI does not directly generate adaptability, but acts through data quality, organizational learning, and human oversight. An alternative explanation holds that in specific operational tasks, algorithmic optimization can improve outcomes independently of deep organizational transformation. For example, more accurate demand forecasting or route optimization can yield immediate, function-level gains. However, such localized gains do not constitute systemic intellectualization unless the organization can explain the underlying decisions, update operational rules, transfer knowledge across actors, or prevent error scaling. This represents the boundary between an effective digital tool and the evolution of an intelligent logistics system as an analytical construct.

Alternative explanations also exist for the phenomena attributed here to intellectualization. Enhanced resilience may stem not from collective intelligence, but from redundant inventory, supplier diversification, regulatory mandates, or financial reserve accumulation. Improved decision quality may result from centralized governance, procedure standardization, or third-party technology adoption rather than intelligence source integration. Increases in sustainability may be driven by normative constraints, market pressures, or customer requirements rather than intellectualization. Acknowledging these alternatives prevents intellectualization from becoming a catch-all explanation for any positive performance outcome. Future empirical studies must explicitly compare these competing mechanisms rather than simply confirming the ideal logic of the proposed model.

For these reasons, the core tenets of the model are formulated to be falsifiable:

– The complementarity of dimensions proposition can be refuted if empirical evidence demonstrates that a single dominant dimension (e.g., technological) consistently explains system adaptability better than a balanced profile across dimensions.

– The mediated impact of AI proposition can be challenged if direct effects of algorithmic solutions on adaptability persist after controlling for data quality, organizational learning, and human oversight.

– The emergent nature of resilience proposition will be weakened if resilience proves to be primarily a function of structural redundancy or contractual mechanisms rather than the interaction of technological, social, and organizational capabilities.

– The distributed intelligence integration proposition will require revision if empirical findings reveal that sources of intelligence impact outcomes independently, without significant mediation by coordination, learning, or feedback loops.

A critical corollary of this discussion is the distinction between digitalization and intellectualization. Digitalization fails to transition into intellectualization when data remains fragmented, inaccurate, or inaccessible to key stakeholders; when algorithms remain opaque and unsubjected to meaningful human oversight; when digital platforms deepen actor dependence instead of fostering reciprocal coordination; when an organization automates outdated or flawed procedures; when technology implementation is uncoupled from personnel learning and decision-rule updating; or when local optimization of a single function compromises overall supply chain performance. In such instances, a system may become more digital, but it does not become more intelligent.

Ultimately, the value of the proposed framework lies not in declaring a new milestone in logistics evolution, but in formulating a testable research problem: which combinations of intelligence sources, integration mechanisms, organizational conditions, and socio-technical constraints

generate true adaptive capabilities in logistics systems? Its theoretical contribution consists in explaining the transition from technological sophistication to systemic capacity for learning and adaptation. Its methodological contribution lies in shifting the unit of analysis toward the network and socio-technical ecosystem. Its institutional contribution rests on positioning the journal not merely to reflect an established field, but to provide a venue for its critical validation, refinement, and expansion. Critical falsifiability – rather than rhetorical appeal – must determine the enduring scholarly viability of the logistics intellectualization concept.

9. Conclusion and Directions for Future Research.

This article has established the utility of conceptualizing the intellectualization of logistics and supply chain management as an integrative conceptual framework and an open research agenda. The primary outputs include narrowing and refining the problem domain, systematizing core streams in contemporary logistics research, identifying the integrative gap among them, articulating a methodology for conceptual synthesis, delineating key analytical categories, constructing a mechanistic-process model of intellectualization, formulating four theoretical propositions, specifying a distinct methodological proposition on the unit of analysis, identifying boundary conditions and risks, constructing a Research Agenda, and detailing an institutional proposition regarding the role of the academic journal.

The scientific contribution of this paper rests on framing logistics intellectualization not as a technological trend, but as a systemic process through which logistics systems develop capabilities for learning, coordination, adaptation, self-organization, and decision-making. The proposed model explains how human intelligence, organizational memory and learning capacity, inter-organizational collective intelligence, and artificial intelligence – mediated by knowledge sharing, coordination, organizational learning, and human oversight of algorithmic decisions – are converted into adaptive capabilities across cognitive, technological, organizational, social, and evolutionary dimensions. The theoretical propositions translate this conceptual logic into testable relationships, the methodological proposition clarifies the appropriate scale of analysis, and the institutional proposition highlights the role of the journal in driving field development.

Future research should focus on operationalizing the dimensions of intellectualization, developing measurement scales and indicators, empirically testing the impact of AI on adaptability and resilience, investigating hybrid intelligence in logistics decision-making, examining digital trust in decentralized ecosystems, and conducting comparative analyses across units of analysis: process, enterprise, supply chain, network, and socio-technical ecosystem. Negative scenarios of intellectualization require dedicated empirical inquiry: algorithmic opacity, cyber risks, technology vendor lock-in, erosion of human expertise, localized optimization at system expense, and the environmental footprint of digital infrastructure. A final avenue for future investigation concerns academic communication itself: evaluating how editorial policies, open data practices, special thematic issues, and conceptual papers shape the emergence and institutionalization of new research fields.

Accordingly, this article does not claim to conclude the debate. Its objective is to establish a methodologically grounded framework suitable for critical discourse, refinement, operationalization, and empirical testing in future studies. This aligns with the purpose of a foundational conceptual paper and the editorial mission of the journal Intellectualization of Logistics and Supply Chain Management.

References

1. Baryannis G., Validi S., Dani S. та ін. Supply chain risk management and artificial intelligence: state of the art and future research directions. International Journal of Production Research. 2019. Vol. 57. No. 7. P. 2179-2202. DOI: https://doi.org/10.1080/00207543.2018.1530476

2. Seyedghorban Z., Tahernejad H., Meriton R. та ін. Supply chain digitalization: past, present and future. Production Planning & Control. 2020. Vol. 31. No. 2-3. P. 96-114. DOI: https://doi.org/10.1080/09537287.2019.1631461

3. Queiroz M. M., Pereira S. C. F., Telles R. та ін. Industry 4.0 and digital supply chain capabilities. Benchmarking: An International Journal. 2021. Vol. 28. No. 5. P. 1761-1782. DOI: https://doi.org/10.1108/bij-12-2018-0435

4. Frederico G. F., Garza-Reyes J. A., Anosike A. та ін. Supply Chain 4.0: concepts, maturity and research agenda. Supply Chain Management: An International Journal. 2019. Vol. 25. No. 2. P. 262-282. DOI: https://doi.org/10.1108/scm-09-2018-0339

5. Toorajipour R., Sohrabpour V., Nazarpour A. та ін. Artificial intelligence in supply chain management: A systematic literature review. Journal of Business Research. 2021. Vol. 122. P. 502-517. DOI: https://doi.org/10.1016/j.jbusres.2020.09.009

6. Riahi Y., Saikouk T., Gunasekaran A. та ін. Artificial intelligence applications in supply chain: A descriptive bibliometric analysis and future research directions. Expert Systems with Applications. 2021. Vol. 173. P. 114702. DOI: https://doi.org/10.1016/j.eswa.2021.114702

7. Modgil S., Singh R. K., Hannibal C. Artificial intelligence for supply chain resilience: learning from Covid-19. The International Journal of Logistics Management. 2022. Vol. 33. No. 4. P. 1246-1268. DOI: https://doi.org/10.1108/ijlm-02-2021-0094

8. Modgil S., Gupta S., Stekelorum R. та ін. AI technologies and their impact on supply chain resilience during COVID-19. International Journal of Physical Distribution & Logistics Management. 2022. Vol. 52. No. 2. P. 130-149. DOI: https://doi.org/10.1108/ijpdlm-12-2020-0434

9. Belhadi A., Mani V., Kamble S. S. та ін. Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: an empirical investigation. Annals of Operations Research. 2024. Vol. 333. No. 2-3. P. 627-652. DOI: https://doi.org/10.1007/s10479-021-03956-x

10. Ferreira A. C. A., Francisco M. B., Pinho A. F. D. The Use of Artificial Intelligence in Supply Chain Management: Systematic Literature Review and Future Research Directions. IEEE Access. 2025. Vol. 13. P. 157828-157841. DOI: https://doi.org/10.1109/access.2025.3603866

11. Le T. V., Fan R. Digital twins for logistics and supply chain systems: Literature review, conceptual framework, research potential, and practical challenges. Computers & Industrial Engineering. 2024. Vol. 187. P. 109768. DOI: https://doi.org/10.1016/j.cie.2023.109768

12. Ivanov D. Intelligent digital twin (iDT) for supply chain stress-testing, resilience, and viability. International Journal of Production Economics. 2023. Vol. 263. P. 108938. DOI: https://doi.org/10.1016/j.ijpe.2023.108938

13. Ivanov D. Conceptualisation of a 7-element digital twin framework in supply chain and operations management. International Journal of Production Research. 2024. Vol. 62. No. 6. P. 2220-2232. DOI: https://doi.org/10.1080/00207543.2023.2217291

14. Zhu Y., Cheng J., Liu Z. та ін. Production logistics digital twins: Research profiling, application, challenges and opportunities. Robotics and Computer-Integrated Manufacturing. 2023. Vol. 84. P. 102592. DOI: https://doi.org/10.1016/j.rcim.2023.102592

15. Liu Y., Pan S., Ballot E. Unveiling the potential of digital twins in logistics and supply chain management: Services, capabilities, and research opportunities. Digital Engineering. 2024. Vol. 3. P. 100025. DOI: https://doi.org/10.1016/j.dte.2024.100025

16. Kapil D., Raut R., Nayal K. та ін. A multisectoral systematic literature review of digital twins in supply chain management. Benchmarking: An International Journal. 2025. Vol. 32. No. 10. P. 3793-3824. DOI: https://doi.org/10.1108/bij-04-2024-0286

17. Zaidi S. A. H., Khan S. A., Chaabane A. Unlocking the potential of digital twins in supply chains: A systematic review. Supply Chain Analytics. 2024. Vol. 7. P. 100075. DOI: https://doi.org/10.1016/j.sca.2024.100075

18. Jesus V., Kalaitzi D., Batista L. та ін. Digital Twins of Supply Chains: A Systems Approach. IEEE Transactions on Engineering Management. 2024. Vol. 71. P. 14915-14932. DOI: https://doi.org/10.1109/tem.2024.3468177

19. Spieske A., Birkel H. Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. Computers & Industrial Engineering. 2021. Vol. 158. P. 107452. DOI: https://doi.org/10.1016/j.cie.2021.107452

20. Rahman T., Paul S. K., Shukla N. та ін. Supply chain resilience initiatives and strategies: A systematic review. Computers & Industrial Engineering. 2022. Vol. 170. P. 108317. DOI: https://doi.org/10.1016/j.cie.2022.108317

21. Roshani A., Walker-Davies P., Parry G. Designing resilient supply chain networks: a systematic literature review of mitigation strategies. Annals of Operations Research. 2024. Vol. 341. No. 2-3. P. 1267-1332. DOI: https://doi.org/10.1007/s10479-024-06228-6

22. Ivanov D., Dolgui A. Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak. International Journal of Production Research. 2020. Vol. 58. No. 10. P. 2904-2915. DOI: https://doi.org/10.1080/00207543.2020.1750727

23. Ivanov D. Supply Chain Viability and the COVID-19 pandemic: a conceptual and formal generalisation of four major adaptation strategies. International Journal of Production Research. 2021. Vol. 59. No. 12. P. 3535-3552. DOI: https://doi.org/10.1080/00207543.2021.1890852

24. Ruel S., El Baz J., Ivanov D. та ін. Supply chain viability: conceptualization, measurement, and nomological validation. Annals of Operations Research. 2024. Vol. 335. No. 3. P. 1107-1136. DOI: https://doi.org/10.1007/s10479-021-03974-9

25. Ivanov D., Dolgui A. OR-methods for coping with the ripple effect in supply chains during COVID-19 pandemic: Managerial insights and research implications. International Journal of Production Economics. 2021. Vol. 232. P. 107921. DOI: https://doi.org/10.1016/j.ijpe.2020.107921

26. Farooque M., Zhang A., Thürer M. та ін. Circular supply chain management: A definition and structured literature review. Journal of Cleaner Production. 2019. Vol. 228. P. 882-900. DOI: https://doi.org/10.1016/j.jclepro.2019.04.303

27. Hazen B. T., Russo I., Confente I. та ін. Supply chain management for circular economy: conceptual framework and research agenda. The International Journal of Logistics Management. 2021. Vol. 32. No. 2. P. 510-537. DOI: https://doi.org/10.1108/ijlm-12-2019-0332

28. Bag S., Pretorius J. H. C. Relationships between industry 4.0, sustainable manufacturing and circular economy: proposal of a research framework. International Journal of Organizational Analysis. 2022. Vol. 30. No. 4. P. 864-898. DOI: https://doi.org/10.1108/ijoa-04-2020-2120

29. Massari G. F., Nacchiero R., Giannoccaro I. Digital technologies for resource loop redesign in circular supply chains: A systematic literature review. Resources, Conservation & Recycling Advances. 2023. Vol. 20. P. 200189. DOI: https://doi.org/10.1016/j.rcradv.2023.200189

30. Agrawal R., Surendra Yadav V., Majumdar A. та ін. Opportunities for disruptive digital technologies to ensure circularity in supply Chain: A critical review of drivers, barriers and challenges. Computers & Industrial Engineering. 2023. Vol. 178. P. 109140. DOI: https://doi.org/10.1016/j.cie.2023.109140

31. Sahu A., Agrawal S., Kumar G. Integrating Industry 4.0 and circular economy: a review. Journal of Enterprise Information Management. 2022. Vol. 35. No. 3. P. 885-917. DOI: https://doi.org/10.1108/jeim-11-2020-0465

32. Kashav V., Garg C. P. Fortifying humanitarian supply chains: evaluating sustainability enablers for strengthened resilience of humanitarian supply chains during calamities and pandemics. Journal of Humanitarian Logistics and Supply Chain Management. 2025. Vol. 15. No. 3. P. 294-308. DOI: https://doi.org/10.1108/jhlscm-04-2024-0050

33. Ahatsi E., Olanrewaju O. A. Enhancing Humanitarian Supply Chain Resilience: Evaluating Artificial Intelligence and Big Data Analytics in Two Nations. Logistics. 2025. Vol. 9. No. 2. P. 64. DOI: https://doi.org/10.3390/logistics9020064

34. Rinaldi M., Caterino M., Riemma S. та ін. Emergency Supply Chain Resilience Enhanced Through Blockchain and Digital Twin Technology. Logistics. 2025. Vol. 9. No. 1. P. 43. DOI: https://doi.org/10.3390/logistics9010043

35. Dubey R., Gunasekaran A., Bryde D. J. та ін. Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. International Journal of Production Research. 2020. Vol. 58. No. 11. P. 3381-3398. DOI: https://doi.org/10.1080/00207543.2020.1722860

36. Gruner R. L., Power D. Conceptual wanderlust: How to develop creative supply chain theory with analogies. Journal of Supply Chain Management. 2023. Vol. 59. No. 4. P. 3-21. DOI: https://doi.org/10.1111/jscm.12305

37. Stephens V., Matthews L., Cornelissen J. P. та ін. Building Novel Supply Chain Theory Using "Metaphorical Imagination". Journal of Supply Chain Management. 2022. Vol. 58. No. 1. P. 124-139. DOI: https://doi.org/10.1111/jscm.12257

38. Pagell M., Wilhelm M. Putting the S in Sustainable Supply Chain Management: A People-Centric Research Agenda. Journal of Supply Chain Management. 2025. Vol. 61. No. 1. P. 83-95. DOI: https://doi.org/10.1111/jscm.12337

39. Pal T., Ganguly K., Chaudhuri A. Digitalisation in food supply chains to build resilience from disruptive events: a combined dynamic capabilities and knowledge-based view. Supply Chain Management: An International Journal. 2024. Vol. 29. No. 6. P. 1042-1062. DOI: https://doi.org/10.1108/scm-02-2024-0108

40. Hautala-Kankaanpää T. The impact of digitalization on firm performance: examining the role of digital culture and the effect of supply chain capability. Business Process Management Journal. 2022. Vol. 28. No. 8. P. 90-109. DOI: https://doi.org/10.1108/bpmj-03-2022-0122

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

36-43
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-2

UDC 005.73:339.9
JEL Classification: M14, M16, O33, F51.

Received: 2026-07-05
Accepted: 2026-08-13
Published: 2026-08-30

Gurina G.S. Academician of the Academy of Sciences of Ukraine, Doctor of Economics Science, Professor, Vice Rector of Kyiv University of Law of the NAS of Ukraine (Ukraine)

ORCID – 0000-0002-1419-4956
Researcher ID
Scopus author id: –
E-Mail: gurina_gs@ukr.net

Podrieza S.M. Academician of the Academy of Sciences of Ukraine, Doctor of Economics Science, Professor (Ukraine)

ORCID – 0000-0003-2396-9570
Researcher ID –
Scopus author id: –
E-Mail: sergey.m410@gmail.com

Podrieza M.S. Doctor of Philosophy in Economics State University «Kyiv Aviation Institute» (Ukraine)

ORCID – 0009-0002-6977-6790
Researcher ID –
Scopus author id: –
E-Mail: mishpodr@gmail.com

TRANSFORMATION OF ORGANIZATIONAL CULTURE AND MANAGEMENT MODELS IN INTERNATIONAL BUSINESS UNDER THE INFLUENCE OF INNOVATION AND GEOPOLITICAL CHANGES

Gurina Ganna, Podrieza Serhii, Podrieza Mykhailo. «Transformation of organizational culture and management models in international business under the influence of innovation and geopolitical changes». *The study focuses on the evolution of corporate governance and the internal organizational environment under the pressure of global turbulence. The article demonstrates that attempts to reshape organizational culture through top-down or directive approaches are ineffective; instead, the key driver of success lies in a shared understanding of change across the entire team and flexible alignment with stakeholder demands.*

Special emphasis is placed on the practical experience of Ukrainian businesses operating under martial law. Shelling, destruction of critical logistics, and the loss of production assets force companies to immediately abandon obsolete operational models in favor of searching for non-standard business solutions. It is

36-43
v.38 (2026)
https://smart-scm.org

substantiated that a culture built on trust and decentralization serves as the primary mechanism for maintaining operations and preserving human capital under extreme force majeure.

The paper concludes that the extraordinary resilience developed by Ukrainian enterprises establishes new benchmarks for international management and opens up avenues for integrating domestic companies into global markets.

***Keywords**:* organizational culture, transformation of management models, anti-crisis management, adaptive management, corporate governance, war risks for business, relocation of enterprises, security factor, organizational viability, sustainability, business adaptability, human capital, stress resistance of organizations, decentralization, international business, geopolitical shocks, innovative business models, cross-cultural management, supply chains, interaction with stakeholders, competitiveness

Ганна Гуріна, Сергій Подрєза, Михайло Подрєза. «Трансформація організаційної культури та управлінських моделей у міжнародному бізнесі під впливом інновацій та геополітичних змін». *Дослідження присвячено проблемам еволюції корпоративного управління та внутрішньоорганізаційного середовища під тиском викликів глобальної турбулентності. У статті доведено, що спроби реформувати організаційну культуру за допомогою силового чи директивного тиску є неефективними; замість цього ключовим чинником успіху є спільне усвідомлення змін усім колективом та гнучке реагування на запити стейкхолдерів.*

Особливу увагу приділено практичному досвіду функціонування українського бізнесу в умовах воєнного стану. Обстріли, руйнування критичної логістики та втрата виробничих об'єктів змушують компанії негайно відмовлятися від застарілих управлінських схем на користь пошуку нестандартних бізнес-моделей. Обґрунтовано, що саме культура, заснована на децентралізації та довірі, виступає головним інструментом збереження операційної діяльності та людського ресурсу в умовах форс-мажору.

Зроблено висновок, що набута українськими підприємствами екстремальна життєздатність створює нові орієнтири для міжнародного менеджменту та відкриває шляхи для інтеграції вітчизняних компаній у світові ринки.

Ключові слова: організаційна культура, трансформація управлінських моделей, антикризове управління, адаптивне управління, корпоративне управління, воєнні ризики для бізнесу, релокація підприємств, безпековий чинник, організаційна життєздатність, стійкість, бізнес-адаптивність, людський капітал, стресостійкість організацій, децентралізація, міжнародний бізнес, геополітичні шоки, інноваційні бізнес-моделі, крос-культурний менеджмент, ланцюги постачання, взаємодія зі стейкхолдерами, конкурентоспроможність

Introduction. Modern enterprises are forced to operate under conditions of extreme geopolitical and economic turbulence, requiring high controllability and adaptability of all internal systems under pressure from external stakeholders. Organizational culture is a complex, "living" organism that does not yield to directive, imperative, or authoritarian administration methods. Building an effective mechanism for its transformation is possible only under the condition of a high level of philosophical maturity and mutual understanding from both leadership and staff. In turn, the process of reforming corporate culture is continuous and serves as a synchronous response of the internal environment to adopted management decisions, where the ultimate goal is achieving a balance between its stability (strength) and flexibility.

In the unique realities of modern Ukraine, this process assumes critical importance. Amid full-scale war, when domestic business suffers direct physical destruction from

36-43
v.38 (2026)
https://smart-scm.org

enemy shelling, and entire logistics hubs and manufacturing capacities are destroyed in an instant, traditional operating models completely lose their efficacy. Under such conditions, a deep transformation of organizational culture becomes not merely a matter of development, but a strategic imperative for survival. It must foster within the team high stress resistance, decentralization in decision-making, and a readiness for the immediate search for fundamentally new business solutions, alternative routes, and flexible operating models.

Thus, the rapid adaptation of corporate culture enables enterprises not only to promptly restore destroyed supply chains, but also to reconfigure internal communications to preserve human capital under conditions of constant danger. It is precisely a culture built on trust, mutual support, and a high level of employee autonomy that allows Ukrainian companies to maintain operational efficiency even during prolonged blackouts or forced relocation. Furthermore, this wartime experience forms a unique type of organizational viability that becomes an important competitive advantage in the international arena. Global business is increasingly adopting Ukrainian crisis management case studies, where the innovativeness of solutions stems not from planned budgets, but from team agility and cohesion. Ultimately, the capacity of organizational culture for rapid self-organization under the influence of extreme external factors transforms critical risks into new opportunities for scaling and expanding into new markets.

Literature review. Ensuring the adaptability and effectiveness of crisis management under martial law relies on the principles outlined in the works of L. Lihonenko and I. Myahkykh [4], which establish that traditional authoritarian (rigid) management methods lose their efficacy during localized critical shocks, such as shelling and physical infrastructure destruction. This reality demands the implementation of flexible mechanisms, decision-making decentralization, and the capacity for rapid self-organization. International research on this issue seamlessly complements domestic academic contributions through the lenses of European and American scholarly traditions.

Specifically, the European management vector focuses on a multi-stakeholder approach, cross-cultural environments, and supply chain resilience. The impact of national and corporate cultural dimensions on organizational behavior amid emerging geopolitical threats is analyzed through the frameworks of G. Hofstede [8] and J. Aarestrup [5]. Furthermore, supply chain resilience under external shocks is explored in the works of S. Seuring and M. Christopher [6], who demonstrate that a firm's capability to rapidly reorganize destroyed logistics hubs depends not only on physical resources but also on the agility of its organizational culture and partner relationships—a view that aligns with F. Ducrot's [7] research on the significance of ethical leadership and synchronizing corporate actions with societal demands during crises.

Concurrently, the American school sets methodological benchmarks for analyzing innovative business models, the VUCA/BANI environment, and organizational resilience. E. Schein's [11] foundational model explains the underlying reasons why cultural transformation cannot be achieved through directive top-down methods. G. P. Pisano [9] substantiates the necessity of balancing creative freedom with rigorous execution discipline to foster crisis-driven innovations. Finally, the conceptual foundations of strategic adaptation proposed by M. E. Porter, alongside N. N. Taleb's [13] concept of "antifragility," demonstrate how extreme external shocks and "black swans" can serve as catalysts not merely for survival, but for the qualitative development of business entities through deep internal transformation.

Despite a significant body of scientific work, most foreign studies consider geopolitical risks and changes in organizational culture in relatively stable or moderately crisis conditions (for example, during economic recessions or the COVID-19 pandemic). At the same time, the specifics of corporate culture transformation and the search for non-standard business solutions in conditions of direct military operations, physical destruction of logistics hubs and infrastructure in Ukraine remain insufficiently conceptualized in the context of international business and require further in-depth analysis.

Purpose and objectives. The main purpose of this study is to conceptualize the mechanisms of transforming organizational culture and management models in international business amidst global geopolitical turbulence and the extreme operational conditions of martial law in Ukraine. To achieve this overarching aim, the study addresses several interconnected research objectives. First, it seeks to analyze the theoretical foundations of organizational culture adaptability and evaluate the limitations of directive, top-down management styles under crisis conditions. Second, the paper aims to examine the impact of severe external shocks - specifically military actions, shelling, and the physical destruction of critical logistics hubs - on the continuity of business operations. Third, it investigates the strategic role of organizational resilience in enabling rapid decision-making decentralization and the preservation of human capital. Fourth, the study explores the integration of innovative business models and supply chain reconfiguration strategies as adaptive responses to geopolitical risks. Fifth, it evaluates the alignment of corporate actions with multi-stakeholder interests, ethical leadership, and societal expectations during crisis periods. Sixth, the research assesses cross-cultural management approaches within multinational enterprises adapting to fragmented global markets. Seventh, it aims to synthesize the unique empirical experience of Ukrainian businesses operating under martial law to formulate best practices for global management. Finally, the study intends to outline actionable recommendations for corporate leaders seeking to transform organizational vulnerability into long-term strategic agility and competitive advantage.

Results, analysis, and discussion. Organizational culture at the current stage of functioning of modern organizations is subject to significant influences and transformations. This is due to the adaptive response of its elements to changes in the external and internal environment. New social, economic trends and complications of the social paradigm of interaction between various institutions require further scientific research in the direction of monitoring exogenous influences and modeling appropriate management steps and processes of organizational culture changes.

Currently, the leaders of most companies understand the importance of developing organizational culture, but many of them cannot build an effective model for its formation. This is due, first of all, to the lack of understanding by management of the need for further development of organizational culture; the lack of personnel with digital skills and knowledge; the lack of customer orientation among managers; insufficient cohesion of the team to achieve the strategic goals of the company. Therefore, in modern business conditions, the problems of developing organizational culture of enterprises, taking into account their industry specifics, are becoming increasingly relevant. Successful transformation of Ukrainian business in the context of global challenges requires a systemic approach to the selection and implementation of management tools, a balance between innovation and stability, the development of competence and organizational culture, flexibility and adaptability to change, as well as a focus on

creating long-term value for all stakeholders. Such transformation will allow Ukrainian business not only to survive in difficult conditions, but also to create a reliable foundation for future sustainable development and increased competitiveness in the world market. At the same time, a critical factor in success is the organization's ability to learn and adapt faster than changes in the external environment.

It should be noted that the external environment, represented by macroeconomic trends, legislative norms, technological innovations and changing consumer preferences, creates the context in which an organization operates. Adaptation to these changes is a key factor in survival and development. Internal factors, such as: quality of management, corporate culture, innovation potential and efficiency of business processes, determine the internal stability of the organization and its ability to respond to external challenges. The combination of these factors forms the profile of the organization and affects its development trajectory. Analysis of internal and external factors allows you to identify potential risks and opportunities that arise at different stages of development. Thanks to this, management can take proactive measures in a timely manner aimed at optimizing business processes, increasing competitiveness and ensuring the long-term success of the enterprise.

Analysis of practical experience of enterprises functioning in conditions of extreme turbulence shows that the preservation of operational activity directly depends on the speed of transformation of intra-organizational processes. The study revealed that the physical destruction of production facilities and the interruption of logistics chains force businesses to switch from long-term planning to a system of operational anti-crisis response. The key factor of stability is the decentralization of management functions, which provides autonomy to regional divisions and line teams to make instant decisions on the spot. The results of the analysis show that the implementation of flexible schedules, digital platforms for coordination and cross-functional interaction allows maintaining high productivity even in the event of power outages or personnel relocation. A special role is played by the reformatting of corporate values towards horizontal trust, mutual assistance and employee safety, which is the main factor in retaining human capital. Discussion of the obtained results confirms that attempts to apply directive pressure in conditions of crises only deepen disorganization and reduce the motivation of the team. Instead, stakeholder focus and ethical leadership create a solid foundation for rapid restructuring of logistics hubs and the search for new market niches. The experience acquired by domestic companies in adapting to extreme security risks forms a new model of anti-crisis management, which turns forced flexibility into a long-term competitive advantage in international business [3]. The process flow illustrates the step-by-step evolution (fig.1) from an initial external shock (extreme security risks) to the establishment of an advanced management system. Forced agility (organizational resilience) serves as the core transformational bridge, leveraging decentralization and corporate culture shifts to turn martial law challenges into strategic assets for international market expansion.

Figure 1 – Conceptual model of transforming security risks into competitive advantage
Source: compiled by the authors.

Further recovery and development of the industry require continued stimulation of development and production in the Defense Tech sector, support for industrial processing, modernization of capacities, and promotion of exports, primarily in non-raw material activities. In addition, during the implementation of these and other important initiatives, it is necessary to review and update the principles of the organizational culture of industrial policy, which should create an institutional basis for industrial development based on the introduction of mechanisms and tools for both adapting the manufacturing sector to changes and needs of wartime and accelerating structural shifts in the conditions of war and post-war recovery.

Since the beginning of the full-scale russian invasion of Ukraine, the industry has suffered significant losses and destruction of assets, production, distribution, and logistics chains. According to the Rapid Assessment of Losses and Needs of Ukraine (RDNA4), total losses in the industry as of the end of 2025 amount to 18.7 billion USD. In total, since the beginning of the war, the assets of more than half a thousand large, medium-sized private and state-owned enterprises, as well as tens of thousands of small private enterprises, have been damaged or destroyed. [9]

Modernizing the organizational culture of industrial policy necessitates a fundamental shift from reactive crisis management toward proactive institutional stewardship. This transformation requires creating transparent, low-friction regulatory frameworks that dramatically accelerate the commercialization of dual-use technologies and Defense Tech innovations. By embedding agile governance principles into state institutions, decision-makers can shorten the feedback loop between battlefield feedback and military-industrial manufacturing. Furthermore, fostering public-private partnerships will prove crucial for attracting venture capital into advanced processing sectors, thereby moving the national economy away from raw-material

dependency. To support structural modernization, the updated organizational culture must prioritize the integration of digital tools and automated workflows across traditional manufacturing supply chains. Institutional support should also extend to international technology transfers, enabling domestic industrial enterprises to seamlessly align with NATO and European Union standards. Simultaneously, establishing specialized industrial parks with tax incentives will facilitate the relocation, consolidation, and scaling of high-tech production capacities. Human capital development must sit at the core of this policy shift, driving comprehensive reskilling programs that equip the workforce with advanced engineering and robotics competencies. Ultimately, aligning organizational principles with long-term export promotion strategies will allow domestic manufacturers to secure competitive positions in global value chains. This holistic institutional foundation will not only sustain the manufacturing sector through wartime pressures but also serve as the primary engine for resilient post-war economic reconstruction.

Conclusions. The conducted study demonstrates that the operation of enterprises amidst extreme geopolitical turbulence and martial law requires a fundamental restructuring of traditional crisis management concepts. A comparison of empirical data proves that traditional, rigid, and centralized management models are entirely incapable of responding to sudden external shocks of such magnitude. The research confirms that the key factor in ensuring business process continuity is the transformation of organizational culture toward the decentralization of authority and the enhancement of front-line team autonomy. Fostering a high level of horizontal trust and prioritizing human capital retention serve as a foundational institutional buffer that allows businesses to maintain operational capacity despite the physical destruction of infrastructure and supply chain disruptions.

An analysis of the scale of domestic business destruction highlights the necessity of shifting from reactive adaptation to the strategic reform of industrial policy. Full-scale security risks, energy deficits, and forced facility relocation compel companies to seek new sources of resilience through the implementation of agile digital platforms and operational supply chain reconfiguration. A key finding of the study is that forced agility in times of crisis transforms from a temporary survival measure into a long-term strategic asset. Particular significance is attached to the development of the Defense Tech sector and high-tech manufacturing, which are becoming the locomotive not only of wartime adaptation but also of post-war economic recovery. Integrating ethical leadership principles and aligning with broader stakeholder demands enable enterprises to pivot manufacturing models toward high-value-added production.

Modernizing the institutional foundations of industrial policy must be grounded in stimulating innovation, streamlining regulatory procedures, and actively attracting investment into dual-use technologies. The capacity of domestic enterprises to rapidly reshape internal values and operational structures forms a unique model of organizational viability that expands contemporary international management theory. The practical experience of Ukrainian business proves that even under conditions of total uncertainty, organizational culture can serve as the primary driver for maintaining competitiveness. The acquired practical adaptation mechanisms create a solid foundation for integrating national manufacturers into global value chains as well as EU and NATO markets. Ultimately, the crisis management model developed under wartime conditions makes it possible to transform forced agility into a long-term competitive advantage in international business. The recommendations synthesized

in this study provide a strategic roadmap for corporate leaders seeking to ensure high antifragility in their organizations amid growing global risks.

References

1. Hrazhevska, N. I., & Yerokhin, O. V. (2023). Transformatsiia biznes-modelei vitchyznianykh pidpryiemstv v umovakh voiennoho stanu ta bezpekovykh vyklykiv [Transformation of business models of domestic enterprises under martial law and security challenges]. Ekonomika ta derzhava, (4), 12–18. https://doi.org/10.32702/2306-6806.2023.4.12

2. Hrishnova, O. A., Doronina, M. S., & Kolotukha, A. V. (2022). Sotsialno-trudovi vidnosyny ta liudskyi kapital v umovakh voiennoi turbulentosti: vyklyky ta adaptatsiia [Social and labor relations and human capital in conditions of military turbulence: Challenges and adaptation]. Ukrainskyi Sotsium, (3), 45–59. https://doi.org/10.15407/socium2022.03.045

3. Gurina G.S., Podrieza S.M., Tseluiko O.I., Liskovych N. Yu. (2025). The role of human capital in a proactive approach to managing economic security threats: integrating agility and risk management. Intellectualization of Logistics and Supply Chain Management: Electronic scientific and practical journal, vol. 34, p. 59-65. DOI: https://doi.org/10.46783/smart-scm/2025-34-6

4. Lihonenko, L. O., & Miagkykh, I. M. (2023). Antykryzove upravlinnia pidpryiemstvom v umovakh voiennoho stanu: adaptyvnist ta stratehichna hnuchkist [Crisis management of the enterprise under martial law: Adaptability and strategic flexibility]. Problemy systemnoho pidkhodu v ekonomitsi, 1(93), 34–41. https://doi.org/10.32702/2520-2200-2023.1.34Aarestrup J. Cross-cultural management in times of geopolitical uncertainty. Journal of World Business. 2021. Vol. 56, No. 4. Art. 101210.

5. Christopher M. Logistics & Supply Chain Management. 5th ed. London : Pearson, 2016. 328 p.

6. Ducrot F. Ethical leadership and stakeholder alignment during crises. European Management Journal. 2022. Vol. 40, No. 2. P. 215–227.

7. Hofstede G. Culture's Consequences: Comparing Values, Behaviors, Institutions, and Organizations Across Nations. 2nd ed. Thousand Oaks : Sage Publications, 2001. 596 p.

8. Pisano G. P. Creative Construction: The DNA of Sustained Innovation. PublicAffairs, 2019. 272 p.

9. Ukraine Rapid Damage and Needs Assessment (RDNA4). URL: https://documents1.worldbank.org/curated/en/099022025114040022/pdf/P1801741ca39ec0d81b5371ff73a675a0a8.pdf

10. Schein E. H. Organizational Culture and Leadership. 5th ed. Hoboken : John Wiley & Sons, 2017. 416 p.

11. Seuring S. Resilience in supply chain management: Adapting to disruption and geopolitical shocks. International Journal of Production Economics. 2020. Vol. 229. Art. 107758.

12. Taleb N. N. Antifragile: Things That Gain from Disorder. New York : Random House, 2012. 544 p.

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

44-66
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-3

UDC 338.45:355.01
JEL Classification: G32, H56, L52, M15, O33.

Received: 2026-07-07
Accepted: 2026-08-25
Published: 2026-08-30

Harmash O.M. PhD (in Economics), Associate Professor 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

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

Davydenko V.V. PhD of Economics, associate professor, associate professor of the department of Industrial Marketing, National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0002-8419-4636
Researcher ID
Scopus author id: –
E-Mail: viold@ukr.net

A DIGITAL EARLY-WARNING FRAMEWORK FOR MONITORING THE ECONOMIC SECURITY OF DEFENCE-INDUSTRIAL ENTERPRISES

Oleh Harmash, Volodymyr Marchuk, Volodymyr Davydenko. «A digital early-warning framework for monitoring the economic security of defence-industrial enterprises». *The article substantiates the need to move from periodic retrospective assessment of the economic security of defence-industrial enterprises to a digital early-warning framework capable of detecting threats on the basis of current financial, production, logistics, contractual, personnel, supplier-related and cybersecurity indicators. The relevance of the study follows from the operating conditions of defence-industrial enterprises, which combine wartime uncertainty, technological dependence, logistics disruption, regulatory pressure and heightened requirements for continuity of critical production programmes. The purpose of the article is to develop a conceptual and methodological approach to building a digital early-warning framework for monitoring the economic security of defence-industrial enterprises. The methodological basis combines conceptual modelling, an indicator-based approach,*

risk-oriented management, multi-criteria assessment and scenario testing. The study proposes an Economic Security Digital Monitoring Index (ESDMI), a digital monitoring architecture, a system of key indicators, a four-level early-warning scale and a scenario matrix for managerial response. A synthetic scenario case is used for the preliminary testing of the model. It reproduces typical risk situations of a defence-industrial enterprise without disclosing sensitive production, contractual, supplier or cybersecurity data. The scientific contribution of the article lies in connecting the traditional logic of enterprise economic security with digital data sources, risk analytics and response protocols. The practical value of the proposed framework is that it can serve as a basis for dashboard monitoring, expert validation of indicators and the further development of a digital twin of economic security for defence-industrial enterprises.

***Keywords**:* economic security, defence-industrial enterprises, digital monitoring, early-warning system, risk management, corporate governance, supply chain security, cybersecurity, business analytics, enterprise resilience

Олег Гармаш, Володимир Марчук, Володимир Давиденко. «Цифрова система раннього попередження для моніторингу економічної безпеки підприємств оборонно-промислового комплексу». *У статті обґрунтовано необхідність переходу від періодичного ретроспективного оцінювання економічної безпеки підприємств оборонно-промислового комплексу до цифрової системи раннього попередження, здатної виявляти загрози на основі актуальних фінансових, виробничих, логістичних, контрактних, кадрових, постачальницьких показників та індикаторів кібербезпеки. Актуальність дослідження зумовлена умовами функціонування підприємств оборонно-промислового комплексу, що поєднують невизначеність воєнного часу, технологічну залежність, порушення логістичних процесів, регуляторний тиск і підвищені вимоги до безперервності виконання критично важливих виробничих програм. Метою статті є розроблення концептуально-методичного підходу до побудови цифрової системи раннього попередження для моніторингу економічної безпеки підприємств оборонно-промислового комплексу. Методологічна основа дослідження поєднує концептуальне моделювання, індикаторний підхід, ризик-орієнтоване управління, багатокритеріальне оцінювання та сценарне тестування. Запропоновано цифровий індекс моніторингу економічної безпеки (Economic Security Digital Monitoring Index – ESDMI), архітектуру цифрового моніторингу, систему ключових індикаторів, чотирирівневу шкалу раннього попередження та сценарну матрицю управлінського реагування. Для попередньої апробації моделі використано синтетичний сценарний кейс, який відтворює типові ризикові ситуації підприємства оборонно-промислового комплексу без розкриття чутливих виробничих, контрактних, постачальницьких даних або інформації з кібербезпеки. Науковий внесок статті полягає в поєднанні традиційної логіки економічної безпеки підприємства із цифровими джерелами даних, ризик-аналітикою та протоколами реагування. Практична цінність запропонованої системи полягає в можливості її використання як основи для панельного моніторингу, експертної валідації індикаторів і подальшого розроблення цифрового двійника економічної безпеки підприємств оборонно-промислового комплексу.*

Ключові слова: економічна безпека, підприємства оборонно-промислового комплексу, цифровий моніторинг, система раннього попередження, управління ризиками, корпоративне управління, безпека ланцюгів постачання, кібербезпека, бізнес-аналітика, стійкість підприємства

1. Introduction. Enterprise economic security is traditionally understood as the ability of a business entity to maintain resilience, resource capacity, financial equilibrium, asset protection and the ability to achieve strategic objectives under internal

and external threats. For defence-industrial enterprises, this concept has a more specific meaning. Economic security is connected not only with profitability or competitiveness, but also with production continuity, fulfilment of defence contracts, protection of critical technologies, reliability of supply and compliance with national security requirements. Under such conditions, economic security ceases to be a purely financial or organisational category. It becomes an integral characteristic of an enterprise's capacity to perform critical functions under deep uncertainty [21; 14; 12].

The contemporary operating environment of the defence-industrial sector is shaped by several groups of risks acting at the same time. Military threats, damage to or overload of logistics infrastructure, shortages of critical components, dependence on a limited number of suppliers, instability of public funding, growing cyber threats, shortages of engineers and production specialists, and tighter contractual deadlines form a dense risk environment. The European Defence Industrial Strategy of 2024 explicitly stresses readiness, competitiveness and resilience of the defence industry, as well as the timely availability of defence products [5; 6; 7]. A similar logic is found in the U.S. National Defense Industrial Strategy, where resilient supply chains, workforce readiness, flexible acquisition and economic deterrence are identified as strategic priorities [25; 26; 27].

Despite the growing role of digitalisation, the monitoring of economic security in many industrial enterprises remains fragmented. Some indicators are generated in financial systems, others in production, logistics, human resource, procurement or security modules. Managers therefore often receive separate signals rather than an integrated picture of risk. Traditional approaches based on quarterly or annual reporting are not sufficient for defence-industrial enterprises, where the decisive issue is not only whether a threat has emerged, but how quickly it is detected, interpreted and translated into managerial action [15; 16; 20].

The scientific problem is that existing studies of enterprise economic security tend either to classify threats and indicators or to analyse digital transformation as a separate development factor. Less attention has been paid to approaches that connect economic security indicators, digital data sources, risk analytics, dashboard monitoring and managerial response protocols within a single early-warning system for defence-industrial enterprises. This gap defines the research focus of the article [11; 15; 16; 20; 24].

The purpose of the article is to develop a digital early-warning mechanism for monitoring the economic security of defence-industrial enterprises under wartime, logistics and technological instability. Three research questions follow from this purpose: which components of economic security are critical for defence-industrial enterprises; which digital data sources and analytical tools can support their operational monitoring; and how an integral index and early-warning model can be built to support managerial decisions.

2. Literature Review.

Studies of enterprise economic security in the context of digital transformation provide an important theoretical basis for understanding how digital technologies both strengthen and complicate the security perimeter of an enterprise. Samoilenko et al. examine enterprise economic security under digital transformation and show that digitalisation changes the nature of threats through the growing role of information security, digital infrastructure and technological dependence [21]. Kukhar, Kravchyk and Brechko interpret digital transformation as a factor in ensuring enterprise economic security and emphasise that the advantages of the digital economy can be realised only when risks, data and organisational change are properly governed [14]. Ivanov, Martseniuk, Angelova and Faifer develop this argument in the field of strategic

risk management of digital transformation in industrial enterprises, pointing to cyber threats, regulatory instability and information leakage as risks that directly affect economic security [12].

A separate body of literature concerns digital monitoring and index systems. Li, Dou, Wen and Li propose a monitoring indicator system for sectoral digital transformation, covering transformation stages, digitalisation of individual domains, integration and cross-system interaction [15]. For this study, the value of their work does not lie in the Chinese sectoral context as such, but in the methodological principle: digital transformation can and should be measured through indicators that reflect not only the presence of technology, but also the level of integration between processes, data and managerial decisions. This logic is useful for building digital monitoring of economic security, because it allows technological, organisational and risk parameters to be considered together.

For defence-industrial enterprises, the literature on supply chains and resilience is especially relevant. Christopher and Peck laid important foundations for the concept of the resilient supply chain, where visibility, flexibility, collaboration and a risk-management culture are central [3]. Ponomarov and Holcomb define supply chain resilience as the adaptive capability of a supply chain to prepare for unexpected events, respond to them and recover from them [19]. Ambulkar, Blackhurst and Grawe offer an empirical approach to measuring firm resilience to supply chain disruptions, stressing resource readiness, flexibility and managerial capabilities [1]. These works matter for the defence-industrial sector because such enterprises often have long production cycles, a limited number of suppliers and high dependence on critical materials. This conclusion is also supported by studies of enterprise and supply chain resilience and the resilient enterprise [13; 22].

The work of Urmston, Song and Lyons is close to the defence-industrial context. They develop risk assessment and supplier resilience models for military industrial supply chains under rare disruptive events [24]. The authors identify financial condition, current data, business continuity planning and supply chain mapping as among the most important categories of supplier resilience. This finding directly supports the need for digital monitoring: without current data on suppliers, critical components, production nodes and disruption scenarios, an enterprise cannot assess its economic security in time [27].

Digital twins and digital supply chains form another important line of research. Ivanov and Dolgui consider a digital supply chain twin as a tool for managing disruption risks and resilience in the Industry 4.0 era [11]. Their approach is relevant for defence-industrial enterprises because a digital twin can model the propagation of disruptions, evaluate alternative scenarios and test managerial decisions before a crisis becomes irreversible. In a broader defence context, Giberna et al. show that digital twins can support modelling, planning, monitoring, training and decision-making, although their use requires attention to integration, interoperability and security [9; 28].

Research on early-warning models is also important. Fang proposes an early-warning system for corporate operational risk based on a combination of Fuzzy C-Means clustering, Random Forest and the CRITIC method for indicator weighting [8]. For this article, the value of that study is not the specific algorithm, but the underlying logic: early warning should rely on groups of indicators, an assessment of their importance, clustering of states and the predictive detection of risk deviations. This confirms the need to move from a static indicator model to a dynamic system that continuously updates the risk assessment.

The normative and methodological basis for integrating such an approach into

44-66
v.38 (2026)
https://smart-scm.org

corporate governance is formed by ISO 31000, COSO ERM, the OECD Principles of Corporate Governance and the NIST Cybersecurity Framework. ISO 31000:2018 defines risk management as an integrated process and stresses the need to identify, analyse, evaluate, treat, monitor and communicate risks within an organisation [10]. COSO ERM links risk management with strategy and performance rather than only with internal control [4]. The OECD/G20 Principles of Corporate Governance 2023 emphasise the role of boards and governing bodies in risk oversight, disclosure and long-term resilience [18]. NIST CSF 2.0 and NIST guidance on enterprise risk management and cybersecurity supply chain risk management provide a practical language for integrating cyber and supplier risks into the general management system of an enterprise [2; 16; 17; 20; 23].

2.1. Comparative Positioning of the Proposed Approach. To clarify the scientific contribution of the study, the proposed digital early-warning framework should be compared with the main groups of approaches used to assess economic security, manage risks, strengthen supply chain resilience, govern cybersecurity and organise digital monitoring. This comparison shows that the problem is not the absence of individual assessment methods. The problem is the insufficient integration of financial, production, logistics, contractual, supplier-related, personnel, cybersecurity and compliance signals into a single managerial early-warning contour [4; 10; 13; 16; 17; 21; 24].

Table 1. Comparison of Existing Approaches with the Proposed Digital Early-Warning Framework

Approach group	Main focus	Strengths	Limitations for defence-industrial enterprises	How the proposed framework complements the approach
Traditional indicator-based approaches to enterprise economic security	Financial stability, resource sufficiency, asset protection, operational threats	Provide a structured view of the components of economic security	Often retrospective; insufficiently account for digital data sources, cyber risks, contractual milestones and rapid escalation logic	Transfers economic security indicators into a digital monitoring contour and links them with subindices, ESDMI and managerial triggers
ERM / ISO 31000 / COSO	Corporate risk management, risk identification, assessment, monitoring and response	Provide a general managerial logic for risk management and integration of risk with strategy	Do not define a sector-specific indicator system for the defence-industrial sector and do not detail the digital architecture of early warning	Specifies ERM logic through defence-industrial indicators, risk scoring, dashboard monitoring and a response matrix
Supply chain resilience models	Supply resilience, adaptability, supply chain visibility and recovery after disruptions	Explain supply risks, dependence on critical components and the value of flexibility	Focus mainly on supply chains and do not fully cover financial, personnel, contractual, cybersecurity and compliance components of economic security	Integrates logistics and supplier risks with financial, production, contractual and cybersecurity subindices
NIST CSF / C-SCRM cybersecurity approaches	Cyber risks, vulnerability management, digital-system and supply-chain risks	Provide a practical language for managing cyber and supplier risks	Cyber risks often remain within the IT function and are not always linked to economic consequences, production deadlines and contractual capacity	Treats the CYB subindex as part of economic security and links cyber incidents with production, contractual and compliance consequences

Approach group	Main focus	Strengths	Limitations for defence-industrial enterprises	How the proposed framework complements the approach
Digital supply chain twin / digital twins	Process modelling, disruption scenarios and a digital representation of the system	Allow modelling of risk propagation and testing of scenarios before a crisis occurs	Require high digital maturity, integrated data and substantial implementation resources	Offers an intermediate working prototype: indicators, ESDMI, dashboard and scenario testing as a basis for a future digital twin
Algorithmic early-warning models	Risk forecasting, anomaly detection, clustering and machine learning	Can provide predictive detection of risk states	Often require large volumes of high-quality historical data; may be difficult for managers to interpret; do not always reflect defence-industrial specificity	Combines an index model, dynamic triggers and managerial interpretation; can be extended with algorithmic methods after data have accumulated
Proposed ESDMI-based early-warning framework	Integral digital monitoring of the economic security of a defence-industrial enterprise	Combines economic, production, logistics, contractual, supplier, personnel, cybersecurity and compliance signals; includes an index, thresholds, dynamic triggers, dashboard and response matrix	Requires further empirical and expert validation; depends on data quality and the correctness of weights	Creates an integrative early-warning contour suitable for staged implementation and further development toward a digital twin of economic security

Source: compiled by the authors.

The comparison shows that existing approaches create an important theoretical and methodological foundation, but each covers only part of the problem field. Traditional approaches to economic security describe the components of enterprise protection well, but they often remain retrospective. ERM approaches provide the general logic of risk management, yet they do not offer a specific digital indicator system for defence-industrial enterprises. Supply chain resilience models explain logistics and supplier risks, but they do not fully cover financial, personnel, contractual and cybersecurity consequences. Cybersecurity approaches, in turn, often remain functionally separate from the general system of economic security [4; 10; 13; 16; 17; 21; 24].

Against this background, the proposed ESDMI-based early-warning framework performs an integrative function. Its contribution is not to replace existing approaches, but to connect them in a single digital monitoring architecture where indicators become subindices, subindices form the integral ESDMI, and both the ESDMI and dynamic triggers become managerial signals for dashboard monitoring and escalation.

Thus, the literature review and comparative positioning show that studies of enterprise economic security, digital transformation, supply chain resilience, cyber risks and corporate risk management have created a sufficient

theoretical basis for early-warning systems. At the same time, an integrated model that simultaneously combines economic security indicators, digital data sources, a subindex structure, integral assessment, dynamic triggers, dashboard monitoring and response protocols for defence-industrial enterprises remains underdeveloped. The model proposed below is intended to address this methodological gap and to provide a basis for the staged implementation of a digital early-warning mechanism.

3. Research Methodology

The study is conceptual and methodological in nature. It does not claim to provide final empirical validation on closed datasets from defence-industrial enterprises, because such data are sensitive and often cannot be used in open publications. Instead, the article proposes a model structure that can be tested through expert assessment, an anonymised case or scenario-based testing. This approach is appropriate for defence-industrial research, where the first task is to design a methodologically sound and security-sensitive contour of indicators.

In the context of defence-industrial enterprises, the use of real operational data in an open scientific publication has significant limitations. Production schedules, contractual deadlines, dependence on specific suppliers, stocks of critical components, data on cyber incidents, the throughput of production nodes and financial parameters of defence contracts may directly or indirectly disclose sensitive information about enterprise capabilities. Full empirical testing on real data therefore requires a closed research regime, and its results can be published only in aggregated or anonymised form.

For this reason, the article uses a synthetic case-based validation approach. Its purpose is not to prove the statistical accuracy of the model on real data, but to test the internal logic of the early-warning framework: whether the model can reflect the deterioration of individual subindices, changes in the integral ESDMI, movement between warning levels and the need for managerial escalation. Synthetic subindex values are set on a normalised scale from 0 to 1 and are designed to reproduce typical risk situations for a defence-industrial enterprise: delay of a critical component, liquidity stress, a cyber incident in a production or contractual system, and a shortage of personnel in critical roles.

The methodology combines five elements. The first is conceptual modelling, through which the economic security of a defence-industrial enterprise is treated as a multidimensional system that includes financial, production, logistics, contractual, personnel, supplier-related, innovation-technological, information and compliance components. The second is an indicator-based approach, which turns these components into measurable indicators. The third is risk-oriented management, where indicators are interpreted not as isolated KPIs but as signals of possible deterioration in economic security. The fourth is multi-criteria assessment, which involves indicator normalisation, weighting and calculation of an integral index. The fifth is scenario testing, which checks whether the model can identify typical threats before they reach critical impact [10; 15; 20].

Calibration of early-warning thresholds is a separate methodological element of the study. In the proposed model, Green, Yellow, Orange and Red thresholds are not treated as universal normative boundaries for all defence-industrial enterprises. They are considered an initial configuration of early warning that should be adjusted to the enterprise type, the criticality of the production programme, the structure of defence contracts, supply chain resilience, the level of digital maturity and the accepted level of risk [8; 10].

Threshold calibration can rely on four complementary approaches: expert assessment, analysis of historical data, scenario testing and review of actual incidents. At the first stage, expert-defined starting boundaries may be used to create an interpretable traffic-light logic. At later stages, these boundaries should be refined on the basis of the observed behaviour of subindices, the frequency of false signals, time to critical impact and the managerial consequences of recorded risk events [8; 10].

Data sources for practical application of the model may include ERP systems, financial and accounting modules, MES, SCM, WMS, TMS, SRM, HRM, EDI, contract management systems, BI platforms, SIEM, cyber incident logs, access control systems, supplier data, information on government contract performance, internal audit results and expert assessments. In the open version of the article these sources are presented at the level of information-system types, without disclosing specific technological, production or defence parameters [15; 16; 17; 20].

The indicator system is built according to three criteria. An indicator should reflect a significant component of the economic security of a defence-industrial enterprise, have a potential digital data source and be suitable for managerial interpretation. For example, a liquidity indicator matters only when it can be connected with the risk of production delay or contract non-performance. Likewise, a supplier delay indicator becomes a security indicator only when it is linked to component criticality, contractual deadlines and the availability of alternative supply [10; 15].

To make the model reproducible, each ESDMI indicator should be described through an operational passport that includes the indicator name, formula or calculation method, direction of influence on the subindex, digital data source, recommended update frequency and managerial interpretation. This prevents indicators from remaining only general labels without a clear measurement procedure. In the open publication, formulas are presented at the level of universal calculation logic, while specific threshold values should be determined by the enterprise or an expert group [15; 20].

4. Research Results

4.1. Components and Indicators of Economic Security in Defence-Industrial Enterprises. In the proposed model, the economic security of a defence-industrial enterprise is understood as an integral state formed not by a single group of indicators, but by the interaction of several subsystems. Table 2 presents the basic structure of components, key risks, potential digital data sources and sample indicators. It is not an exhaustive list, but it can serve as a methodological basis for building a specific monitoring system within an enterprise.

Table 2. Components of Digital Monitoring of Economic Security in Defence-Industrial Enterprises

Economic security component	Key risk	Potential digital data sources	Sample indicators
Financial security	Liquidity shortage, rising debt burden, funding delays	ERP, accounting system, BI, treasury module	Current liquidity ratio, cash conversion cycle, share of overdue receivables, debt load
Production security	Production-cycle disruption, underload or overload of capacity	MES, ERP, production dashboards	Production delay rate, schedule adherence, capacity utilisation, backlog pressure

Economic security component	Key risk	Potential digital data sources	Sample indicators
Logistics security	Delays of critical materials, route disruption, longer lead time	SCM, WMS, TMS, EDI	Supplier delay index, average lead time deviation, critical inventory days, route disruption score
Contractual security	Non-fulfilment of defence contracts, penalties, missed deadlines	Contract management system, ERP, procurement systems	Contract fulfilment deviation, milestone delay rate, penalty exposure, order-to-delivery deviation
Supplier security	Dependence on one supplier, supplier financial weakness, import dependence	SRM, procurement analytics, supplier databases	Supplier concentration ratio, single-source dependency, supplier financial risk score, alternative supplier availability
Personnel security	Shortage of critical specialists, staff turnover, overload of key teams	HRM, time tracking, access systems	Critical staff availability, turnover in critical roles, overtime intensity, training coverage
Innovation-technological security	Technological lag, low readiness of digital solutions, dependence on legacy systems	PLM, R&D systems, IT asset management	R&D continuity index, technology readiness score, legacy system dependency, modernisation backlog
Information and cybersecurity	Cyber incidents, data leakage, compromise of production or contract systems	SIEM, SOC tools, vulnerability scanners, backup systems	Incident frequency, mean time to respond, overdue critical vulnerabilities, backup recovery success rate
Compliance security	Regulatory violations, non-compliance with contractual and security standards	Compliance platforms, audit systems, document management	Audit finding severity, compliance breach alerts, corrective action closure rate

Source: compiled by the authors.

The proposed structure reflects the specifics of defence-industrial enterprises because it combines classical financial indicators with production, contractual, supplier-related and cybersecurity parameters. This integration is essential. A single financial indicator may not signal a crisis, but its simultaneous deterioration together with supplier delays and a growing production backlog may indicate the approach of systemic risk.

4.1.1. Operationalisation of Key ESDMI Indicators

For practical use, the proposed monitoring system must not only classify indicators by component of economic security, but also operationalise them. Operationalisation means defining the calculation method, direction of influence on the subindex, digital data source, update frequency and managerial interpretation for each indicator. Table 3 presents an example of a basic indicator set that can be used to build a working prototype of ESDMI. In practice, this set may be expanded or adjusted depending on the type of defence-industrial enterprise, the structure of the production programme, contract criticality and data availability [15; 20].

The table is not a closed list of indicators. Its purpose is to show how general components of economic security can be transformed into measurable parameters of digital monitoring. For each defence-industrial enterprise, the list of indicators should be refined with regard to critical production processes, the structure of defence orders, contractual obligations, technological complexity and confidentiality requirements.

44-66
v.38 (2026)
https://smart-scm.org

Table 3. Operationalisation of Key Indicators for Digital Monitoring of Economic Security in Defence-Industrial Enterprises

Component	Indicator	Formula / calculation method	Direction of influence	Digital data source	Recommended update frequency
Financial security	Current liquidity ratio	Current assets / current liabilities	Stimulant	ERP, accounting system, treasury module	Weekly / monthly
Financial security	Share of overdue receivables	Overdue receivables / total receivables	Destimulant	ERP, accounting system, BI	Weekly
Production security	Production schedule adherence	Number of production tasks completed on time / total planned tasks	Stimulant	MES, ERP, production dashboard	Daily / weekly
Production security	Share of delayed production orders	Delayed production orders / total production orders	Destimulant	MES, ERP	Daily / weekly
Logistics security	Deviation of actual lead time from planned lead time	(Actual lead time - planned lead time) / planned lead time	Destimulant	SCM, TMS, WMS, EDI	Daily / weekly
Logistics security	Critical component inventory days	Available stock of critical component / average daily consumption	Stimulant within the minimum required level	WMS, ERP, SCM	Daily
Contractual security	Share of overdue contractual milestones	Overdue milestones / total active milestones	Destimulant	Contract management system, ERP	Weekly
Contractual security	Potential penalty exposure	Potential penalties for delay / value of the relevant contract	Destimulant	Contract management system, ERP, finance module	Weekly / monthly
Supplier security	Supplier concentration ratio	Purchases from the largest supplier of critical components / total purchases of critical components	Destimulant	SRM, procurement analytics	Monthly
Supplier security	Availability of alternative suppliers	Critical components with a qualified alternative supplier / total critical components	Stimulant	SRM, supplier database, procurement system	Monthly / quarterly
Personnel security	Availability of personnel in critical roles	Available employees in critical roles / required number of such employees	Stimulant	HRM, time tracking, access control system	Weekly
Personnel security	Overtime intensity of critical teams	Overtime hours of critical teams / standard working-time fund	Destimulant	HRM, time tracking	Weekly / monthly
Innovation-technological security	Dependence on legacy systems	Critical processes running on legacy or unsupported systems / total critical processes	Destimulant	IT asset management, PLM, internal audit	Quarterly

Component	Indicator	Formula / calculation method	Direction of influence	Digital data source	Recommended update frequency
Innovation-technological security	Readiness level of critical technologies	Average technology readiness level of critical solutions / target readiness level	Stimulant	PLM, R&D systems, project portfolio system	Quarterly
Information and cybersecurity	Share of critical vulnerabilities not remediated on time	Critical vulnerabilities with overdue SLA / total critical vulnerabilities	Destimulant	SIEM, SOC tools, vulnerability scanner	Daily / weekly
Information and cybersecurity	Backup recovery success rate	Successful recovery tests / total recovery tests	Stimulant	Backup system, SOC, IT audit	Monthly
Compliance security	Timeliness of corrective-action closure	Corrective actions closed on time / total corrective actions	Stimulant	Compliance platform, audit system	Monthly
Compliance security	Audit finding criticality index	Weighted sum of audit findings by severity / maximum possible weighted score	Destimulant	Audit system, document management system	Quarterly

Source: compiled by the authors.

Operationalised indicators are then transformed into normalised values used to calculate ESDMI subindices. For stimulant indicators, an increase in the value is interpreted as an improvement in the relevant component of economic security. For destimulant indicators, an increase means higher risk. Each indicator must therefore be classified by direction of influence before normalisation. This ensures methodological consistency between digital data sources, the indicator level, subindices and the integral ESDMI [15].

4.2. Integral Index of Digital Monitoring of Economic Security

To aggregate indicators, the article proposes the Economic Security Digital Monitoring Index (ESDMI), which reflects the current level of economic security of a defence-industrial enterprise within a digital monitoring contour. The index is calculated as a weighted sum of subindices for the key components:

$$ESDMI = W_{fs} \cdot FS + W_{os} \cdot OS + W_{ls} \cdot LS + W_{cs} \cdot CS + W_{hr} \cdot HR + W_{cyb} \cdot CYB + \\ + W_{sup} \cdot SUP + W_{is} \cdot IS + W_{com} \cdot COM$$

where FS is financial security; OS is operational or production security; LS is logistics security; CS is contractual security; HR is personnel security; CYB is information and cybersecurity; SUP is supplier security; IS is innovation and technological security; COM is compliance security; and W denotes the weight coefficients of the corresponding components.

Each subindex is formed from normalised indicators. For stimulant indicators, where a higher value means a better security state, normalisation may be performed as follows:

$$Z_{ij} = \frac{(X_{ij} - X_{min})}{(X_{max} - X_{min})}.$$

For destimulant indicators, where a higher value means higher risk, inverse normalisation is appropriate:

$$Z_{ij} = \frac{(X_{max} - X_{ij})}{(X_{max} - X_{min})}.$$

The component subindex is calculated as a weighted sum of normalised indicators:

$$S_i = \sum_i V_{ij} \cdot Z_{ij},$$

where V_{ij} is the weight of the *j-th* indicator within the *i-th* component. The overall *ESDMI* value is interpreted within the interval from 0 to 1. Values close to 1 indicate a high level of economic security; values close to 0 indicate critical deterioration.

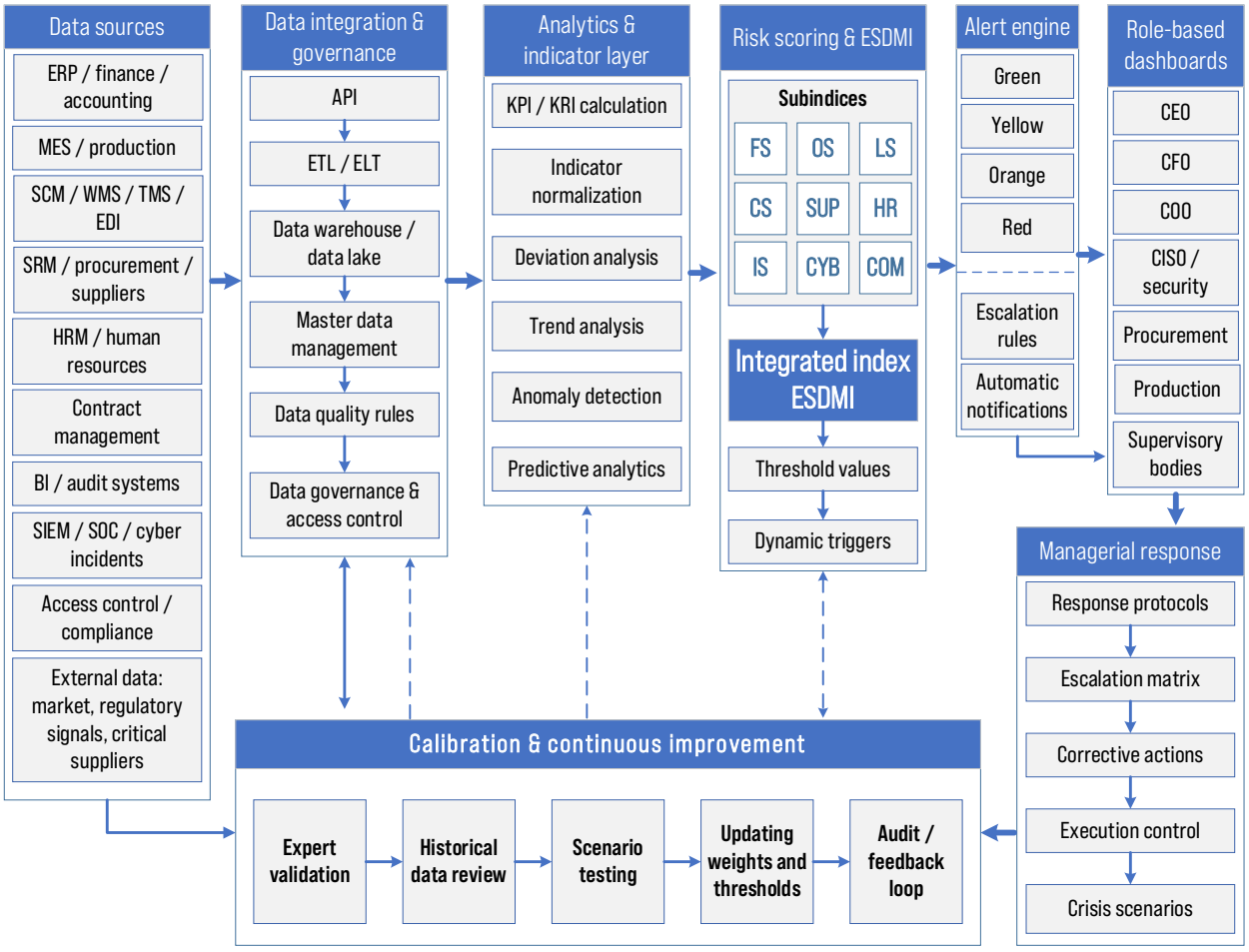
Component weights may be determined in several ways. At the first stage, expert assessment with specialists in finance, production, logistics, procurement, corporate governance, cybersecurity and defence management is appropriate. To improve methodological reliability, the Delphi procedure, AHP or the CRITIC method can be combined, while the consistency of expert assessments can be checked using Kendall's coefficient of concordance [29; 30; 31]. Later, weights may be refined using historical enterprise data and the observed impact of individual risks on contract performance, financial stability and production continuity.

4.3. Architecture of the Digital Early-Warning Framework

A digital early-warning mechanism cannot be reduced to the calculation of an index. It must include an architecture for data collection, integration, analysis, interpretation and managerial response. The proposed architecture has six layers [10; 15; 20]:

Data layer -> Integration layer -> Analytics layer -> Risk scoring layer -> Dashboard layer -> Managerial response layer.

The data layer brings together primary digital sources: ERP, MES, SCM, SRM, HRM, contract management systems, BI, SIEM, audit systems and access control systems. The integration layer supports data exchange through APIs, ETL/ELT processes, a corporate data warehouse, master data management and data quality rules. The analytics layer calculates indicators, detects deviations, analyses trends, compares values with thresholds and, where sufficient data are available, forecasts risk states. The risk scoring layer translates indicators into subindices, the integral ESDMI and warning levels. The dashboard layer presents results for different managerial roles: CEO, CFO, COO, head of security, procurement director, production manager and oversight bodies. The final layer, managerial response, contains action scenarios, an escalation matrix, responsible persons and control over corrective measures [15; 16; 17; 20].



***Abbreviations**: FS – financial security; OS – operational security; LS – logistics security; CS – contract security; SUP – supplier security; HR – human resources security; IS – innovation and technological security; CYB – information and cybersecurity; COM – compliance security.*

Figure 1. Architecture of the digital early-warning mechanism for monitoring economic security.

Source: compiled by the authors.

In this architecture, the dashboard is not merely a visualisation tool. It is a managerial interface between risk signals and decisions. For example, deterioration of the logistics subindex may be only an informational signal on its own. But if it is accompanied by falling critical inventory days, a rising supplier concentration ratio and a deviation from a contractual milestone, the system should raise the warning level and launch a scenario check for the risk of supply failure.

4.4. Early-Warning Model

A four-level early-warning scale is proposed for interpreting ESDMI. It follows a traffic-light logic, but its function is not limited to colour-coding the state of economic security. Each level is linked to a type of managerial response. The proposed thresholds should be treated as starting calibration boundaries for a working prototype of the early-warning system, not as universal standards for all defence-industrial enterprises [8; 10].

Methodologically, the scale performs three functions. First, it allows managers to interpret the integral ESDMI quickly. Second, it creates a basis for risk escalation between functional units. Third, it enables comparison not only of the current level of economic

security, but also of the rate at which it deteriorates over time. Absolute threshold values should therefore be combined with dynamic triggers that capture a sharp fall in critical subindices even when the integral ESDMI has not yet entered a critical zone [8; 10].

Table 4. Calibrated Early-Warning Scale Based on ESDMI

Level	ESDMI value	Economic security state	Managerial interpretation	Response type	Threshold logic
Green	0.80-1.00	Stable	Risks remain within an acceptable level	Standard monitoring	Zone of sufficient resilience, where most subindices show no critical deviations
Yellow	0.65-0.79	Tense	Deviations requiring explanation have been recorded	Cause analysis and local actions	Early managerial signal zone, where risk is not yet critical but requires functional analysis
Orange	0.50-0.64	Critical	Risks may affect financial, production or contractual resilience	Managerial intervention and escalation	Systemic risk zone, where deterioration of several subindices may affect critical functions
Red	0.00-0.49	Threatening	There is a high probability of disruption of critical functions	Anti-crisis protocol	Zone of potential loss of production, contractual or operational capability

Source: compiled by the authors.

The proposed boundaries serve as an initial scale for interpreting the integral index. Their advantage is managerial simplicity: decision-makers receive a clear signal about the current state of economic security. At the same time, for defence-industrial enterprises, reliance on the integral ESDMI alone is insufficient because a single critical subindex may deteriorate sharply before the integral index moves into the Orange or Red zone.

The early-warning model should therefore operate on the principle of dual control: the absolute threshold of the integral ESDMI and dynamic triggers for critical subindices. For defence-industrial enterprises, the production, logistics, contractual, supplier and information-cybersecurity subindices should be treated as critical, because their rapid deterioration can directly affect defence contract fulfilment, production continuity or the protection of critical data [17; 24; 27].

Table 5. Dynamic Triggers for Early-Warning Escalation

Trigger type	Activation condition	Managerial logic	Recommended response
Fall of a critical subindex	Decrease of OS, LS, CS, SUP or CYB by more than 25-30% over a short period	Integral ESDMI may remain acceptable, while one critical subsystem already creates a threat	Raise the warning level by at least one level
Critical subindex value	Any critical subindex below 0.50	A specific area of economic security is losing resilience	Escalate to Orange regardless of integral ESDMI
Near-critical subindex value	Any critical subindex below 0.35	There is a risk of losing functional capacity	Launch a Red-level anti-crisis check

Trigger type	Activation condition	Managerial logic	Recommended response
Combined risk	Simultaneous deterioration of two or more critical subindices	The risk is cross-functional and may spread quickly	Hold a cross-functional management meeting and conduct scenario testing
Contractual impact	Any deviation affecting a defence contract milestone	Even a local risk becomes strategic if it threatens contract fulfilment	Escalate to enterprise leadership
Speed of deterioration	Decrease of ESDMI by more than 0.10 in one monitoring cycle	The speed of decline is more important than the current level	Conduct an extraordinary cause review and revise the forecast

Source: compiled by the authors.

In general, the warning level may be determined not only by the absolute value of ESDMI, but also by the maximum-risk-signal rule:

$$L_t = \max\{L(ESDMI_t), L(S_{i,t}), L(\Delta S_{i,t}), L(C_t)\},$$

where L_t is the final warning level at time t; $L(ESDMI_t)$ is the level determined by the integral index; $L(S_i,t)$ is the level determined by the critical value of an individual subindex; $L(\Delta S_i,\ t)$ is the level determined by the rate of subindex deterioration; and $L(C_t)$ is the level determined by the contractual or production criticality of the risk. This approach reduces the probability that the integral index will mask a sharp deterioration in one critical area of economic security.

In addition to absolute thresholds, the system should account for dynamic triggers. If the integral index remains in the Green zone but one critical subindex falls by more than a defined percentage over a short period, the system should issue a warning. For example, a sharp decline in supplier security may not immediately change ESDMI, but for a defence-industrial enterprise it is a signal of a possible future production disruption. The model should therefore assess not only the current state, but also the speed of deterioration, the interdependence between indicators and the criticality of the specific process [8; 24; 27].

4.5. Scenario Testing of the Model on a Synthetic Case

A synthetic case of a conditional defence-industrial enterprise is used for preliminary testing of the proposed early-warning framework. This approach was chosen because real production, contractual, supplier, financial and cybersecurity data of defence enterprises cannot usually be used openly. The synthetic case is not empirical proof of universal model accuracy. It is used to demonstrate the logic of ESDMI, the behaviour of subindices under different types of risk shocks, and the link between the warning level and managerial response.

The synthetic case includes nine subindices: financial, production, logistics, contractual, supplier, personnel, innovation-technological, information-cybersecurity and compliance. Each subindex is normalised from 0 to 1, where 1 represents the best security state and 0 represents critical deterioration. Component weights are illustrative for a defence-industrial enterprise where production continuity, contractual fulfilment, supplier reliability and logistics resilience are especially important.

44-66
v.38 (2026)
https://smart-scm.org

Table 6. Component Weights and Baseline State of the Synthetic Case

Component	Symbol	Weight	Baseline subindex value
Financial security	FS	0.12	0.82
Production security	OS	0.16	0.84
Logistics security	LS	0.14	0.81
Contractual security	CS	0.14	0.86
Supplier security	SUP	0.14	0.80
Personnel security	HR	0.08	0.78
Innovation-technological security	IS	0.08	0.76
Information and cybersecurity	CYB	0.10	0.79
Compliance security	COM	0.04	0.85
Total / ESDMI	**-**	**1.00**	**0.815**

The baseline ESDMI value is 0.815, which corresponds to the Green warning level. This means that the conditional enterprise initially has an acceptable level of economic security and that risks remain within the standard monitoring range. At the same time, individual subindices differ in their initial resilience: the innovation-technological, personnel and cybersecurity blocks are relatively lower, which reflects typical vulnerabilities of defence-industrial enterprises to shortages of competencies, technological lag and digital threats.

Table 7. Results of ESDMI Scenario Testing on a Synthetic Case with the Maximum-Risk-Signal Rule

Scenario	Main change in subindices	ESDMI after shock	Level by ESDMI	Dynamic trigger	Final level by maximum-risk-signal rule	Managerial interpretation
Baseline state	No risk shock	0.815	Green	None	Green	Standard monitoring
Critical component delay	LS: 0.81 -> 0.38; SUP: 0.80 -> 0.40; OS: 0.84 -> 0.58; CS: 0.86 -> 0.57	0.616	Orange	LS and SUP fall by more than 30%	Orange	Risk of disruption of the production programme and contractual milestone
Liquidity stress	FS: 0.82 -> 0.35; CS: 0.86 -> 0.58; OS: 0.84 -> 0.70	0.697	Yellow	FS falls by more than 40%	Orange	Financial strain is not yet a systemic crisis, but requires CFO intervention
Cyber incident in a production or contract system	CYB: 0.79 -> 0.32; OS: 0.84 -> 0.52; CS: 0.86 -> 0.62; COM: 0.85 -> 0.70	0.677	Yellow	CYB falls by more than 50%	Orange with a Red-level check	The integral index has not yet moved to Orange, but the critical cyber signal requires escalation
Personnel shortage in a critical role	HR: 0.78 -> 0.35; OS: 0.84 -> 0.60; CS: 0.86 -> 0.68	0.717	Yellow	HR falls by more than 40%	Yellow with enhanced monitoring	Risk of losing production capacity in the medium term

Source: compiled by the authors.

The scenario testing shows that the warning level should not always be determined only by the integral ESDMI value. In the liquidity stress and cyber incident scenarios, the integral index formally remains in the Yellow zone, but a sharp deterioration of an individual subindex activates a dynamic or subindex trigger and raises the final level of managerial attention. This confirms the value of the maximum-risk-signal rule, according to which the final early-warning level is set by the most critical signal rather than by the aggregate score alone.

The cyber incident scenario is particularly illustrative. After the shock, ESDMI equals 0.677, which corresponds to Yellow on the absolute scale. However, the CYB subindex falls from 0.79 to 0.32 and enters a near-critical zone. Under the maximum-risk-signal rule, this situation should be classified as Orange with a Red-level check, because a cyber incident in a production or contractual system may quickly become a production, contractual or compliance risk.

The critical component delay scenario demonstrates a systemic cross-functional effect. Simultaneous deterioration of the logistics, supplier, production and contractual subindices reduces ESDMI to 0.616, which corresponds to Orange. In this case, the integral index and dynamic triggers provide a consistent signal: the enterprise should move from local monitoring to managerial escalation, search for an alternative supplier, review critical stock levels and adjust the production schedule.

The liquidity stress scenario shows that financial risk may be underestimated if managers rely only on the integral ESDMI. After the shock, the index is 0.697 and formally remains in the Yellow zone. Yet the financial subindex falls from 0.82 to 0.35, which indicates a sharp deterioration in solvency. For a defence-industrial enterprise, this can quickly affect procurement, payment for critical components, contract performance and production continuity. The final warning level should therefore be raised to Orange as a signal of financial escalation.

The critical personnel shortage scenario has a different character. Although the HR subindex falls from 0.78 to 0.35, the integral ESDMI remains at 0.717. This risk does not always create an immediate crisis, but it may have a delayed effect on production capacity and contractual deadlines. The final level may therefore remain Yellow, but with enhanced monitoring, competency reserves and preparation of backups for critical roles.

The synthetic case-based validation therefore demonstrates that ESDMI should not be used as a self-sufficient aggregate rating. Its practical value increases when the integral assessment is combined with dynamic triggers, critical subindices and a managerial escalation matrix.

5. Discussion

The proposed approach changes the logic of managing the economic security of defence-industrial enterprises. In a traditional model, economic security is assessed mainly after the reporting period. Such an approach is useful for analysing the past, but it is insufficient in an environment where risks spread quickly between financial, production, logistics and digital subsystems. The early-warning framework shifts economic security from retrospective control to current observation and preventive management [10; 20].

One of the main advantages of the model is that it connects economic and digital signals. For a defence-industrial enterprise, a cyber incident cannot be treated only as a technical event, just as a supplier delay cannot be treated only as a logistics problem. Both may have economic consequences: contract disruption, higher costs, loss of production capacity, reputational damage or breach of security requirements. NIST CSF 2.0 and guidance on cybersecurity supply chain risk management are therefore relevant not only for IT units, but also for the broader

economic security mechanism of the enterprise [2; 16; 17].

From the perspective of corporate governance, the proposed model can strengthen the role of supervisory and executive bodies in risk oversight. The OECD/G20 Principles of Corporate Governance 2023 emphasise that effective corporate governance requires appropriate disclosure, risk oversight and orientation toward long-term resilience [18]. In defence-industrial enterprises, this logic must be adapted to closed data and security restrictions. An internal management dashboard may contain detailed indicators, while aggregated and security-cleared information may be prepared for state authorities or supervisory bodies.

The practical value of the framework lies in its support for different managerial roles. The CEO receives an integrated picture of economic security and can see which subsystems generate the greatest risk. The CFO can track financial signals before a liquidity crisis. The COO receives early warnings about production and logistics deviations. The procurement director can see supplier concentration, dependence on critical components and weak points in the supplier base. The information security manager can show how cyber risk affects production and economic outcomes. This cross-functional visibility is a condition of enterprise resilience [18; 20].

The model also has limitations. First, the quality of ESDMI depends on the quality of primary data. If data are incomplete, delayed or incompatible between systems, the integral index may create a false sense of control. Second, indicator weights must be adapted to the profile of a specific enterprise, because an electronics manufacturer, a repair enterprise, an ammunition producer and an engineering design organisation have different risk profiles. Third, excessive formalisation can be dangerous if managers treat the index as a substitute for professional judgement. ESDMI should support decisions, not replace managerial responsibility [4; 10].

6. Practical implementation mechanism

The practical implementation of a digital early-warning mechanism should proceed in stages. First, the enterprise should identify critical processes that directly affect defence contract fulfilment, production continuity and financial stability. Second, it should build a map of risks and indicators, where each risk is linked to a digital data source, responsible unit, update frequency and managerial threshold. Third, data from ERP, MES, SCM, SRM, HRM, BI and SIEM should be integrated at the level of a data warehouse or analytical platform. Fourth, indicator weights should be defined and ESDMI calculated. Fifth, a dashboard and managerial response matrix should be created. Sixth, the model should undergo scenario testing. Seventh, it should be regularly updated on the basis of actual incidents, audit results and expert review [4; 10; 15; 20].

Table 8. Stages of Implementing Digital Monitoring of Economic Security

Stage	Work content	Expected result
Diagnosis	Identify critical processes, contracts, resources and threats	Map of critical zones of economic security
Indicator design	Select indicators, data sources, thresholds and responsible persons	ESDMI indicator register
Data integration	Connect ERP, MES, SCM, SRM, HRM, BI, SIEM and other systems	Unified digital data contour

Stage	Work content	Expected result
Risk scoring	Normalise indicators, define weights and calculate subindices	Integral index and risk profile
Dashboard	Visualise the security state for managerial roles	Early-warning management dashboard
Response protocols	Define actions for Green, Yellow, Orange and Red levels	Escalation and responsibility matrix
Model review	Audit signal accuracy and update weights and thresholds	Continuous improvement of the system

Source: compiled by the authors.

In practice, it is better to begin not with the most complex AI model, but with a controlled minimum monitoring contour. A first working prototype may include 20-30 key indicators, several critical business processes and a simple four-level warning scale. After historical data have accumulated, the model can be expanded with predictive analytics, state clustering, anomaly detection or a digital twin of enterprise economic security [8; 11; 28].

7. Limitations and directions for further research

The main limitation of the study is its conceptual and methodological character. The proposed model requires empirical validation using data from defence-industrial enterprises or through an expert procedure involving specialists in defence industry, finance, logistics, production, cybersecurity and corporate governance. Because of the sensitivity of the defence sector, such validation must comply with confidentiality requirements, and its results may be published only in aggregated or anonymised form.

The use of a synthetic case is methodologically justified for preliminary testing of the model's logic, but it does not replace full empirical validation. Synthetic subindex values do not reflect the actual state of a specific defence-industrial enterprise and cannot be used for inter-organisational comparison. Their function is to show how ESDMI, thresholds, dynamic triggers and managerial escalation can work within one early-warning contour. The next stage of research should test the model on anonymised data from defence-industrial enterprises or through a Delphi/AHP expert procedure followed by an assessment of the consistency of weighting coefficients [29; 30].

A second limitation is the general character of the proposed structure. Defence-industrial enterprises differ in production cycles, technological complexity, supply structure and dependence on public procurement. ESDMI should therefore be treated not as a fixed standard, but as a methodological template that must be adapted to a specific enterprise type. A third limitation concerns data: digital monitoring can be effective only when an enterprise has sufficient data maturity, integrated information systems and clear data governance rules [15; 17; 24].

A separate limitation is the initial character of the proposed ESDMI thresholds. The Green, Yellow, Orange and Red boundaries used in this article are a starting calibration scale for demonstrating the logic of early warning. They should not be interpreted as universal norms for all defence-industrial enterprises. In practical application, thresholds should be refined on the basis of expert assessment, historical data, actual incidents, risk appetite and the criticality of specific production and contractual processes. Further research should test threshold stability, estimate the frequency of false positive and false negative signals, and determine optimal boundaries for different types of defence-industrial enterprises.

Further research should focus on expert validation of ESDMI weights, development of sectoral indicator profiles for different types of defence-industrial enterprises, methods for assessing the accuracy of early-warning signals, integration of cyber risks with financial and production consequences, and the construction of a digital twin of enterprise economic security. A separate promising direction is comparative research on defence-industrial enterprises in different countries in terms of digital maturity, supply chain resilience and corporate mechanisms of risk governance [11; 18; 24; 28].

8. Conclusions.

Defence-industrial enterprises need not a one-time assessment of economic security, but continuous digital monitoring capable of detecting risk deviations before they become a crisis. Wartime, logistics, technological and cyber instability make traditional retrospective approaches insufficient, because managerial decisions must be made not after the end of a reporting period, but at the moment an early threat signal appears.

The article proposes a digital early-warning framework that combines economic security indicators, digital data sources, the integral ESDMI, dashboard-monitoring architecture, a four-level warning scale and a scenario matrix for managerial response. The scientific contribution lies in integrating enterprise economic security with the logic of digital risk monitoring, supply chain resilience, cybersecurity risk management and corporate governance. The practical value of the model is that it can be used as a basis for an internal management dashboard of a defence-industrial enterprise, expert risk assessment and further empirical validation.

Scenario testing on a synthetic case shows that the proposed model can reflect not only integral deterioration of economic security, but also critical changes in individual subindices. This is especially important for defence-industrial enterprises, where a single risk, such as a cyber incident, shortage of a critical component or loss of a key competence, may have a delayed but systemic effect on production continuity and defence contract fulfilment. ESDMI should therefore be used not as a self-sufficient automatic rating, but as an element of a broader managerial contour that combines index assessment, dynamic triggers, dashboard monitoring and response protocols.

The proposed model does not eliminate risks automatically. It reduces the time needed to detect them, improves the transparency of cross-functional interaction and helps connect financial, production, logistics, personnel, supplier and cybersecurity signals within one system for managing economic security. This shift from fragmented control to digital early warning is a necessary condition for the resilience of defence-industrial enterprises under contemporary security challenges.

References

1. Ambulkar S., Blackhurst J., Grawe S. Firm's resilience to supply chain disruptions: scale development and empirical examination. *Journal of Operations Management*. 2015. Vol. 33-34. P. 111-122. DOI: https://doi.org/10.1016/j.jom.2014.11.002

2. Boyens J., McWhite R., Calloway L., Bartol N., Scarfone K. *NIST Cybersecurity Framework 2.0: Quick-Start Guide for Cybersecurity Supply Chain Risk Management (C-SCRM)*. NIST Special Publication 1305. 2024. DOI: https://doi.org/10.6028/NIST.SP.1305

3. Christopher M., Peck H. Building the resilient supply chain. *The International Journal of Logistics Management*. 2004. Vol. 15, No. 2. P. 1-14. DOI: https://doi.org/10.1108/09574090410700275

4. Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management: Integrating with Strategy and Performance* [Electronic resource]. 2017. URL: https://www.coso.org/enterprise-risk-management (accessed: 25.06.2026).

5. European Commission ; High Representative of the Union for Foreign Affairs and Security Policy. *A new European Defence Industrial Strategy: Achieving EU readiness through a responsive and resilient European Defence Industry* [Electronic resource] : Joint Communication JOIN(2024) 10 final. Brussels, 2024. URL: https://defence-industry-space.ec.europa.eu/document/download/643c4a00-0da9-4768-83cd-a5628f5c3063_en (accessed: 25.06.2026).

6. European Commission. *Proposal for a Regulation establishing the European Defence Industry Programme and a framework of measures to ensure the timely availability and supply of defence products (EDIP)* [Electronic resource] : COM(2024) 150 final. Brussels, 2024. URL: https://defence-industry-space.ec.europa.eu/document/download/6cd3b158-d11a-4ac4-8298-91491e5fa424_en (accessed: 25.06.2026).

7. European Commission. First ever defence industrial strategy and a new defence industry programme to enhance Europe's readiness and security [Electronic resource]. 2024. URL: https://defence-industry-space.ec.europa.eu/first-ever-defence-industrial-strategy-and-new-defence-industry-programme-enhance-europes-readiness-2024-03-05_en (accessed: 25.06.2026).

8. Fang X. Early warning strategies for corporate operational risk: a study by an improved random forest algorithm using FCM clustering. *PLOS ONE*. 2025. Vol. 20, No. 3. Article e0318491. DOI: https://doi.org/10.1371/journal.pone.0318491

9. Giberna M., Voos H., Tavares P., Nunes J., Sorg T., Masini A., Sanchez-Lopez J. L. *On Digital Twins in Defence* [Electronic resource]. arXiv, 2025. URL: https://arxiv.org/abs/2508.05717 (accessed: 25.06.2026).

10. International Organization for Standardization. *ISO 31000:2018. Risk management - Guidelines* [Electronic resource]. Geneva : ISO, 2018. URL: https://www.iso.org/standard/65694.html (accessed: 25.06.2026).

11. Ivanov D., Dolgui A. A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. *Production Planning & Control*. 2021. Vol. 32, No. 9. P. 775-788. DOI: https://doi.org/10.1080/09537287.2020.1768450

12. Ivanov M., Martseniuk L., Angelova M., Faifer S. Strategic risk management of digital transformation in the economic security of industrial enterprises. *Economics Ecology Socium*. 2025. Vol. 9, No. 2. P. 124-137. URL: https://ees-journal.com/index.php/journal/article/view/298 (accessed: 25.06.2026).

13. Kamalahmadi M., Parast M. M. A review of the literature on the principles of enterprise and supply chain resilience: major findings and directions for future research. *International Journal of Production Economics*. 2016. Vol. 171. P. 116-133. DOI: https://doi.org/10.1016/j.ijpe.2015.10.023

14. Kukhar O., Kravchyk Y., Brechko O. Digital transformation as a factor in ensuring economic security of enterprises. *Baltic Journal of Economic Studies*. 2023. Vol. 9, No. 5. P. 143-152. DOI: https://doi.org/10.30525/2256-0742/2023-9-5-143-152

15. Li J., Dou K., Wen S., Li Q. Monitoring index system for sectors' digital transformation and its application in China. *Electronics*. 2021. Vol. 10, No. 11. Article 1301. DOI: https://doi.org/10.3390/electronics10111301

16. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29

17. National Institute of Standards and Technology. *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* [Electronic resource]. NIST Special Publication 800-161 Rev. 1. 2024. URL: https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final (accessed: 25.06.2026).

18. OECD. *G20/OECD Principles of Corporate Governance 2023*. Paris : OECD Publishing, 2023. DOI: https://doi.org/10.1787/ed750b30-en

19. Ponomarov S. Y., Holcomb M. C. Understanding the concept of supply chain resilience. *The International Journal of Logistics Management*. 2009. Vol. 20, No. 1. P. 124-143. DOI: https://doi.org/10.1108/09574090910954873

20. Quinn S., Pillitteri V., Barrett M., Smith M., Witte G. *NIST Cybersecurity Framework 2.0: Enterprise Risk Management Quick-Start Guide*. NIST Special Publication 1303. 2024. DOI: https://doi.org/10.6028/NIST.SP.1303

21. Samoilenko Y., Britchenko I., Levchenko I., Losonczi P., Bilichenko O., Bodnar O. Economic security of the enterprise within the conditions of digital transformation. *Economic Affairs*. 2022. Vol. 67, No. 4. P. 619-629. DOI: https://doi.org/10.46852/0424-2513.4.2022.28

22. Sheffi Y., Rice J. B. A supply chain view of the resilient enterprise. *MIT Sloan Management Review*. 2005. Vol. 47, No. 1. P. 41-48. URL: https://sloanreview.mit.edu/article/a-supply-chain-view-of-the-resilient-enterprise/ (accessed: 25.06.2026).

23. Stefani E., Costa I., Gaspar M. A., Goes R. de S., Monteiro R. C., Petrili B. R., Pereira A. de P. Information security risk framework for digital transformation technologies. *Systems*. 2025. Vol. 13, No. 1. Article 37. DOI: https://doi.org/10.3390/systems13010037

24. Urmston A., Song D., Lyons A. The development of risk assessments and supplier resilience models for military industrial supply chains considering rare disruptions. *Logistics*. 2024. Vol. 8, No. 2. Article 57. DOI: https://doi.org/10.3390/logistics8020057

25. U.S. Department of Defense. *The National Defense Industrial Strategy: Enabling a Modernized Defense Industrial Ecosystem* [Electronic resource]. 2024. URL: https://www.businessdefense.gov/NDIS.html (accessed: 25.06.2026).

26. Hellberg R., Lundmark M. Transformation in European defence supply chains as Ukraine conflict fuels demand. *Scandinavian Journal of Military Studies*. 2025. DOI: https://doi.org/10.31374/sjms.303

27. Lucas R., Ekstrom T., Fusaro P., Roer E. H., Retter L. *Toward Defense Supply Chain Disruption Management: A Research Agenda for Defense Supply Chain Resilience* [Electronic resource]. RAND Corporation, 2023. URL: https://www.rand.org/pubs/research_reports/RRA2504-1.html (accessed: 25.06.2026).

28. Sani S., Schaefer D., Milisavljevic-Syed J. Utilising digital twins for increasing military supply chain visibility. *Advances in Transdisciplinary Engineering*. 2022. Vol. 25. P. 225-232. DOI: https://doi.org/10.3233/ATDE220595

29. Linstone H. A., Turoff M. (eds.). *The Delphi Method: Techniques and Applications*. Reading, MA : Addison-Wesley, 1975. URL: https://web.archive.org/web/20080520015240/http://is.njit.edu/pubs/delphibook/ (accessed: 26.06.2026).

30. Saaty T. L. *The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation*. New York : McGraw-Hill, 1980.

31. Diakoulaki D., Mavrotas G., Papayannakis L. Determining objective weights in multiple criteria problems: The CRITIC method. *Computers & Operations Research*. 1995. Vol. 22, No. 7. P. 763-770. DOI: https://doi.org/10.1016/0305-0548(94)00059-H

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

67-79
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-5

UDC 339.138:339.13/.17
JEL Classification: L81, M31.

Received: 2026-07-12
Accepted: 2026-08-22
Published: 2026-08-30

Sibruk V.L. PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute." (Ukraine)

ORCID – 0000-0001-7997-5641
Researcher ID ACI-7107-2022
Scopus author id: – 57219598344
E-Mail: sibruk.viktor@edu.kpi.ua

Suvorova I.M. PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute. " (Ukraine)

ORCID – 0009-0004-7820-9856
Researcher ID
Scopus author id: –
E-Mail: suvorova.iryna@lll.kpi.ua

Yarmoliuk O.Ya. PhD in Economics, Docent, Associate Professor of Industrial Marketing Department National Technical University of Ukraine "Igor Sikorsky Kyiv Polytechnic Institute. " (Ukraine)

ORCID – 0000-0002-2156-3879
Researcher ID
Scopus author id: –
E-Mail: yarmoliuk.oleksii@lll.kpi.ua

MERCHANDISING TRANSFORMATION UNDER THE INFLUENCE OF TECHNOLOGICAL, COMPETITIVE AND CONSUMER FACTORS: A COMPREHENSIVE CONCEPT FOR RETAIL

Viktor Sibruk, Iryna Suvorova, Oleksii Yarmoliuk. "Merchandising transformation under the influence of technological, competitive and consumer factors: a comprehensive concept for retail". *The article examines the transformation of merchandising in the context of retail digitalization and intensifying competition. Based on an analysis of classical theories of retail format evolution, the necessity of rethinking traditional approaches to retail space organization with consideration of modern technological innovations is substantiated. Four groups of factors that comprehensively influence merchandising effectiveness are identified: technological, consumer, competitive, and economic. An integrated multi-factor model for evaluating merchandising effectiveness is proposed, which is intended to enable quantitative assessment of*

each factor group's contribution to overall retail performance. Practical tools for improving merchandising effectiveness are examined: basket analytics for identifying complementary products, including the use of large language models; checkout automation integrated with loyalty programs; and dynamic customer flow management across various functional zones of the retail space. Recommendations are developed for phased implementation of innovative solutions in retail enterprises, considering the specifics of various formats – from supermarkets to specialized hardware stores.

***Keywords**:* modern merchandising, retail trade, influencing factors, innovations, integrated multi-factor model

Віктор Сібрук, Ірина Суворова, Олексій Ярмолюк. "Трансформація мерчандайзингу під впливом технологічних, конкурентних та споживчих факторів: комплексна концепція для ритейлу". *У статті досліджується трансформація мерчандайзингу в умовах цифровізації роздрібної торгівлі та посилення конкуренції. На основі аналізу класичних теорій еволюції форм роздрібної торгівлі обґрунтовано необхідність перегляду традиційних підходів до організації торговельного простору з урахуванням сучасних технологічних інновацій. Визначено чотири групи факторів, що комплексно впливають на ефективність мерчандайзингу: технологічні , споживчі , конкурентні та економічні. Запропоновано інтегральну багатофакторну модель оцінки ефективності мерчандайзингу, яка має дозволити кількісно визначити внесок кожної групи факторів у загальну результативність торговельної діяльності. Розглянуто практичні інструменти підвищення ефективності мерчандайзингу: аналітику споживчого кошика для виявлення товарів-компліментів, зокрема з використанням великих мовних моделей; автоматизацію касових розрахунків та інтеграцію з програмами лояльності; динамічне управління потоком покупців у різних функціональних зонах торговельного закладу. Вироблені рекомендації щодо поетапного впровадження інноваційних рішень у діяльність підприємств роздрібної торгівлі з урахуванням специфіки різних форматів — від супермаркетів до спеціалізованих будівельних центрів.*

Ключові слова: сучасний мерчандайзинг, роздрібна торгівля, фактори впливу, інновації, інтегральна багатофакторна модель оцінки ефективності

Introduction. The current state of retail trade is characterized by a profound transformation driven not only by shifts in consumer behavior but also by the rapid advancement of technology. Retail is an industry that responds both to the slightest fluctuations in global processes and to changes in consumer preferences, under the influence of which modern retail is undergoing significant structural and institutional changes. According to forecasts by Wellbrock W. and Traumann Ch. [23], the coming decade can confidently be expected to bring changes unseen over the past fifty years. This dynamic necessitates a rethinking of established approaches to organizing retail space and customer interaction.

Despite considerable progress in the theoretical understanding of the evolution of retail formats, there is a substantial gap between established concepts (cyclical and environmental theories, conflict theory, and the Big Middle concept) and the contemporary challenges that retailers face in the field of merchandising. Classical theories, as rightly noted by Brown S. [3], offer a division into three groups: cyclical theories, related to economic cycles; environmental theories, pertaining to the operating environment; and conflict theory, which is based on the idea that institutional changes result from competitive behavior among retail organizations. It should be noted that classical theories, as emphasized by Fernie J., Fernie S. and Moore C. [6], reflect only the

general picture of the development of certain retail formats, without accounting for the influence of many environmental factors, particularly technological innovations, which are today reshaping the very nature of merchandising.

With regard to the integration of analytical tools for identifying complementary products and developing effective cross-category solutions, according to McArthur E., Weaven S., and Dant R.P. [12], existing theories remain disconnected from one another due to an overly narrow approach to the topic, and the overall understanding of retail functioning is composed of a multitude of heterogeneous variables.

Contemporary trends in the development of multichannel, cross-channel, and omnichannel strategies, alongside the persistence of traditional store-based and non-store retail formats, are creating a new reality to which existing theoretical frameworks must be adapted. Issues such as the automation of checkout processes, personalization of loyalty programs, and dynamic management of customer flow within the sales floor are gaining relevance [22]. Modern retail establishments typically seek to develop several formats and brands simultaneously, covering different segments of the consumer market, which complicates the application of traditional practices and calls for more flexible, adaptive approaches to retail space management. There is a growing need to systematize innovative merchandising approaches that take into account the specifics of various retail formats – from supermarkets to specialized outlets.

Analysis of recent studies and publications. In the field of basket analytics, Pan Y., Russell G., Gruca T. S., and Li C. recently developed the MVL (Multivariate logistic model) -Poisson model to account for the impact of marketing activities on visit frequency and cross-category dependencies between product categories [14]. Kumar et al. introduced an innovative approach to cross-category recommendations that combines traditional basket analysis with LLM (Large language model)-generated associations, enabling the proposal of novel, contextually relevant product combinations [8]. In the work of Basu S., the concept of "agentic commerce" is proposed – autonomous AI systems that go beyond generating recommendations and actively manage end-to-end retail processes, including dynamic pricing, assortment management, and operational orchestration in an omnichannel environment [2].

Contemporary research, particularly Kwak confirms the high effectiveness of implementing self-checkout systems, although they also reveal certain peculiarities in their usage, including longer transaction times with fewer items per basket compared to traditional checkout counters [9;20]. Current trends in POS (Point-of-sale) system development include integration with mobile applications, biometric authentication, and smart basket scanning [13]. According to an analytical report, loyalty programs are evolving into a key element of data-driven business models, where retail media function as a continuous optimization cycle. These capabilities enable higher basket efficiency, better retention, and increased revenue from Retail Media. [16].

Customer flow management has gained new momentum through RFID (Radio-frequency identification) technologies: Dey S., Lahon J., Boruah S. and Deka P. used RFID tags to visualize customer movement trajectories and identify the most and least visited zones within a store [5]. Sharma P., drawing on empirical A/B testing, confirmed the effectiveness of the "decompression zone" concept, demonstrating that customers need time to adapt to the store environment upon entry [19].

Identification of previously unresolved parts of the overall problem. Despite a considerable number of scholarly studies devoted to the evolution of retail formats, the practical aspects of implementing modern

67-79
v.38 (2026)
https://smart-scm.org

merchandising technologies remain insufficiently explored. Above all, further investigation is needed into how exactly technological innovations – electronic shelf labels, dynamic pricing systems based on demand elasticity, basket analytics tools for identifying complementary products, automated checkout integrated with loyalty programs, as well as RFID technologies for monitoring customer movement – affect the evolution of retail formats. This is particularly relevant across different formats, ranging from supermarkets to specialized hardware stores, where merchandising strategies differ substantially.

Furthermore, the issue of customer flow management across various functional zones of a retail establishment remains open. The concept of the "decompression zone" at the entrance, route optimization within the main sales floor, and the organization of the checkout area with its high impulse-purchase potential, while having practical applications, require theoretical generalization and empirical validation. The challenge of dynamic queue management during peak activity periods also remains unresolved. In addition, the differentiated effectiveness of loyalty programs depending on the retail format and consumer type has been insufficiently studied.

Formulation of the article's objectives. The purpose of this study is to develop theoretically grounded and practically oriented recommendations for improving merchandising in retail trade through the integration of modern technological innovations across various retail formats. The research is intended to bridge the gap between classic theoretical approaches to the evolution of retail formats and the contemporary challenges facing retailers in the context of digitalization, intensifying competition, and shifting consumer behavior.

Presentation of the main research material. The methods and forms of retail management are evolving rapidly within various conceptual frameworks, each with its own distinctive features, advantages, and limitations. For the purposes of this study, the most relevant approach appears to be the integration of environmental theory by Davies K., which emphasizes the adaptation of retail enterprises to changes in the macroenvironment, and the Big Middle concept described in the work of Levy M., Grewal D., Peterson R.A., Connolly B. [4;10]. The Big Middle concept structures the market into four segments, with the optimal one being precisely the middle segment – where retailers offer innovative products in a wide assortment at reasonable prices, and where innovative merchandising becomes particularly critical as one of the most significant factors in competitiveness. The influence of various factors on the formation of modern merchandising is presented in Figure 1.

The contemporary competitive environment of retail trade is characterized by unprecedented dynamism, compelling retailers to rethink traditional approaches to merchandising. Competition in retail can lead to paradoxical effects: instead of the expected price reductions, it stimulates assortment expansion and price increases, since a broader assortment becomes a strategy for attracting customers away from competitors and also allows for better segmentation of consumers with heterogeneous preferences. This creates new challenges for merchandising, which must ensure not only an attractive price but also a unique value proposition.

67-79
v.38 (2026)
https://smart-scm.org

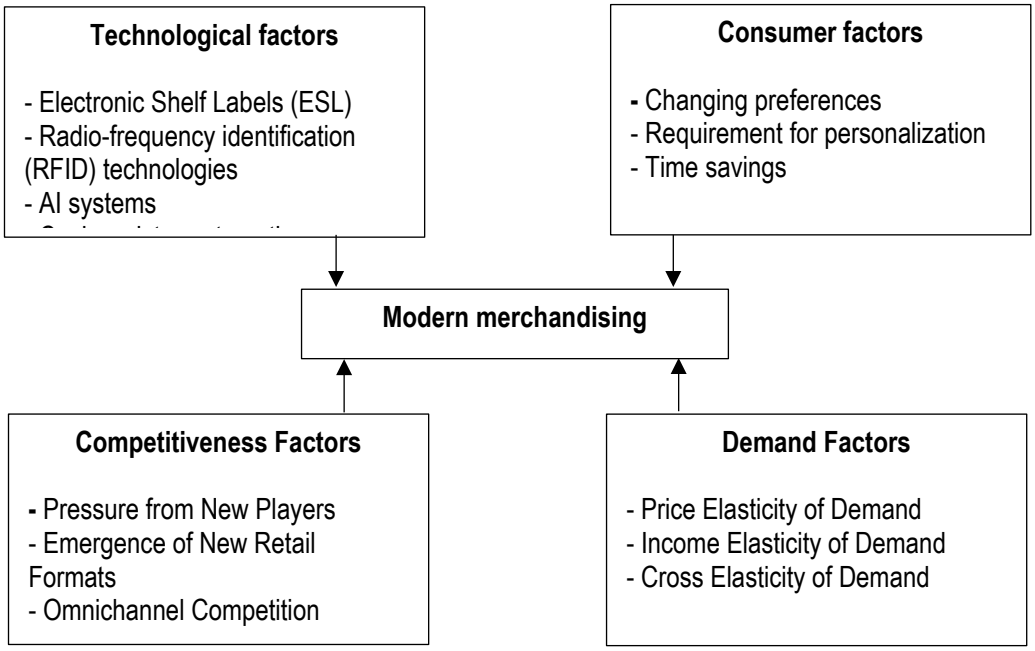


Figure 1- Integration model of factors influencing modern merchandising
Source: Developed by the authors based on [10; 6]

Pressure from new players significantly transforms merchandising strategies. The emergence of new competitors, especially discount formats, makes it critically important for incumbent retailers to develop unique service portfolios that protect against customer switching. Traditional retailers are forced to invest in additional services – from culinary studios to yoga studios – in order to create barriers to entry for new players. At the same time, unique services that are not duplicated by competitors demonstrate particular effectiveness: they foster customer loyalty to a specific store, reducing the likelihood of switching to a new player.

The emergence of new retail formats is changing the very logic of merchandising. For example, the showroom format, which is being actively implemented by online retailers, involves a fundamentally different organization of retail space: here, the customer does not purchase the product directly but gains an experience of interacting with the product, after which they place an order online. This necessitates a rethinking of the role of sales staff, product display, and navigation. In turn, traditional department stores are transforming from multi-category retail outlets into multi-brand, experience-oriented spaces where success is measured not only by sales per square meter but also by social media activity and the share of e-commerce.

Omnichannel competition is becoming a defining factor in modern merchandising. The blurring of boundaries between sales channels means that customers expect a seamless experience regardless of whether they are in a store, on a website, or in a mobile app [25]. This requires retailers to integrate online and offline merchandising—for example, through in-store recommendations of products that are available exclusively online, which creates synergy between channels and increases overall profitability. At the same time, competition from platforms such as Temu and TikTok is changing young shoppers' expectations regarding speed, price, and novelty of offerings, forcing traditional retailers to accelerate assortment updates and incorporate elements of "treasure hunting" into merchandising.

Competitive pressure also stimulates the adoption of technological innovations in merchandising. Research shows that retailers facing intense competition are more likely to

invest in digital tools for display and price management, as this enables more rapid responses to competitors' actions. This is particularly relevant for categories with high purchase frequency, where even small changes in price or assortment can significantly impact market shares.

Understanding the nature of demand and its sensitivity to various factors is a fundamental basis for making effective merchandising decisions. Modern retailers use elasticity analysis to optimize pricing policies, manage assortment, and improve overall sales efficiency [7].

Price elasticity of demand is one of the most important indicators determining consumer response to price changes. It can vary significantly across sales channels: specifically, own-price elasticity of demand in offline stores is higher in absolute value (on average –1.74) compared to the online channel (on average –0.87) [24]. This means that consumers in traditional stores are more sensitive to price changes, which is explained by higher search costs and a lesser ability to compare offers in real time. For modern merchandising, this implies the need for a differentiated approach to pricing depending on the sales channel, as well as the importance of using analytical tools to determine precise elasticity values at the level of individual products and stores [17].

Particular attention in merchandising practice is paid to KVIs (Key Value Items), which account for less than 10% of the assortment but determine consumers' perception of the overall price level of the entire store. As experts note, it is precisely these products that shape the retailer's price image: if prices on them are competitive, the customer extrapolates this impression to the entire store offering. Products belonging to this category typically have high price elasticity, as consumers are well aware of their market value and react sensitively to any changes. Price optimization for KVIs requires continuous monitoring of the competitive environment, seasonal fluctuations, and changes in consumer behavior, making them a critical element of strategic pricing.

Income elasticity of demand reflects the sensitivity of sales volume to changes in consumer income levels. Research empirically confirms that income elasticity varies depending on the type of product and retail format. In particular, an analysis of the Seoul market showed that a 1% increase in income leads to a 1.083% increase in supermarket sales, a 1.5% increase in restaurant sales, and a 2.184% increase in mobile phone store sales [18]. The lowest income elasticity is observed for essential goods, which form the core of the supermarket assortment, making this channel more resilient to economic fluctuations.

Cross-elasticity is critical for understanding the interrelationships between products in the assortment and for effective cross-merchandising planning. Research shows that cross-elasticity is higher in offline channels (on average 0.17) compared to online channels (0.04), indicating that consumers in physical stores are more inclined to search for substitute products in response to price changes [24]. This is explained by the fact that in a traditional store, the customer has invested time and effort in the visit, making them more inclined to purchase an alternative product in the same store rather than abandoning the purchase altogether.

Understanding cross-elasticity is the foundation of many merchandising strategies, in particular the use of loss leaders to drive traffic. As economists explain, selling certain products below cost or with minimal margin can be profitable because it increases cross-price elasticity of demand for other, higher-margin products. This strategy demonstrates the importance of considering interrelationships between products when formulating pricing policies and merchandising decisions.

For practical implementation of demand analysis, modern retailers use structural vector autoregressions (SVAR) and multiple price elasticity identification methods, which

67-79
v.38 (2026)
https://smart-scm.org

allow combining data with managerial insights about market functioning. This approach helps overcome endogeneity problems arising from the correlation between price and unobserved demand shocks, yielding more reliable estimates. In particular, studies on large samples of nearly 2,000 stores demonstrate that traditional methods often yield paradoxical positive price elasticity estimates that contradict the behavioral foundations of demand, whereas modern multiple identification approaches provide sufficient accuracy for practical use in pricing [17]. Merchandisers, faced with high uncertainty in elasticity identification, must continuously monitor the effectiveness of pricing strategies and be prepared to frequently adjust the marketing mix in response to the dynamics of market characteristics.

The comprehensive impact on modern merchandising can be viewed as a combination of four groups of factors, each of which must be taken into account when planning and developing product displays, pricing, and customer flow management. Technological factors provide the instrumental foundation for change, consumer factors determine the direction of these changes, competitive factors compel the acceleration of innovation adoption, and demand factors either constrain or stimulate particular solutions.

One of the effective tools of modern merchandising is Market Basket Analysis, which allows for the identification of stable pairs and groups of products that are purchased together (complementary goods) (Table 1). In contrast to the traditional intuitive approach, where sellers have a rough idea or assumption about which products "go well together," modern methods employ association rule mining algorithms, particularly the Apriori algorithm [1], which enables the quantitative assessment of three key metrics: support – the frequency with which an itemset appears in all transactions; confidence – the probability of purchasing item B given the purchase of item A; and lift – a measure of how much more often two items are purchased together than would be expected by chance.

Table 1. Application of complementary product analytics across retail formats

Retail Format	Typical Complementary Pairs	Placement Strategy	Expected Effect
Supermarket (FMCG)	Pasta + sauce; chips + beer; coffee + cream	Placement nearby or on separate "Dinner Idea" shelves	Increase in average transaction value by 15–25%
DIY (do-it-yourself) outlet	Tiles + adhesive + grout; paint + brush + masking tape	Problem-oriented grouping ("For the bathroom," "For walls")	Reduction of cognitive load; increase in sales of related products by 30%
Electronics Store	Laptop + case + mouse; phone + screen protector + case	Cross-merchandising on a single display stand	Higher margins through accessory sales
Pharmacy	Shampoo + conditioner; vitamins + probiotics	Placement nearby; "Buy two, get a discount" promotion	Increase in repeat purchases

Source: Developed by the authors based on [8]

Contemporary research, particularly the work of Kumar A., Pathak N., Agrawal A., Gupta R., and Gupta C, proposes the use of large language models (LLM) to identify new, non-obvious categories of complementary products. In contrast to classical basket

67-79
v.38 (2026)
https://smart-scm.org

analysis, which relies exclusively on historical purchase data, LLMs enable the generation of contextually relevant associations that extend beyond observed patterns [8]. An LLM can analyze textual product descriptions, customer reviews, and repair forums to suggest less obvious combinations – for example, a specialized joint sealant that is not purchased together with tiles but is logically related to them in the context of solving a specific task. This approach allows for going beyond observed data and creating new consumer value, opening up new opportunities for cross-category merchandising, particularly in specialized formats where consumers often come to solve a specific problem rather than to buy a single product.

The checkout area is a critical point of customer interaction that can either strengthen loyalty or ruin the positive impression of the entire store visit. Traditional queues at checkout counters, especially during peak hours, are one of the main reasons for purchase abandonment and reduced customer satisfaction. The solution to this problem lies in comprehensive automation, which includes several interrelated components. The first approach involves the implementation of self-checkout systems (SCO), which allow customers to scan and pay for goods independently. As evidenced by Decathlon's experience in transitioning to 100% self-service, this not only reduces queues but also enables the reallocation of cashiers to the role of sales floor consultants, thereby improving service quality. According to Decathlon Turkey, the introduction of self-checkout reduced waiting time in queues by 50% [11]. The effectiveness of self-checkout systems increases significantly when combined with smart basket scanners, where customers scan items directly while selecting them from the shelf and only pay for the already compiled receipt at the checkout.

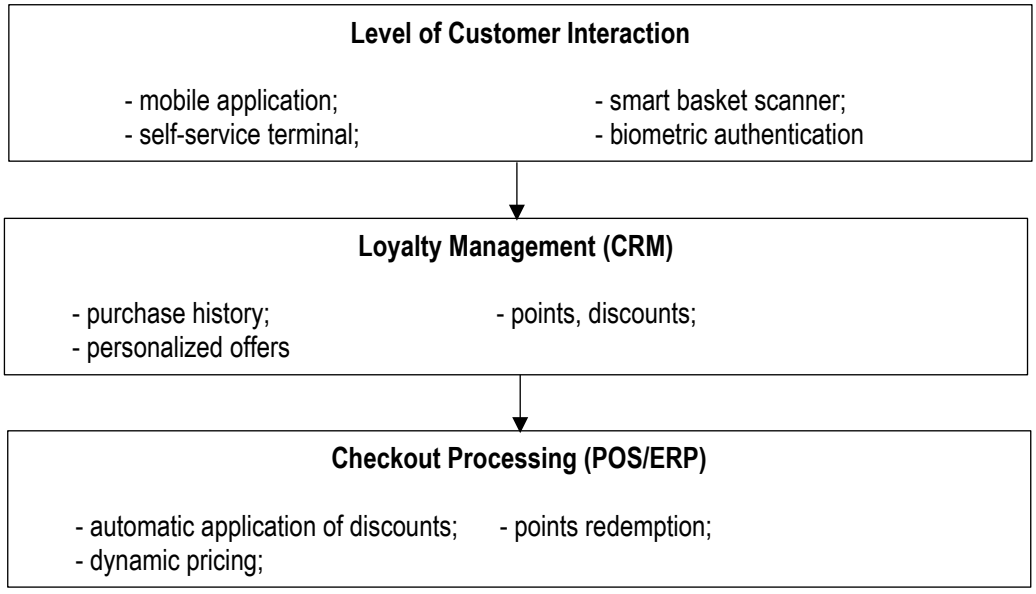


Figure 2 – Architecture of an integrated automation system for checkout and loyalty
Source: Developed by the authors

The second approach to optimizing service processes is the deep integration of point-of-sale (POS) systems with loyalty programs. Modern architecture enables automatic customer recognition (via mobile app, biometrics, or smart card), retrieval of their personalized offers, and automatic application of discounts without requiring

67-79
v.38 (2026)
https://smart-scm.org

any additional action on the part of the customer or the cashier (Fig. 2). This approach, known as "background loyalty," not only speeds up checkout but also creates a sense of care and a personalized approach.

Thirdly, automation enables the implementation of dynamic pricing directly at the checkout. This is particularly relevant for products with a short shelf life, where the system can automatically offer a discount on a product expiring today, or for stimulating sales during "dead hours." Electronic shelf labels (ESL) play a key role here, as they allow real-time synchronization of the price on the shelf and at the checkout, avoiding conflicts and confusion [21].

Effective management of customer movement within the store is one of the most underestimated reserves for increasing sales. Different zones of the retail space have different functional purposes and generate different revenue volumes, which requires a differentiated approach to their organization (Table 2).

Table 2. Characteristics of functional zones in a retail establishment

Zone	Share of Total Area	Share of Turnover	Primary Function	Key Products
Entrance Zone (Decompression)	2–5%	up to 10%	Forming the first impression, capturing attention	Seasonal items, new arrivals, emotional products
Main Zone (Sales Floor)	70–85%	75–85%	Core sales, navigation, selection	Planned purchase products (groceries, tiles, etc.)
Checkout Zone (Impulse)	<1%	up to 5%	Impulse purchasing	Small cheap items (batteries, gum, chocolate)

Source: Developed by the authors based on [19;5]

The entrance zone, referred to in academic sources as the "decompression zone," is the space where customers adapt to the store environment, shifting their attention from external stimuli to internal tasks. Research shows that shoppers often overlook the first display upon entry, as they need time to orient themselves within the space; therefore, placing key POS materials directly at the entrance may prove ineffective [19]. It is considered optimal to position the first display at a distance of 2–3 meters from the entrance door, after the customer has already oriented themselves toward the main sales floor. In the entrance zone, it is advisable to place seasonal items, new arrivals, and products that create an emotional atmosphere (flowers, fresh baked goods).

The main sales floor area should be organized to provide a logical traffic flow that covers the maximum number of product categories. The use of RFID technologies and CCTV (closed-circuit television) cameras with video analytics capabilities makes it possible to visualize actual customer movement trajectories, determine dwell time in various sections, and identify "cold zones" that customers tend to bypass [15]. The data obtained serves as the basis for store replanning, navigation optimization, and POS material placement. Of particular importance is the identification of so-called "dead

67-79
v.38 (2026)
https://smart-scm.org

corners" – areas with low foot traffic due to planning errors – and their correction through route adjustments or the placement of targeted-demand products in these zones.

Despite its small area, the checkout zone generates a significant volume of impulse purchases, which are based on different merchandising methods than those used in the main area. A customer standing in the checkout queue has already made their purchasing decision, calculated their budget, and did not plan any additional expenditures. Therefore, products in the checkout zone must meet several criteria: low price, small packaging, emotional appeal, and no need for lengthy selection.

For a comprehensive consideration of the factors influencing merchandising effectiveness, an integrated multi-factor model can be proposed that allows for the quantitative assessment of the contribution of each group and the calculation of a single integral indicator – the Merchandising Effectiveness Index (MEI). Similar approaches to constructing integral indices in the field of trade and services are used to assess the impact of various sales channels on customer satisfaction and business model efficiency.

The model is based on the assumption that each group of factors has a different weight depending on market specifics, store format, and current operating conditions. Weighting coefficients can be determined either through expert assessment or on the basis of empirical data – for example, through regression analysis of the relationship between factors and actual sales performance. For each group of factors, an aggregate indicator is calculated that combines several measurable indicators characterizing individual aspects of influence.

The calculation of the integral index can be performed as the sum of the products of weighting coefficients and the aggregate indicators of the corresponding factor groups. In turn, each group of factors is determined by functions for the respective factors.

The technological factors group may include: the electronic shelf label adoption index, defined as the share of product items equipped with electronic shelf labels in the total number of items; the RFID coverage index, which reflects the share of products identified using radio-frequency tags, enabling automated inventory management and product movement monitoring. The artificial intelligence usage index assesses the extent to which machine learning algorithms are applied for demand forecasting, dynamic pricing, and personalized recommendations. The checkout automation index is defined as the ratio of the number of self-checkout terminals to the total number of checkout terminals.

For consumer factors, the aggregate indicator may include the Customer Satisfaction Index, measured on the basis of surveys, review analysis, and return data. The Loyalty Program Penetration Index, calculated as the share of purchases made by loyalty program members in total turnover. The Service Time Index reflects the average time a customer spends at checkout, normalized relative to a target value.

Competitive factors may include: the Competitive Pressure Index, which assesses the number of new players in the market and their market share; the New Formats Emergence Index, which reflects the degree of penetration of alternative retail forms (discounters, showrooms, DTC channels); and the Omnichannel Index, which measures the integration of online and offline sales channels. The demand factors group may include elasticity coefficients calculated on the basis of statistical analysis of sales and price data, with subsequent normalization to a scale from 0 to 1 to ensure compatibility with other indicators.

Validation of the model should involve data collection for a group of stores that differ significantly in their level of technological equipment, calculation of the integral MEI indicator for each of them, and comparison with actual performance metrics (growth in

average transaction value, increase in impulse purchases, reduction in queue waiting time). The correlation coefficient between the MEI and the selected performance indicators allows for an assessment of the model's adequacy. At correlation coefficient values >0.7, the model can be considered suitable for practical use.

In addition to diagnosing the current state, the model should allow for simulation of various scenarios of changes in external conditions. For example, during a period of economic instability accompanied by a decline in household incomes, the weight of demand factors increases, which is reflected in the integral indicator and signals the need to reallocate resources in favor of flexible pricing tools and discounts for price-sensitive customer groups. Such modeling enables retail company managers to make informed management decisions under conditions of uncertainty.

From the practical recommendations for retail enterprises seeking to implement innovative approaches to merchandising, several strategies can be highlighted. First, the implementation of innovations can begin with the analysis of existing data. Most retailers already possess historical transaction data, which is an invaluable source for identifying complementary products. Even a simple basket analysis in Excel or Google Sheets can yield initial insights that allow for optimizing product displays and increasing cross-sales without additional investment in equipment. It is also worth considering a pilot implementation of electronic shelf labels in a specific category or in one of the network's stores. This would allow for assessing the real effect of dynamic pricing, testing customer response, and refining operational procedures before scaling up. It is advisable to start with categories with a short shelf life (fresh products) or seasonal items, where price sensitivity is highest.

Checkout automation can be combined with active communication with customers. Consumers often fear new technologies, so it is important to explain the benefits of self-service (speed, control over the process) and ensure the presence of support staff to assist with any issues. A positive experience with the technology is the best advertisement for attracting new users. Loyalty programs should be rethought as a data collection tool, not merely as a means of encouraging repeat purchases. Every transaction made by a loyal customer is information about their preferences, which can be used for personalizing offers, optimizing assortment, and managing inventory.

Conclusions.

The conducted research demonstrates that modern merchandising is undergoing a profound transformation driven by the integration of technological innovations, shifts in consumer behavior, and intensifying competition. Classical theories of retail format evolution, while conceptually significant, require supplementation with consideration of digital tools, without which they lose explanatory power in the contemporary retail environment. The analysis of four groups of factors – technological, consumer, competitive, and economic – confirms that their combined impact on merchandising is decisive for sales performance, and the proposed integrated MEI model enables quantitative assessment of each group's contribution and adaptation of management decisions to the specifics of various formats. The implementation of electronic shelf labels, self-checkout systems, and their integration with loyalty programs reduces service time, minimizes pricing errors, and creates a foundation for personalized offers. Customer flow management, including optimization of functional zones and dynamic queue regulation technologies, significantly improves operational efficiency and customer satisfaction. The use of large language models for identifying complementary products opens new opportunities for cross-category merchandising by generating associations based on semantic analysis of textual data. The practical value of the research lies in

recommendations for phased innovation implementation with continuous monitoring through the MEI model, enabling timely strategy adjustments in response to environmental changes. Future research should focus on calibrating the model's weighting coefficients based on empirical data from different markets and developing software tools for real-time monitoring.

References

1. Agrawal R., & Srikant R. (1994). Fast Algorithms for Mining Association Rules. In Proceedings of the 20th International Conference on Very Large Data Bases (VLDB '94) (pp. 487–499). Santiago, Chile. https://www.vldb.org/conf/1994/P487.PDF

2. Basu S. (2026). Agentic commerce applications: How autonomous AI is redefining the retail & e-commerce industry. International Journal of Computational and Experimental Science and Engineering, 12(1). https://doi.org/10.22399/ijcesen.5091

3. Brown S. (1987). Institutional Change in Retailing: A Review and Synthesis. European Journal of Marketing, 21(6), 5-36. https://www.emerald.com/ejm/article-abstract/21/6/5/33404/Institutional-Change-in-Retailing-A-Review-and?redirectedFrom=fulltext

4. Davies, K. (1998). Applying Evolutionary Models to the Retail Sector. The International Review of Retail, Distribution and Consumer Research, 8 (2), 165–181.

5. Dey S., Lahon J., Boruah S., & Deka P. (2024). Analyzing customer movement in retail stores using RFID and POS data for enhanced shopping experience. Journal of Theoretical and Applied Information Technology, 102(7), 3086-3095.

6. Fernie J., Fernie S., Moore C. (2015). Principles of Retailing. 2nd Edition. Abingdon, Oxon: Routledge. https://catalog.uttyler.edu/cgi-bin/koha/opac-detail.pl?biblionumber=914793&shelfbrowse_itemnumber=981095&__cf_chl_f_tk=nu3lm_4nN1dk4Fmj.YqCmDgHDnsSDkqXjz_UjVfdoK8-1782895795-1.0.1.1-cuDUQ0wor26sO9V9OuIn3rcd1ezRiZu.Tz7lQnbdv2g#shelfbrowser

7. Haschka, R. E., & Herwartz, H. (2025). Utilizing managerial beliefs for set identification of price elasticities of demand. Journal of Business Economics, 53, 1482–1505.

8. Kumar A., Pathak N., Agrawal A., Gupta R., & Gupta C. (2025). Beyond co-occurrence: LLM-based novel category discovery for e-commerce. arXiv, arXiv:2505.12718v2. https://arxiv.org/abs/2505.12718v2

9. Kwak J. K. (2020). Empirical Analysis on Comparison between Self-checkout and Regular Staffed-checkout lanes in a Poland Retail Store. International Journal of Advanced Culture Technology, 8(1), 56–61. https://koreascience.kr/article/JAKO202009759220175.pub

10. Levy M., Grewal D., Peterson R.A., Connolly B. (2005). The concept of the «Big Middle». Journal of Retailing, 81(2), 83-88.

11. Logo Software and Decathlon deliver a seamless customer experience in the cloud. (2023). https://perakende.org/logo-yazilim-ve-decathlondan-bulutta-kesintisiz-musteri-deneyimi/#content_skip_link_anchor

12. McArthur E.S., Weaven S., Dant R.P. (2016). The Evolution of Retailing. Journal of Macromarketing, 36(3), 272-286.

13. Miller C. (2025). Emerging Biometric Authentication at the Point of Sale Scorecard. https://javelinstrategy.com/research/2025-emerging-biometric-authentication-point-sale-scorecard

14. Pan Y., Russell G., Gruca T. S., & Li C. (2026). Multicategory purchase behavior: basket choice, shopping frequency, and promotional analysis. Journal of Retailing, 102(1), 44-62.

15. Pott J. (2024). Queue management for retailers: Customer convenience by respecting their time. EuroShop Magazine. https://origin-www.euroshop-tradefair.com/en/media-news/euroshopmag/retail-technology/queue-management-in-retail-for-greater-customer-convenience

16. Reeve J. (2026). Changing loyalty landscape: Here's what retail leaders need to know. https://www.retailbiz.com.au/contributor/changing-loyalty-landscape-heres-what-retail-leaders-need-to-know/

17. Rodrigues, A. (2025). Consumer Choice Over Shopping Baskets: A Linear Demand Approach. arXiv, arXiv:2511.11846. https://doi.org/10.48550/arXiv.2511.11846.

18. Seong E.Y., Chang G.C. (2017). A Study on the Impact of Income and Physical Location Characteristics on Retail Sales - Focusing on Restaurants, Supermarkets, and Mobile Phone Stores in Seoul. Real Estate Studies. vol.23, no.4, pp. 77-91. DOI : 10.19172/KREAA.23.4.6.

19. Sharma P. (2023). Decoding the Decompression Zone in Retail Stores. Indore Management Journal, 15(1), 35-48.

20. Sharma P, Ueno A., & Kingshott R. (2020). Self-service technology in supermarkets – Do frontline staff still matter? [Journal article]. Curtin University. https://curate.curtin.edu.au/articles/journal_contribution/31711852

21. Stamatopoulos I., Sanders R., & Bray R. (2025). Electronic Shelf Labels Have Not Led to Surge Pricing in US Grocery Retail, Despite Regulator Concerns. SSRN. https://doi.org/10.2139/ssrn.5271491

22. Verhoef P.C., Kannan P.K., Inman J.J. (2015). From Multi-Channel Retailing to Omni-Channel Retailing: Introduction to the Special Issue on Multi-Channel Retailing. Journal of Retailing, 91(2), 174-181. https://doi.org/10.1016/j.jretai.2015.02.005

23. Wellbrock W., Traumann Ch. (2012). Zukünftige Herausforderungen im Bereich des Handels. Chancen und Risiken ausgewählter Supply-Chain-Management-Konzepte. Discussion Papers on Logistics and Supply Chain Management. Philipps-Universität Marburg. Nr. 3. https://de.readkong.com/page/discussion-papers-on-logistics-and-supply-chain-management-6606075

24. Xingyue L. Zh., Haluk D. (2021). Between online and offline markets: A structural estimation of consumer demand. Information & Management. Volume 58, Issue 4. https://doi.org/10.1016/j.im.2021.103467

25. Yu J., Ren Y., & Zhou C. (2024). Strategic Interactions in Omnichannel Retailing: Analyzing Brand Competition and Optimal Strategy Selection. Journal of Theoretical and Applied Electronic Commerce Research, 19(4), 2557-2581.

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

80-88
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-4

UDC 339.37:338.24:004.9:005.52
JEL Classification: L81, M14, O32, Q01, L86.

Received: 2026-07-07
Accepted: 2026-08-22
Published: 2026-08-30

Dranus V.V. PhD in Economics, Associate Professor, Associate Professor of the Department of Finance and Credit, Petro Mohyla Black Sea National University, Mykolaiv (Ukraine)

ORCID – 0000-0001-5617-6740
Researcher ID PTE-5151-2026
Scopus author id: – 57216991567
E-Mail: drval8@ukr.net

Dranus L.S. PhD in Economics, Associate Professor, Associate Professor of the Department of Management, Petro Mohyla Black Sea National University, Mykolaiv (Ukraine)

ORCID – 0000-0002-6427-1315
Researcher ID IAM-4250-2023
Scopus author id: – 57216993629
E-Mail: lyuba_melnichuk@ukr.net

Prokopyshyn O.S. PhD in Economics, Associate Professor, Associate Professor of the Department of Accounting and Taxation, Stepan Gzhytskyi National University of Veterinary Medicine and Biotechnologies Lviv (Ukraine)

ORCID – 0000-0002-7027-3499
Researcher ID GXM-8717-2022
Scopus author id: – 57929185900
E-Mail: os378@ukr.net

INFORMATISATION AND DIGITALISATION OF BUSINESS PROCESSES AS TOOLS FOR THE STRATEGIC MANAGEMENT OF LOGISTICS ACTIVITY AND SUSTAINABLE DEVELOPMENT OF TRADE ENTERPRISES

Valentyn Dranus, Liubov Dranus, Oksana Prokopyshyn. "Informatisation and digitalisation of business processes as tools for the strategic management of logistics activity and sustainable development of trade enterprises". *The study examines informatisation and digitalisation of business processes as integrated tools of strategic logistics management in trade enterprises operating under conditions of military risk, supply chain instability, and accelerating European integration. The research combines a systematic synthesis of scholarly literature on digital platforms, regulatory governance, and sustainable supply chains with conceptual modelling used to formalise the relationships identified. Unlike approaches that treat digitalisation mainly as a means of automating operations and cutting costs, the analysis demonstrates its system-forming role in reshaping the architecture of logistics management, integrating business processes, and*

building digital trade ecosystems; digital platforms are shown to simultaneously lower traditional market-entry barriers and generate new strategic dependencies for enterprises joining established ecosystems, while technologies such as the Internet of Things, Big Data Analytics, and cloud solutions create competitive advantage only when embedded within a coherent management architecture. The regulatory dimension, anchored in European Union digital-services legislation, is found to transform compliance from a technical obligation into a source of strategic advantage for enterprises that adapt proactively. On this basis, the study proposes an original Digital-Sustainable Logistics Strategy that integrates three equally weighted dimensions - efficiency, resilience, and environmental, social, and governance–oriented responsibility - into a unified strategic management architecture, with digitalisation positioned as a system-forming factor of strategic sustainability rather than an auxiliary operational tool, linking digital transformation, regulatory compliance, and sustainability outcomes within a single decision-making framework. The results offer a methodological basis for designing corporate digital transformation programmes and sustainability-oriented logistics strategies, with further research needed on the environmental and social effects of logistics digitalisation and on the post-war restructuring of digital logistics ecosystems in Ukraine.

***Keywords**:* digital platforms, supply chain resilience, digital ecosystems, regulatory compliance, competitive advantage, ESG responsibility

Валентин Дранус, Любов Дранус, Оксана Прокопишин. "Інформатизація та цифровізація бізнес-процесів як інструменти стратегічного управління логістичною діяльністю та сталим розвитком торговельних підприємств". *В дослідженні розглянуто інформатизацію та цифровізацію бізнес-процесів як інтегровані інструменти стратегічного управління логістикою торговельних підприємств, що функціонують в умовах воєнних ризиків, нестабільності ланцюгів постачання та прискорення європейської інтеграції. Дослідження ґрунтується на системному узагальненні наукової літератури щодо цифрових платформ, регуляторного управління та сталих ланцюгів постачання в поєднанні з концептуальним моделюванням, застосованим для формалізації виявлених взаємозв'язків. На відміну від підходів, що трактують цифровізацію переважно як засіб автоматизації операцій і скорочення витрат, аналіз демонструє її системоутворюючу роль в трансформації архітектури логістичного управління, інтеграції бізнес-процесів та побудові цифрових торговельних екосистем; показано, що цифрові платформи одночасно знижують традиційні бар'єри входу на ринок і породжують нові стратегічні залежності для підприємств, що приєднуються до вже сформованих екосистем, тоді як такі технології, як Інтернет речей, Big Data Analytics та хмарні рішення, забезпечують конкурентну перевагу лише за умови їх вбудованості в цілісну управлінську архітектуру. Встановлено, що регуляторний вимір, закріплений в законодавстві Європейського Союзу про цифрові послуги, перетворює комплаєнс із технічного обов'язку на джерело стратегічної переваги для підприємств, що діють на випередження. На цій основі запропоновано оригінальну Цифрово-сталу логістичну стратегію, що інтегрує три рівнозначні виміри: ефективність, стійкість та ESG-орієнтовану відповідальність в єдину архітектуру стратегічного управління, в якій цифровізація позиціонується як системоутворюючий фактор стратегічної сталості, а не допоміжний операційний інструмент, поєднуючи цифрову трансформацію, регуляторну відповідність та результати сталого розвитку в межах єдиної системи прийняття рішень. Отримані результати становлять методологічну основу для розроблення корпоративних програм цифрової трансформації та логістичних стратегій, орієнтованих на сталий розвиток, а подальші дослідження мають зосередитися на оцінці екологічних і соціальних ефектів цифровізації логістики та повоєнній реструктуризації цифрових логістичних екосистем в Україні.*

Ключові слова: цифрові платформи, стійкість ланцюгів постачання, цифрові екосистеми, регуляторна відповідність, конкурентна перевага, ESG-відповідальність

80-88
v.38 (2026)
https://smart-scm.org

Introduction. The full-scale war, the global digital transformation of the economy, and the growing instability of supply chains have fundamentally altered the operating conditions of trade enterprises. The destruction of transport and logistics infrastructure, supply disruptions, shortages of specific resources, cyber threats, rising logistics costs, and the need for rapid adaptation to a continuously changing external environment have substantially intensified the requirements placed on strategic logistics management systems. Under these conditions, the informatisation and digitalisation of business processes cease to be tools of purely technological modernisation or the automation of individual operations. They are transformed into a strategic resource that ensures business continuity, the resilience of logistics systems, rapid managerial decision-making, adaptability to crisis situations, and the formation of long-term competitive advantages.

Despite the rapid development of digital technologies and a substantial body of scholarly research, the prevailing approach in the contemporary literature continues to view digitalisation predominantly through the lens of operational efficiency gains, cost reduction, the automation of logistics processes, inventory optimisation, and faster order processing. At the same time, its strategic functions remain insufficiently studied, in particular its role in shaping adaptive management models, strengthening the resilience of logistics systems to military, economic, and technological shocks, transforming competitive relationships, developing digital trade ecosystems, integrating ESG principles, and ensuring the sustainable development of enterprises. These issues are of particular relevance to Ukraine, where military risks, the imperative of post-war economic recovery, and integration into the European digital space require a reconceptualisation of digitalisation, not merely as a technological factor but as a strategic driver of enterprise development. It is precisely the need to formulate a coherent concept of strategic logistics management grounded in informatisation, digitalisation, and sustainable development principles that defines the scientific problem addressed in this study.

The transformative impact of digital platforms on traditional market structures has been examined by Oluka (2024), who established that digitalisation substantially lowers market entry barriers and fosters economic inclusion, while simultaneously generating new challenges for regulation and market participant protection. Gilardi (2022) demonstrated that effective governance of digital technologies requires adaptive, forward-looking, and internationally coordinated regulatory approaches capable of anticipating change rather than merely reacting to it. The regulatory dimension of digital trade in the EU is codified in the Digital Services Act (European Commission, 2022), which establishes new standards of platform accountability. The interrelationship between digital transformation, strategic sustainability, and sustainable development has been investigated by Prokopyshyn et al. (2026, 2024). Among international studies, particular significance attaches to research on sustainable logistics (Bag et al., 2019), digital business ecosystems (Bohnsack et al., 2024; Veile et al., 2020), and data management and digital platform operation (Guo et al., 2020; Qadri et al., 2025; Nozari et al., 2021; Sestino et al., 2020; Chen et al., 2015; Teece, 2018; vom Brocke et al., 2016). Notwithstanding this substantial body of research, the question of formulating a digital-sustainable logistics strategy for trade enterprises that integrates informatisation, ESG principles, and strategic sustainability into a single concept remains insufficiently developed and only partially systematised.

The purpose of this article is to substantiate the conceptual foundations of

informatisation and digitalisation of business processes as an integrated instrument of strategic logistics management for trade enterprises in the context of ensuring their sustainable development, by demonstrating the systemic impact of digitalisation on market structures, the regulatory environment, and the ESG dimension of logistics strategy. To achieve this purpose, the study examines the following research tasks: to synthesise the theoretical foundations of digital platform impact on market structures and regulatory governance; to identify the mechanisms through which digitalisation generates verifiable sustainability outcomes in logistics; and to develop an original conceptual model that integrates digital transformation, strategic resilience, and ESG-oriented management into a unified logistics strategy framework.

Theoretical framework.

Understanding informatisation and digitalisation of business processes as instruments of strategic logistics management in trade enterprises requires moving beyond conventional technological conceptions toward a comprehensive examination of their impact on the transformation of market structures, the regulatory environment, and the implementation of ESG principles.

Oluka (2024) established that digital platforms fundamentally alter the market structures of trade through reduced transaction costs, network effects, and the emergence of new business models. For trade enterprises, this translates into lower barriers to market entry, intensifying competitive pressure from platform aggregators such as Amazon and Alibaba, and the emergence of new forms of logistics relationships among trade enterprises, suppliers, and consumers. Importantly, digitalisation is not solely a threat to traditional trade formats but also a strategic opportunity: enterprises that build their own digital ecosystems or actively integrate into existing platform ecosystems gain access to new markets and logistics networks without a proportional increase in operating costs (Bohnsack et al., 2024; Veile et al., 2020). Research on omnichannel retailing confirms that the integration of physical and digital channels constitutes an important determinant of trade enterprise competitiveness (Radomska et al., 2025).

Gilardi (2022) demonstrated that effective governance of digital technologies requires adaptive, forward-looking, and internationally coordinated regulatory approaches that evolve in tandem with technological progress. The principal regulatory benchmark for trade enterprises oriented toward EU markets is the Digital Services Act (European Commission, 2022), which establishes requirements regarding platform accountability, the transparency of algorithmic recommendations, and data protection. Its implementation directly affects the operating conditions of trade enterprises' logistics systems: requirements concerning product traceability, the protection of customers' personal data, and supply chain transparency become mandatory standards rather than voluntary practices. For domestic trade enterprises seeking integration into EU markets as part of the European integration process, this creates new requirements for the digital architecture of logistics systems and for strategic management.

Research in the field of sustainable logistics (Bag et al., 2019) and digital transformation (Qadri et al., 2025; Nozari et al., 2021) reveals an inseparable connection between a trade enterprise's level of digital maturity and its capacity to comply with ESG principles. Digitalisation facilitates ESG compliance through specific mechanisms. In the environmental dimension, route optimisation through transport management systems and artificial intelligence reduces mileage and CO_2 emissions, automated inventory management lowers the level of surplus stock and waste, and digital document workflows eliminate paper-based documentation. Within the social dimension, omnichannel trade increases product

accessibility, digital platforms foster transparent working conditions throughout supply chains (Oluka, 2024; Radomska et al., 2025), and the development of staff digital competencies enhances their competitiveness in the labour market. The governance dimension is supported by digital controlling and KPI monitoring that increase the transparency and accountability of managerial decisions, blockchain that verifies ESG commitments throughout the supply chain, and data analytics that enable accessible public ESG reporting.

RESULTS AND DISCUSSION. The analysis of the reviewed scholarly sources allows for several generalisations that directly underpin the authors' concept. First, the studies of Oluka (2024) and Gilardi (2022) jointly demonstrate that digitalisation exerts a systemic effect on market structures along two simultaneous trajectories: a disruptive one, eroding traditional entry barriers and redistributing market power in favour of platform aggregators, and a constructive one, opening opportunities to build proprietary digital ecosystems and enter new markets without a proportional increase in costs. Teece (2018) refines this logic by pointing to the dual nature of platforms: they simultaneously confer advantages on early adopters and create new strategic dependencies for those entering already established ecosystems. This implies that the strategic choice between developing a proprietary platform and integrating into an external one is a decisive determinant of a trade enterprise's long-term competitive position. Second, the analysis of research on data management (Chen, Preston, & Swink, 2015; Sestino et al., 2020) and digital business ecosystems (Bohnsack et al., 2024; Veile et al., 2020) confirms that the technological basis of digitalisation, namely the Internet of Things, Big Data Analytics, cloud solutions, and AI-driven optimisation, loses its strategic value outside the context of business processes and organisational architecture. Digital tools generate competitive advantage only when embedded within a coherent management system with clearly defined processes, accountability, and performance metrics (vom Brocke, Zelt, & Schmiedel, 2016). Third, the synthesis of research on sustainable logistics (Bag, Gupta, & Foropon, 2019; Qadri et al., 2025; Nozari et al., 2021) and omnichannel trade (Radomska et al., 2025) confirms that the measurable impact of digitalisation on sustainability indicators is substantial and empirically verified: AI-based route optimisation reduces the transport carbon footprint by 10–15 per cent, automated inventory management reduces spoilage-related waste by 20–30 per cent, and Big Data Analytics-based digital reporting reduces the cost of ESG reporting preparation by 40–60 per cent (Bohnsack et al., 2024). These effects are not automatic; they materialise only when digital systems are purposefully designed with ESG objectives in mind. Fourth, the EU regulatory vector embodied in the Digital Services Act (European Commission, 2022) and examined by Gilardi (2022) transforms digital compliance from a technical requirement into a strategic competitive advantage: enterprises that proactively adapt to requirements concerning supply chain traceability, data protection, and algorithmic transparency gain a time advantage over competitors who wait for the formal introduction of regulatory obligations. Prokopyshyn et al. (2024, 2026) substantiate that precisely this proactive adaptation to regulatory change constitutes one of the key mechanisms for building strategic sustainability under conditions of digital economic transformation and wartime uncertainty.

A defining conclusion common to all the reviewed studies is that none of the effects identified above is achieved through the isolated adoption of an individual technology or compliance with a single regulatory requirement. Realising the potential of digitalisation requires the systemic integration of the technological, regulatory,

and value-based dimensions within a unified management architecture. It is precisely this conclusion that constitutes the starting point for the authors' Digital-Sustainable Logistics Strategy (DSLS) concept.

The DSLS concept rests on three equally weighted strategic dimensions, each of which is necessary but insufficient without the other two. The first dimension, efficiency, defines digitalisation as a source of operational advantage: reduced transaction costs, accelerated logistics cycles, improved demand-forecasting accuracy, and inventory optimisation through the integration of transport management systems, warehouse management systems, and AI-driven analytics. The second dimension, resilience, treats digitalisation as the foundation of resilience, that is, the capacity of logistics systems to maintain functionality under military risk, supply chain disruption, and global uncertainty through decentralised management, channel redundancy, and end-to-end information transparency. The third dimension, responsibility, positions digitalisation as an instrument for implementing ESG principles, ranging from automated carbon accounting and digital document workflows to the blockchain-based verification of social commitments across supply chains and public ESG reporting underpinned by Big Data Analytics. These three dimensions are not sequential stages but operate concurrently, reinforcing one another: efficiency gains free up resources for ESG investment; resilience ensures the continuity of ESG commitments even under crisis conditions; and ESG responsibility enhances reputational resilience and broadens access to international capital markets, which, in turn, finances the further development of digital infrastructure (vom Brocke, Zelt, & Schmiedel, 2016). To visualise the internal logic of the DSLS concept and the interrelationships among its elements, a conceptual model has been developed, presented in Figure 1.

The conceptual model presented in Figure 1 reflects the authors' approach to formulating a Digital-Sustainable Logistics Strategy for a trade enterprise, integrating the digitalisation of business processes, the strategic management of logistics activity, and ESG principles within a single decision-making system. Unlike existing models that predominantly emphasise individual digital technologies or the automation of logistics processes, the proposed model treats digitalisation as a strategic mechanism for ensuring the enterprise's long-term sustainability under conditions of high uncertainty, military risk, European integration transformations, and intensifying sustainable development requirements.

The novelty of the proposed model lies in the integration of three mutually reinforcing strategic components, namely digital transformation, strategic sustainability, and ESG-oriented management, within a single conceptual architecture of logistics management. Unlike conventional approaches, in which digitalisation performs an auxiliary function with respect to the automation of operational processes, in the proposed model it acts as a system-forming factor that ensures the continuity of logistics system operation, adaptability to changes in the external environment, informational transparency, the speed of managerial decision-making, and improved coordination among all supply chain participants. At the same time, ESG principles are integrated not as a separate corporate responsibility track but as a constituent element of strategic management that determines the environmental, social, and governance performance of digital transformation. The concluding element of the conceptual model is the block of strategic results, which demonstrates the anticipated effects of the comprehensive implementation of the Digital-Sustainable Logistics Strategy. Unlike existing models, which predominantly assess the effectiveness of digitalisation through isolated operational or financial indicators,

80-88
v.38 (2026)
https://smart-scm.org

the proposed approach reflects a comprehensive strategic outcome that combines enhanced competitiveness, the assurance of strategic sustainability, the adaptability of logistics systems to military and other crisis risks, integration into the European digital space, compliance with Digital Services Act and ESG requirements, and the achievement of long-term sustainable development. This allows the model to be applied not only as a conceptual foundation for the digital transformation of logistics, but also as a practical instrument for shaping strategic managerial decisions, determining priorities for investment in digital technologies, evaluating the effectiveness of digitalisation, and planning the development of a trade enterprise under conditions of high uncertainty.

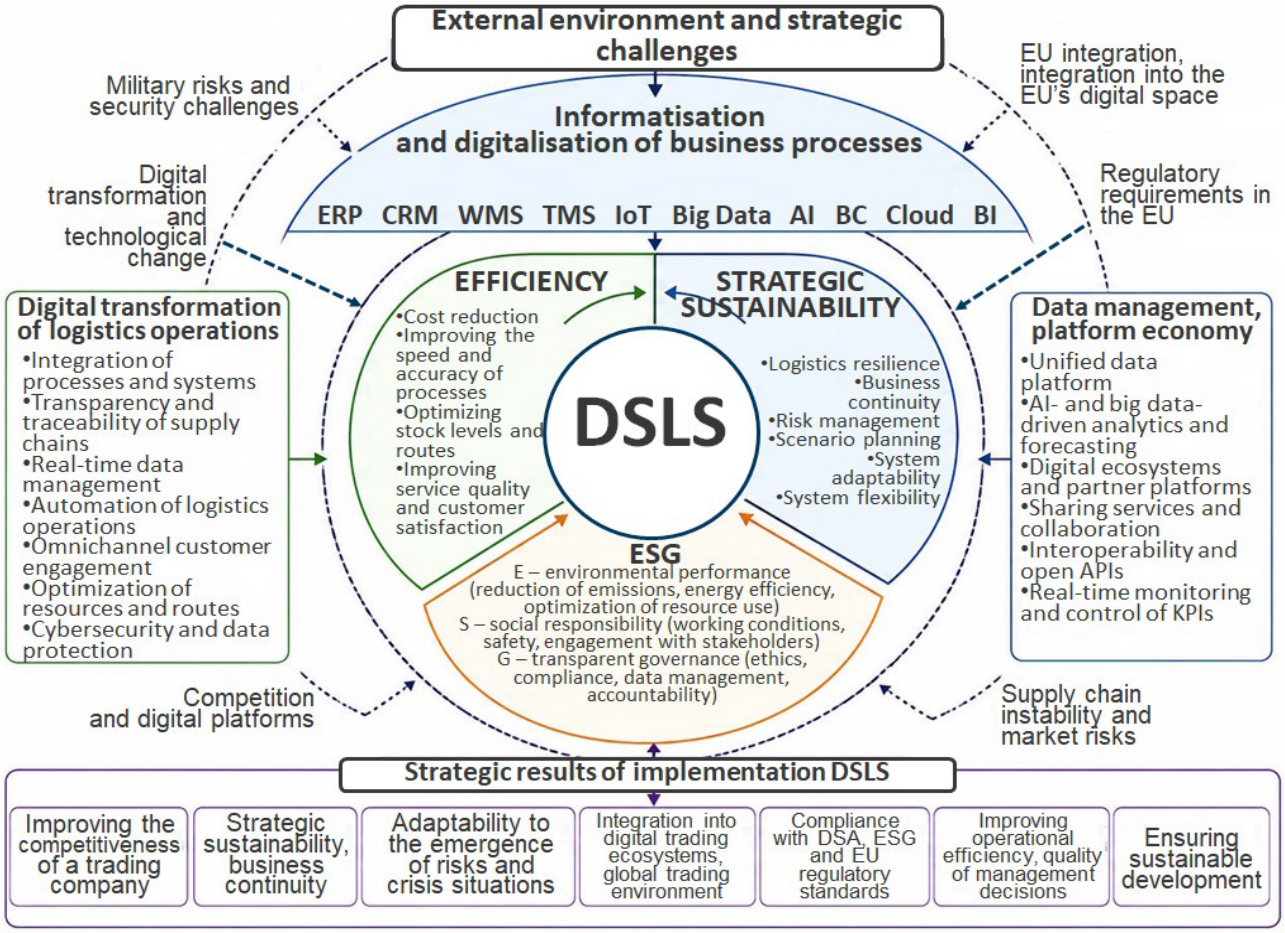


Figure 1-Conceptual model of the integration of ESG principles and digitalisation into the logistics strategy of a trade enterprise (DSLS)
Source: developed by the authors.

The practical value of the proposed model lies in its potential use as a methodological foundation for the formulation and implementation of trade enterprises' logistics strategies. Its application would enable a systematic assessment of the relationship among digital technologies, the effectiveness of logistics processes, the level of strategic sustainability, and sustainable development indicators; the identification of priority directions for digital modernisation; an increase in enterprises' adaptability to crisis and wartime challenges; the minimisation of logistics risks; compliance with

European regulatory requirements (the Digital Services Act, ESG, and supply chain traceability requirements); and the formation of long-term competitive advantages. In addition, the model may serve as a conceptual basis for designing corporate digital transformation programmes, constructing systems of strategic key performance indicators, and assessing the effectiveness of logistics digitalisation in the context of achieving sustainable development goals.

Conclusions.

The study substantiates that the informatisation and digitalisation of business processes constitute an integrated strategic instrument that simultaneously transforms the operational efficiency of logistics processes, the market structures of trade, the regulatory environment, and the mechanisms for ensuring the sustainable development of trade enterprises. Unlike approaches that reduce digitalisation to the automation of operations or the adoption of individual technological solutions, the proposed Digital-Sustainable Logistics Strategy (DSLS) concept integrates three strategic dimensions, namely efficiency, resilience, and social responsibility, within a unified system of strategic management.

It has been established that the regulatory dimension of digitalisation is an independent strategic factor that directly determines the parameters of the digital architecture of logistics systems, rather than merely an external constraint on enterprise activity. For Ukrainian trade enterprises pursuing European integration, proactive adaptation to EU digital regulatory requirements is a source of strategic competitive advantage. The research purpose formulated in the Introduction, namely to substantiate the conceptual foundations of digitalisation as integrated tools of strategic logistics management oriented toward sustainable development, has been achieved through the synthesis of the theoretical foundations of digital platform impact and the development of the DSLS conceptual model.

Directions for further research include the development of methodological tools for assessing the ESG effects of trade enterprises' logistics digitalisation; the formulation of a practical mechanism for adapting logistics strategies to EU regulatory requirements within the European integration process; and the examination of the impact of digital platforms on the restructuring of domestic trade enterprises' logistics chains following the cessation of hostilities.

References

1. Bag, S., Gupta, S., & Foropon, C. (2019). Examining the role of dynamic remanufacturing capability on supply chain resilience in circular economy. Management Decision, 57(4), 863–885. https://doi.org/10.1108/MD-07-2018-0724

2. Bohnsack, R., Rennings, M., Block, C., & Bröring, S. (2024). Profiting from innovation when digital business ecosystems emerge: A control point perspective. Research Policy, 53(3), Article 104961. https://doi.org/10.1016/j.respol.2024.104961

3. Chen, D. Q., Preston, D. S., & Swink, M. (2015). How the use of big data analytics affects value creation in supply chain management. Journal of Management Information Systems, 32(4), 4–39. https://doi.org/10.1080/07421222.2015.1138364

4. European Commission. (2022). Digital Services Act. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act

5. Gilardi, F. (2022). Digital technology, politics, and policy-making. Cambridge University Press. https://doi.org/10.1017/9781108887304

6. Guo, S., Choi, T. M., & Shen, B. (2020). Green Product Development under Competition: A Study of the Fashion Apparel Industry. European Journal of Operational Research, Vol.10 No.4, 280, 523-538. https://doi.org/10.1016/j.ejor.2019.07.050

7. Nozari, H., Szmelter-Jarosz, A., & Ghahremani-Nahr, J. (2021). The Ideas of Sustainable and Green Marketing Based on the Internet of Everything-The Case of the Dairy Industry. Future Internet, 13(10), 266. https://doi.org/10.3390/fi13100266

8. Oluka, A. (2024). The impact of digital platforms on traditional market structures. Technology Audit and Production Reserves, 2(4/76), 21–29. https://doi.org/10.15587/2706-5448.2024.303462

9. Prokopyshyn, O., Dranus, L., & Dranus, V. (2024). Strategic sustainability of e-commerce enterprises under global digital transformation. Efficient Economy, 9. http://doi.org/10.32702/2307-2105.2024.9.32

10. Prokopyshyn, O., Trushkina, N., Dranus, V., & Dranus, L. (2026). Strategic sustainability as the basis of competitiveness and sustainable development of economic entities in the digital age. Financial Space, 2(60), 135–148. https://doi.org/10.30970/fp.2(60).2026.135147148

11. Qadri U.A., Moustafa A.M.A, & Waqas M. (2025). Sustainable supply chain excellence: how technology integration, CSR/SDG engagement and environmental stewardship drive competitive advantage. Journal of Enterprise Information Management, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/JEIM-03-2025-0190

12. Radomska, J., Kawa, A., Hajdas, M., Klimas, P., & Silva, S.C. (2025). Unveiling retail omnichannel challenges: developing an omnichannel obstacles scale. International Journal of Retail & Distribution Management, Vol. 53 No. 13 pp. 1–20, doi: https://doi.org/10.1108/IJRDM-04-2024-0169

13. Sestino, A., Prete, M. I., Piper, L., & Guido, G. (2020). Internet of Things and Big Data as enablers for business digitalization strategies. Technovation, 98, Article 102173. https://doi.org/10.1016/j.technovation.2020.102173

14. Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world. Research Policy, 47(8), 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015

15. Veile, J. W., Kiel, D., Müller, J. M., & Voigt, K. I. (2020). Lessons learned from Industry 4.0 implementation in the German manufacturing industry. Journal of Manufacturing Technology Management, 31(5), 977–997. https://doi.org/10.1108/JMTM-08-2018-0270

16. vom Brocke, J., Zelt, S., & Schmiedel, T. (2016). On the role of context in business process management. International Journal of Information Management, 36(3), 486–495. https://doi.org/10.1016/j.ijinfomgt.2015.10.002

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

89-99
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-6

UDC 351.86:004.8
JEL Classification: H56, H83, O33.

Received: 2026-07-12
Accepted: 2026-08-20
Published: 2026-08-30

Dabizha V.V. PhD in Public administration, Associate Professor, Associate Professor of the Department of International Relations and Political Consulting, HEI "Open International University of Human Development "UKRAINE" (Ukraine)

ORCID – 0000-0002-7000-4635
Researcher ID GPX-2585-2022
Scopus author id: – 57218620866
E-Mail: verynchik@ukr.net

Nekriach A.I. Doctor of Political Science, Professor, Professor of the Department of International Relations and Political Consulting, HEI "Open International University of Human Development "UKRAINE" (Ukraine)

ORCID – 0000-0001-5058-4145
Researcher ID JDM-2733-2023
Scopus author id: – 57226269387
E-Mail: anastasian1947@gmail.com

ARTIFICIAL INTELLIGENCE IN THE ACTIVITIES OF THE SECURITY AND DEFENSE FORCES OF UKRAINE: PUBLIC AND ADMINISTRATIVE ASPECT

Vira Dabizha, Anastasiia Nekriach "Artificial intelligence in the activities of the security and defense forces of Ukraine: public and administrative aspect". *The article examines the use of artificial intelligence in the activities of Ukraine's security and defence forces from the perspective of public administration. It is substantiated that, under conditions of digital transformation, increasing volumes of information, and a more complex security environment, artificial intelligence is becoming not only a technological tool but also an instrument for information and analytical support of management processes in the field of national security and defence. The functional roles of the security forces and defence forces are distinguished, and the specific features of AI application are identified in accordance with the competences and tasks of individual actors. The main areas of artificial intelligence use in the activities of the Armed Forces of Ukraine and other components of the defence forces, the National Guard of Ukraine, the State Border Guard Service of Ukraine, the Security Service of Ukraine, intelligence agencies, the National Police of Ukraine, civil protection forces, and cybersecurity and cyber defence actors are systematised. The information and analytical, monitoring, forecasting, planning, coordination, and management decision-support functions of AI are identified. Particular attention is paid to the potential of artificial intelligence to facilitate interagency interaction, integrate relevant data, develop shared situational awareness, and improve the timeliness of responses to complex threats to national security. The necessity of distinguishing between the output generated by an AI system and a management decision is substantiated. It is argued that artificial intelligence should be*

89-99
v.38 (2026)
https://smart-scm.org

regarded as an intelligent tool for supporting public management decisions, while final decision-making and responsibility for its consequences should remain with the authorised public authority or official. Prospective areas for further integration of artificial intelligence into the public administration system of Ukraine's security and defence forces are identified.

***Keywords**:* artificial intelligence, public administration, security forces, defence forces, security and defence sector, national security, management decisions, interagency interaction, information and analytical support, digital transformation

Віра Дабіжа, Анастасія Некряч «Штучний інтелект у діяльності сил безпеки і оборони України: публічно-управлінський аспект». *У статті досліджено використання штучного інтелекту в діяльності сил безпеки і оборони України з позицій публічного управління. Обґрунтовано, що в умовах цифрової трансформації, зростання обсягів інформації та ускладнення безпекового середовища штучний інтелект набуває значення не лише технологічного засобу, а й інструменту інформаційно-аналітичного забезпечення управлінських процесів у сфері національної безпеки і оборони. Розмежовано функціональне призначення сил безпеки та сил оборони та визначено особливості застосування технологій ШІ відповідно до компетенції і завдань окремих суб'єктів. Систематизовано основні напрями використання штучного інтелекту у діяльності Збройних Сил України та інших складових сил оборони, Національної гвардії України, Державної прикордонної служби України, Служби безпеки України, розвідувальних органів, Національної поліції України, сил цивільного захисту та суб'єктів кібербезпеки і кіберзахисту. Виокремлено інформаційно-аналітичну, моніторингову, прогностичну, планувальну, координаційну функції ШІ та функцію підтримки прийняття управлінських рішень. Особливу увагу приділено потенціалу штучного інтелекту у забезпеченні міжвідомчої взаємодії, інтеграції релевантних даних, формуванні спільної ситуаційної обізнаності та підвищенні оперативності реагування на комплексні загрози національній безпеці. Обґрунтовано необхідність розмежування результату функціонування системи ШІ та управлінського рішення. Доведено, що штучний інтелект доцільно розглядати як інтелектуальний інструмент підтримки публічно-управлінських рішень, тоді як остаточне рішення та відповідальність за його наслідки мають залишатися за уповноваженим суб'єктом. Визначено перспективні напрями подальшої інтеграції ШІ в систему публічного управління силами безпеки і оборони України.*

Ключові слова: штучний інтелект, публічне управління, обороноздатність, сили безпеки і оборони, сектор безпеки і оборони, національна безпека, управлінські рішення, міжвідомча взаємодія, інформаційно-аналітичне забезпечення, цифрова трансформація

Introduction. The development of artificial intelligence is one of the key determinants of the contemporary digital transformation of public administration systems and, at the same time, has a significant impact on the nature of national security and defence provision. The ability of artificial intelligence systems to process large volumes of heterogeneous data, identify patterns, detect potential threats, model possible scenarios, and provide information and analytical support for decision-making creates new opportunities for the activities of security and defence sector actors. Accordingly, artificial intelligence is gradually becoming not only a technological tool but also an important element of modern management processes in the security and defence domain.

For Ukraine, these processes are of particular importance in the context of the full-scale armed aggression of the Russian Federation, the hybrid nature of contemporary threats, the highly dynamic

security environment, and the need to make management decisions under severe time constraints and considerable information uncertainty. Modern confrontation takes place simultaneously across military, information, cyber, technological, and other domains, which significantly increases the volume of information requiring analysis and complicates the processes of forecasting, planning, and coordinating the activities of relevant public institutions.

Under these conditions, the use of artificial intelligence technologies is becoming one of the factors enhancing the capacity of the security and defence forces to detect threats in a timely manner, assess risks, analyse changes in the operational environment, and provide information support for management decision-making. The potential of AI can be realised in intelligence and analytical activities, situational awareness, cybersecurity, state border protection, critical infrastructure protection, logistics, threat forecasting, the operation of unmanned systems, information security, and other areas of activity of the security and defence forces.

At the same time, the use of artificial intelligence in this field should not be limited exclusively to the introduction of individual technological solutions. From the perspective of public administration, the integration of AI capabilities into the system of management relations is of fundamental importance. Such a system encompasses the delineation of actors' competences, the organisation of information exchange, interagency interaction, coordination of activities, formulation of management decisions, monitoring of their implementation, and evaluation of their effectiveness.

Another specific feature of the issue is that the security forces and defence forces, while constituting components of Ukraine's security and defence sector, have different functional purposes. However, under contemporary conditions, addressing a significant proportion of security challenges requires their systematic interaction. Threats to national security are increasingly complex in nature and are not confined to the area of responsibility of a single public authority. This necessitates interagency data exchange, interoperability of information systems, harmonisation of analytical procedures, and the establishment of a shared information environment.

It is in this context that artificial intelligence can be regarded as an instrument for strengthening both horizontal and vertical interaction among security and defence sector actors. The integration of data from various sources, their automated analysis, and the timely provision of relevant information to the appropriate levels of management can reduce the time between threat detection and decision-making, enhance situational awareness, and enable a more informed allocation of forces and resources.

At the same time, the proliferation of AI is transforming the traditional mechanism of management decision-making. In the classical management model, the decision-maker receives information, analyses it, identifies alternatives, and makes a decision. The application of artificial intelligence, however, introduces an additional information and analytical layer between the acquisition of primary data and the formulation of a management decision. Algorithmic systems can preprocess information, identify hidden patterns, assess risks, forecast possible scenarios, and generate recommendations for an authorised official.

This provides grounds for considering AI as an intelligent tool for supporting public management decisions in the security and defence domain rather than as an independent decision-making actor. The final decision, particularly where it may entail legal, security-related, or other socially significant consequences, should remain within the competence and responsibility of the authorised actor. Based on the above, the technological advantages of AI must be

combined with the fundamental principles of public administration, namely legality, accountability, responsibility, and the controllability of management activities.

A relevant scientific task is therefore to conduct a comprehensive study of the use of artificial intelligence in the activities of Ukraine's security and defence forces specifically from the perspective of public administration. This requires identifying the system of actors involved in such use, systematising the main areas of AI application, determining its role in the performance of management functions, examining the potential of intelligent technologies for interagency coordination, and substantiating their impact on the mechanisms for preparing, making, and implementing management decisions in the field of national security and defence.

Analysis of recent research and publications. The issue of the use of artificial intelligence in the field of national security and defence has received increasing attention in recent years in both Ukrainian and international academic research. Scholars primarily focus on the practical applications of AI technologies, their use in the military domain, ensuring state security and cybersecurity, the automation of specific processes, threat forecasting, and decision-making support.

S. Hurzhii examines the role and significance of artificial intelligence technologies in the military-technical sphere, analyses global trends in their application, the specific features of AI use by armed forces, as well as the associated risks and threats. The research conducted by S. Bielai, V. Hladkov, O. Pivnenko, D. Pokhodenko, and M. Skliar is also important for the issues under consideration, as the authors substantiate conceptual directions for the implementation of artificial intelligence to meet the needs of Ukraine's security and defence sector. The researchers propose an approach to establishing nationwide, departmental, and interagency artificial intelligence platforms and emphasise the need for cooperation among the defence forces, public institutions, the academic community, and civilian technology developers.

In turn, Yu. Danyk, A. Dykyi, V. Shestakov, and R. Shyrshov provide a comprehensive analysis of the possibilities for the implementation and use of artificial intelligence to meet the needs of Ukraine's security and defence sector. The authors examine the application of AI in cybersecurity, critical infrastructure protection, information operations, and other areas of national security. Particular attention is paid to the need to establish an effective system for managing AI implementation processes, ensuring the safety of its use, managing risks, training personnel, and applying human-machine models.

V. Hmyria, V. Korniienko, and M. Styshuk examine the organisational and legal foundations for the use of artificial intelligence in the field of state security, including law enforcement activities. In their research, they focus on the legislative framework governing the use of AI, issues of responsibility, personal data protection, cybersecurity, and compliance with ethical principles in the application of relevant technologies.

Thus, existing academic research provides a sufficient theoretical foundation for identifying the technological, military, security, organisational, and legal aspects of artificial intelligence use. At the same time, the application of AI specifically from the perspective of public administration of Ukraine's security and defence forces remains insufficiently systematised. In particular, further research is required into the system of actors involved in the use of AI, its management functions, the possibilities for ensuring interagency information and analytical interaction, and the impact of AI technologies on the processes of preparing, making, and implementing management decisions in the field of national security and defence.

89-99
v.38 (2026)
https://smart-scm.org

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the public administration principles governing the use of artificial intelligence in the activities of Ukraine's security and defence forces, to determine its functional role within the national security system, and to reveal the potential of AI as a tool for information and analytical support, interagency coordination, and enhancing the soundness of management decision-making.

Presentation of the main results. The study of the use of artificial intelligence in the activities of the security and defence forces requires, first and foremost, determining the place of the relevant actors within the overall system of ensuring Ukraine's national security. This approach is of fundamental methodological importance, since the concepts of the "security and defence sector", "security forces", and "defence forces" are not identical, and treating them as equivalent complicates the identification of management functions and areas of application of AI technologies [13].

According to the Law of Ukraine "On National Security of Ukraine", the security and defence sector constitutes a system comprising public authorities, the Armed Forces of Ukraine, other military formations, law enforcement and intelligence agencies, state bodies of special purpose with law enforcement functions, civil protection forces, the defence-industrial complex, and other entities defined by law whose activities are aimed at protecting Ukraine's national interests from threats [13].

According to the legislation, the structure of the sector comprises four interconnected components: the security forces; the defence forces; the defence-industrial complex; and citizens and public associations that voluntarily participate in ensuring national security. Therefore, the security forces and defence forces should not be regarded as synonymous concepts but rather as functionally distinct yet interconnected components of a unified national security system.

Under the legislation, the security forces are defined as law enforcement and intelligence agencies, state bodies of special purpose with law enforcement functions, civil protection forces, and other bodies entrusted with functions related to ensuring national security. The defence forces comprise the Armed Forces of Ukraine, other military formations, law enforcement and intelligence agencies, and state bodies of special purpose with law enforcement functions that are entrusted with functions related to ensuring the defence of the state [14].

Such a regulatory distinction indicates that whether a particular actor belongs to the security forces or the defence forces is determined not only by its institutional status but primarily by the nature of the functions it performs. Moreover, certain actors may perform tasks both within the security forces and as part of the defence forces, depending on the applicable legal regime, the nature of threats, and the tasks assigned to them. A notable example is the National Guard of Ukraine, which in peacetime forms part of the security forces and performs law enforcement functions, while simultaneously developing the capabilities required to perform tasks as part of the defence forces.

From the perspective of public administration, this specific feature is directly relevant to determining the model for the use of artificial intelligence. AI does not operate independently of the competence of the respective public authority. The areas of its application should be determined by the functional purpose of the respective actor, the nature of the tasks assigned to it, the type of information being processed, the level of the management decision, and the potential consequences of such a decision [15].

In this regard, it is appropriate to distinguish between the institutional and functional dimensions of artificial intelligence application. The institutional dimension characterises the range of bodies and

structures that use, implement, coordinate, or support the functioning of AI systems. The functional dimension reflects the specific management tasks for which the relevant technologies are applied, including monitoring, analysis, forecasting, planning, coordination, resource allocation, information support, and decision-making support [3].

It is the functional approach that makes it possible to explain why the same artificial intelligence technology may serve different management purposes. For example, computer vision technologies may be used by the defence forces to analyse the operational environment and recognise objects, by border guard units to monitor the state border, by law enforcement agencies to perform security tasks defined by law, and by civil protection actors to assess the consequences of emergencies. The technological basis may be similar; however, the management purpose, legal regime governing data, level of risk, and responsibility of the respective actors differ significantly [1].

In this context, the concept of the management function of AI becomes particularly important. This does not imply granting artificial intelligence any public authority or decision-making powers; rather, it involves identifying those stages of the management process at which AI technologies can enhance the speed, completeness, and soundness of the activities of public administration actors [6].

In our view, six main functional areas of AI use can be distinguished in the activities of the security and defence forces:

1. information and analytical – automated processing of large volumes of structured and unstructured data, their systematisation, identification of interrelationships, and generation of analytical information;

2. monitoring – continuous observation of changes in the security environment, information and cyberspace, as well as the condition of individual facilities and systems;

3. forecasting – identification of trends, risk assessment, forecasting of potential threats, and modelling of possible scenarios for the development of a situation;

4. planning – information support for strategic, operational, and resource planning, identification of alternative courses of action, and assessment of their potential consequences;

5. coordination – facilitating the rapid exchange of relevant information among actors, harmonising data from different sources, and creating a shared information environment;

6. management decision-making support – generating analytical assessments, forecasts, and possible alternatives for subsequent decision-making by the authorised actor.

This classification demonstrates that, from the perspective of public administration, the greatest potential of AI lies not in replacing humans in the management process, but in reducing the time between receiving primary information and formulating a well-founded decision [2]. This is particularly important in the field of national security and defence, where time itself often constitutes an independent factor in management effectiveness.

At the same time, it should be taken into account that the application of artificial intelligence changes the traditional configuration of information flows. Under the classical model, information sequentially passes through individual organisational levels, units, and officials, at each of which it is summarised, analysed, and transmitted to the next level [9]. Where a large number of actors are involved, such a model may lead to duplication of information, delays in its transmission, and institutional fragmentation.

The use of AI technologies potentially enables a transition towards an integrated model in which data from different sources are combined within a shared information

89-99
v.38 (2026)
https://smart-scm.org

and analytical environment, processed automatically, and provided to the relevant management actor in accordance with its competence [10]. Within such a model, AI does not function as an independent management centre but rather as a technological element that facilitates information exchange between different stages of the management cycle.

Therefore, interagency coordination becomes critically important. Contemporary threats to national security are characterised by their interconnected nature and their ability to manifest simultaneously across military, information, cyber, economic, and social domains. Accordingly, the effectiveness of responses increasingly depends on the capacity of public institutions not only to collect their own data but also to promptly integrate them with information obtained from other actors, develop a shared understanding of the security environment, and coordinate management actions.

In this context, artificial intelligence can serve as an integrative element within the information and analytical framework of interagency interaction, facilitating the processing of heterogeneous data and their transformation into information suitable for use at the relevant level of management. However, establishing such an integrated framework requires not only the technological interoperability of systems but also a clear delineation of powers, rules governing access to information, responsibility for data quality, procedures for data exchange, and appropriate oversight mechanisms [12].

The public administration approach to the use of artificial intelligence in the activities of the security and defence forces therefore requires AI to be considered not as an isolated technology but as an integral component of the management cycle, embedded within a system of actors, functions, information flows, and interagency interaction.

Table 1. Functional Areas of Artificial Intelligence Use in the Activities of Ukraine's Security and Defence Forces

Subjects / Functional Area	Prospective Areas of AI Use	Management Functions	Expected Management Effect
Armed Forces of Ukraine and other components of the Defence Forces	analysis of the operational environment; processing of intelligence data; computer vision; unmanned and robotic systems; forecasting; logistics	analysis; forecasting; planning; organisation; decision-making support	enhanced situational awareness; reduced information processing time; resource optimisation; increased timeliness of decision-making
National Guard of Ukraine	analysis of the security environment; monitoring; protection of designated facilities; use of unmanned systems; data analysis while performing tasks as part of the Defence Forces	monitoring; analysis; forecasting; coordination; decision-making support	integration of security and defence capabilities; more rapid response; improved coordination efficiency
State Border Guard Service of Ukraine	intelligent monitoring of the state border; analysis of photo and video data; anomaly detection; risk forecasting; unmanned monitoring	monitoring; risk identification; forecasting; control	enhanced effectiveness of border control; early detection of threats; optimisation of the use of forces and resources
Security Service of Ukraine and intelligence agencies	analysis of large datasets; identification of relationships and patterns; threat analysis; information-analytical and counterintelligence support	analysis; forecasting; risk assessment; information support for decision-making	early detection of threats; improved quality of analytical information; enhanced forecasting capacity
National Police of Ukraine	intelligent data analytics; analysis of information resources as provided by law; support for situational analysis; risk identification	monitoring; analysis; forecasting; organisation of response measures	faster response; more efficient use of resources; enhanced situational awareness

89-99
v.38 (2026)
https://smart-scm.org

State Emergency Service of Ukraine and civil protection forces	forecasting of emergencies; analysis of the consequences of destruction; monitoring of hazardous areas; analysis of geospatial information; resource planning	forecasting; planning; coordination; control	early identification of risks; optimisation of response measures; increased effectiveness of rescue operations
Cybersecurity and cyber defence actors	automated anomaly detection; cyber threat analysis; forecasting of cyberattacks; detection of malicious activity	monitoring; analysis; forecasting; prevention	faster detection of cyber incidents; enhanced cyber resilience; reduced response time
Strategic and interagency governance bodies	data integration; scenario modelling; strategic forecasting; assessment of complex risks	strategic analysis; planning; coordination; control	development of a comprehensive picture of the security environment; enhanced evidence-based strategic decision-making

Source: systematised by the author.

The systematisation presented in Table 1 provides grounds for asserting that the use of artificial intelligence in the activities of the security and defence forces is characterised by a cross-sectoral and interagency nature. Despite differences in the competences of the respective actors, a common management logic of AI application can be identified, encompassing data acquisition and processing, detection of potential threats, risk assessment, forecasting of situational developments, formulation of alternative scenarios, and provision of information support for management decision-making.

At the same time, the most significant differences between the use of AI by the security forces and the defence forces are manifested not so much at the level of the technologies themselves as in the objectives of their application and the nature of management tasks. For the defence forces, the primary focus is on the use of AI technologies to ensure national defence, enhance situational awareness, support planning, intelligence, logistics, and military management decision-making. For the security forces, priority areas include threat detection and prevention, state border protection, ensuring state and public security, cybersecurity, civil protection, and critical infrastructure protection [11].

At the same time, the contemporary nature of threats is gradually reducing the possibility of a clear organisational separation between these areas of activity. A cyberattack on critical infrastructure, an information operation, sabotage activities, or a combined attack may simultaneously require the involvement of actors with different competences [4]. Consequently, the effectiveness of AI application depends not only on the technological capabilities of an individual authority but also on the state's capacity to ensure effective interagency information exchange and interaction.

On this basis, it is proposed to distinguish three levels of artificial intelligence use within the public administration system of security and defence.

The first is the institutional level, at which AI technologies are used by an individual actor in accordance with its competence and functional purpose. At this level, internal processes of information collection, processing and analysis, forecasting, and planning are automated and enhanced through intelligent technologies.

The second is the interagency level, at which AI facilitates the analytical integration of information generated by different actors within the security and defence forces. Its purpose is to overcome institutional fragmentation of information, develop shared situational awareness, and provide information and analytical support for coordinated responses to complex threats.

The third is the strategic level, at which the results of intelligent analysis are used to assess threats to national security, conduct scenario-based forecasting, support strategic

89-99
v.38 (2026)
https://smart-scm.org

planning, determine state priorities, and assist decision-making by the highest public authorities in the field of national security and defence

The proposed three-level approach makes it possible to consider AI not as a set of isolated technological solutions applied by different public authorities, but as a potential element of an integrated information and analytical management framework in the field of security and defence.

One of the key challenges of public administration in the field of national security is the need to coordinate a significant number of institutions, each of which generates its own information resources, exercises powers defined by law, and uses respective departmental systems. Under such conditions, the mere availability of large volumes of data does not guarantee an improvement in the quality of governance [5]. Of crucial importance is the capacity to transform heterogeneous data into relevant information in a timely manner and to ensure its use by the actor authorised to make the respective decision.

The traditional model of interagency interaction is largely based on the sequential transmission of information between authorities and levels of management. Under crisis conditions, such a model may result in time delays, duplication of analytical work, and the formation of different assessments of the same security situation [7]. Artificial intelligence technologies potentially make it possible to transform this approach through the automated integration, structuring, and analysis of information from various sources [8].

From the perspective of public administration, the result of such a transformation should not be the centralisation of all information within a single authority, but rather the establishment of an integrated information and analytical framework in which each actor retains its legally defined competence, while technological interaction ensures the necessary level of data exchange and shared situational awareness.

Accordingly, the functioning of such a framework can be represented by the following sequence: data sources → departmental information systems → integration of relevant data → intelligent processing → threat detection → risk assessment → scenario forecasting → identification of competent actors → management decision support → interagency coordination → response → evaluation of results

A fundamental feature of the proposed approach is that artificial intelligence is positioned within the information and analytical, rather than the authoritative decision-making, segment of the system. AI may perform analysis and forecasting, rank risks, and generate alternatives; however, it does not acquire the status of a public administration actor and does not substitute for the competence of a public authority or an authorised official.

The public administration value of artificial intelligence lies not only in its ability to process information more rapidly. Of considerably greater importance is its potential to transform interaction among security and defence forces from a predominantly departmental model of information support towards an integrated model of situational awareness, coordination, and management decision support.

The analysis demonstrates that the public administration potential of artificial intelligence in the activities of Ukraine's security and defence forces is determined not only by the technological possibilities of its application but, above all, by its capacity to be integrated into management processes, provide information and analytical support, enhance situational awareness, and facilitate interagency coordination. At the same time, the use of AI technologies does not alter the subjectivity of public administration: management decision-making and responsibility for its consequences must

remain with the respective public authority or authorised official. Therefore, AI should be regarded as a tool for enhancing analytical capacity and management effectiveness in the field of security and defence rather than as a substitute for the actor exercising management functions.

Conclusions.

The study has demonstrated that the use of artificial intelligence in the activities of Ukraine's security and defence forces should be considered not only as a direction of technological development but also as an important component of the transformation of public administration in the field of national security and defence. AI has the potential to enhance the information and analytical capabilities of public administration actors, accelerate data processing, threat detection and risk assessment, as well as support forecasting and management decision-making.

The main management functions of artificial intelligence in the activities of the security and defence forces have been systematised, including information and analytical, monitoring, forecasting, planning, coordination, and management decision-support functions. It has been established that specific areas of AI application are determined by the functional purpose, competence, and nature of the tasks performed by the respective actor.

The use of AI is of particular importance in ensuring interagency interaction between the security and defence forces. The integration and intelligent analysis of relevant data can contribute to the development of shared situational awareness, reduce information fragmentation, and improve the timeliness of coordination and response to complex threats to national security.

Artificial intelligence should be regarded as an intelligent tool for supporting public management decisions rather than as an independent management actor. The final decision and responsibility for its consequences should remain with the authorised public authority or official. Prospects for further research are associated with the development of an organisational and functional mechanism for integrating AI technologies into the public administration system of Ukraine's security and defence forces, as well as with improving mechanisms for interagency information and analytical interaction.

References

1. Boulanin, V., Saalman, L., Topychkanov, P., Su, F., & Peldán Carlsson, M. (2020). Artificial intelligence, strategic stability and nuclear risk. Stockholm International Peace Research Institute. Retrieved from: https://www.sipri.org/publications/2020/policy-reports/artificial-intelligence-strategic-stability-and-nuclear-risk

2. European Parliament & Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

3. Korniienko, V., Hmyria, V., & Styshuk, M. (2025). Organizational and legal principles of use of artificial intelligence in the field of state security. Honor and Law, 1(92), 59–69. DOI: https://doi.org/10.33405/2078-7480/2025/1/92/332039. Retrieved from: https://chiz.nangu.edu.ua/article/view/332039

4. National Security Commission on Artificial Intelligence. (2021). Final report. National Security Commission on Artificial Intelligence. Retrieved from: https://www.dwt.com/-/media/files/blogs/artificial-intelligence-law-advisor/2021/03/nscai-final-report--2021.pdf

5. NATO. (2024). Summary of NATO's revised artificial intelligence (AI) strategy. Retrieved from: https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy

6. Sayler, K. M. (2020). Artificial intelligence and national security (CRS Report R45178). Congressional Research Service. Retrieved from: https://www.congress.gov/crs-product/R45178

7. Taddeo, M., Ziosi, M., & Tsamados, A. (2022). Artificial intelligence for national security: The predictability problem. Centre for Emerging Technology and Security, The Alan Turing Institute. Retrieved from: https://cetas.turing.ac.uk/publications/artificial-intelligence-national-security-predictability-problem

8. U.S. Department of Defense. (2022). Responsible artificial intelligence strategy and implementation pathway. U.S. Department of Defense. Retrieved from: https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Responsible%20AI%20Strategy%20and%20Implementation%20Pathway.pdf

9. Hurzhii, S. V. (2024). Trends in the application of artificial intelligence technologies in the military-technical sphere. Information and Law, 3(50). DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311713. Retrieved from: https://il.ippi.org.ua/article/view/311713

10. Husak, Yu. A., Kitik, S. V., & Kanduiev, D. V. (2023). Modern aspects of the use of artificial intelligence by the Armed Forces of Ukraine under martial law. Current Issues of National Jurisprudence, (2), 91–95. DOI: https://doi.org/10.32782/39221475

11. Danyk, Yu., Dykyi, A., Shestakov, V., & Shyrshov, R. (2025). Analysis and substantiation of the introduction and use of artificial intelligence for the needs of the security and defence sector of Ukraine. Society and Security, 6(12), 64–76. DOI: https://doi.org/10.26642/sas-2025-6(12)-64-76. Retrieved from: https://sas.ztu.edu.ua/article/view/349744

12. Pivnenko, O., Hladkov, V., Bielai, S., Skliar, M., & Pokhodenko, D. (2025). Substantiation of conceptual directions for the implementation of artificial intelligence for the needs of the security and defence sector of Ukraine. Society and Security, 3(9), 48–55. DOI: https://doi.org/10.26642/sas-2025-3(9)-48-55. Retrieved from: https://sas.ztu.edu.ua/article/view/334358

13. Verkhovna Rada of Ukraine. (2018). On National Security of Ukraine: Law of Ukraine No. 2469-VIII of June 21, 2018. Bulletin of the Verkhovna Rada of Ukraine, (31), Art. 241. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19

14. President of Ukraine. (2021). On the Decision of the National Security and Defense Council of Ukraine of March 25, 2021 "On the Military Security Strategy of Ukraine": Decree of the President of Ukraine No. 121/2021 of March 25, 2021. Retrieved from: https://zakon.rada.gov.ua/laws/show/121/2021

15. Cabinet of Ministers of Ukraine. (2020). On approval of the Concept for the Development of Artificial Intelligence in Ukraine: Order No. 1556-r of December 2, 2020. Retrieved from: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

100-110
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-7

UDC 351.86:004.8:005.21
JEL Classification: H56, H83, O33.

Received: 2026-07-18
Accepted: 2026-08-28
Published: 2026-08-30

Volska O.M. Doctor of Science in Public Administration, Professor, Professor of the Department of Public Administration and Local Self-Government, Kherson National Technical University, Khmelnytskyi, (Ukraine)

ORCID – 0000-0001-5047-4579
Researcher ID
Scopus author id: – 57201896051
E-Mail:

ARTIFICIAL INTELLIGENCE AS A TOOL FOR ENHANCING THE GOVERNANCE CAPACITY OF UKRAINE'S SECURITY AND DEFENCE FORCES

Olena Volska "Artificial intelligence as a tool for enhancing the governance capacity of Ukraine's security and defence forces". *The article examines artificial intelligence as a tool for enhancing the management capacity of Ukraine's security and defence forces. It is substantiated that, under conditions of increased risk, time constraints, incomplete information, adversarial interference and rapidly changing operational environments, the effectiveness of the relevant actors largely depends on the speed of data processing, the quality of forecasting, the coordination of actions and the timeliness of management decisions. The authors propose defining the management capacity of Ukraine's security and defence forces as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. Its structure comprises institutional, information and analytical, forecasting, planning, coordination and adaptive capacities, as well as the capacity to adopt and implement decisions. The article presents an AI-supported management cycle encompassing data acquisition, information verification and integration, situational analysis, threat identification, risk assessment, forecasting, the development of courses of action, decision-making and monitoring of decision implementation. The information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions of AI, together with its decision-support function, are systematised. It is emphasised that artificial intelligence should not be regarded as an autonomous management actor but as an information, analytical and forecasting tool supporting the activities of authorised actors. Effective AI application requires a human–machine interaction model in which algorithmic capabilities are combined with professional experience, critical thinking, contextual understanding and human legal responsibility. Final decision-making and responsibility for its consequences must remain with the competent official.*

Keywords: artificial intelligence, management capacity, security forces, defence forces, security and defence sector, public administration, management decisions, threat forecasting, situational awareness, human–machine interaction

100-110
v.38 (2026)
https://smart-scm.org

Олена Вольська «Штучний інтелект як інструмент підвищення управлінської спроможності сил безпеки і оборони України». *У статті досліджено штучний інтелект як інструмент підвищення управлінської спроможності сил безпеки і оборони України. Обґрунтовано, що в умовах підвищеного ризику, обмеженого часу, неповноти інформації, протидії противника та швидкої зміни оперативної обстановки ефективність діяльності відповідних суб'єктів значною мірою залежить від швидкості оброблення даних, якості прогнозування, узгодженості дій і своєчасності прийняття управлінських рішень. Запропоновано авторське визначення управлінської спроможності сил безпеки і оборони України як комплексної здатності відповідних органів, військових формувань та інших суб'єктів сектору безпеки і оборони реалізовувати визначені законом повноваження шляхом своєчасного отримання й аналізу інформації, оцінювання ризиків, прогнозування загроз, планування діяльності, організації взаємодії, прийняття та реалізації управлінських рішень. У її структурі виокремлено інституційну, інформаційно-аналітичну, прогностичну, планувальну, координаційну, адаптаційну спроможності та спроможність до прийняття і реалізації рішень. Представлено управлінський цикл використання ШІ, що охоплює отримання, перевірку й об'єднання даних, аналіз обстановки, виявлення загроз, оцінювання ризиків, прогнозування, розроблення варіантів дій, прийняття рішення та контроль його виконання. Систематизовано інформаційно-аналітичну, моніторингову, прогностичну, планувальну, координаційну, ресурсно-оптимізаційну, контрольну функції ШІ та функцію підтримки прийняття управлінських рішень. Наголошено, що штучний інтелект має розглядатися не як самостійний суб'єкт управління, а як інструмент інформаційно-аналітичної та прогностичної підтримки діяльності уповноважених суб'єктів. Встановлено, що результативне використання ШІ потребує формування моделі людино-машинної взаємодії, за якої алгоритмічні можливості поєднуються з професійним досвідом, критичним мисленням, контекстуальним розумінням і юридичною відповідальністю людини.*

Ключові слова: штучний інтелект, управлінська спроможність, сили безпеки і оборони, сектор безпеки і оборони, публічне управління, управлінські рішення, прогнозування загроз, обороноздатність, ситуаційна обізнаність, людино-машинна взаємодія.

Introduction. The contemporary security environment is characterised by dynamism, uncertainty, the simultaneous emergence of threats of different types, and a rapid increase in the volume of information required for management decision-making. In the context of the full-scale armed aggression against Ukraine, the ability of the security and defence forces to obtain, process, and analyse data in a timely manner, forecast developments, coordinate the activities of relevant actors, and promptly make well-founded decisions is of particular importance.

Under such conditions, traditional management mechanisms do not always ensure the necessary speed of information processing and response to threats. Large volumes of heterogeneous data, information received from numerous sources, rapid changes in the operational environment, and the need to coordinate the activities of different components of the security and defence sector create a demand for the implementation of modern information and analytical technologies. One such technology is artificial intelligence, whose capabilities make it possible to automate certain information processes, identify patterns in large datasets, assess risks, model possible scenarios, and provide information support for management decision-making.

The use of artificial intelligence in the activities of the security and defence forces is not limited to the development of new weapons, military equipment, unmanned systems, and autonomous systems. An

equally important area is the direct application of AI in management activities, including information collection and analysis, monitoring of the security environment, threat forecasting, operational planning, resource allocation, coordination of interagency interaction, and the preparation of management decision alternatives.

In this context, artificial intelligence should be regarded as a tool for enhancing the management capacity of Ukraine's security and defence forces. This refers to the ability of the relevant actors to exercise their legally defined powers, identify threats in a timely manner, assess risks, ensure effective planning, organise interaction, and make well-founded decisions under conditions of limited time, uncertainty, and information overload.

According to the Law of Ukraine "On National Security of Ukraine", the security forces and defence forces encompass a broad range of military formations, law enforcement and intelligence agencies, and other public authorities whose activities are aimed at protecting Ukraine's national interests. At the same time, these actors differ in their legal status, functional purpose, competence, organisational structure, and the nature of the tasks they perform. Therefore, the implementation of AI in their activities requires not only appropriate technological support but also a coordinated management approach that takes into account the specific characteristics of each actor, ensures the interoperability of information systems, and facilitates effective data exchange.

The importance of this research is further reinforced by the fact that artificial intelligence can simultaneously improve the quality of management and generate new risks. The use of algorithmic systems is associated with the possibility of erroneous or biased outputs, insufficient algorithmic transparency, dependence on data quality, cyber threats, risks of unauthorised access to information, and uncertainty regarding responsibility for decisions prepared or made with the use of AI.

Particular attention should be paid to determining the appropriate balance between algorithmic support and human decision-making. Artificial intelligence should contribute to improving the speed and soundness of management processes without removing humans from the assessment of the situation or from responsibility for the final decision. This approach is consistent with NATO's Principles of Responsible Use of AI in Defence: lawfulness; responsibility and accountability; explainability and traceability; reliability; governability; and bias mitigation.

Ukraine has already established a general strategic framework for the development of artificial intelligence. The Concept for the Development of Artificial Intelligence in Ukraine identifies national security and defence among the priority areas for the application of relevant technologies, while the Action Plan for 2025–2026 provides for the further implementation of its provisions. At the same time, the existing policy documents do not provide a comprehensive understanding of how AI should be integrated specifically into the management processes of the security and defence forces, which management functions should be supported by algorithmic systems, or what criteria should be applied to assess the effectiveness of their use.

Therefore, scientific consideration is required not only of the technological capabilities of AI but, above all, of its place within the system of public and military management, its impact on the management capacity of the security and defence forces, the limits of its use in the preparation and adoption of decisions, and the conditions under which the application of relevant technologies can contribute to strengthening Ukraine's defence capability.

Analysis of recent research and publications. The use of artificial intelligence in the security and defence sector has been

studied by foreign and Ukrainian scholars, primarily in the context of automating military processes, developing command-and-control systems, deploying autonomous systems, analysing operational information, and supporting decision-making. S. Alon-Barkat and M. Busuioc examine the interaction between humans and algorithmic systems in public-sector decision-making. In their research, they draw attention to the risk of "automation bias", whereby public officials may uncritically rely on algorithmic recommendations, as well as to the selective adherence to such recommendations. Their findings are important for determining the limits of AI use in the management activities of security and defence forces. B. Boudreaux, M. Ashby, F. Morgan, A. Lohn and other scholars have systematised the principal areas of military AI application and characterised the associated ethical, operational and strategic risks. The researchers emphasise that achieving a technological advantage requires the simultaneous introduction of risk-mitigation mechanisms and the responsible use of

In Ukrainian academic literature, O. Nikoliuk, O. Rodina and T. Savchenko identify the principal areas of artificial intelligence application in the development of management solutions in public administration. T. Pshenychna examines the integration of artificial intelligence technologies into public administration. O. Harmash, T. Fedorenko and O. Hvozdova investigate information and analytical support, cyber-risk monitoring and assessment, substantiating the need to transform cyber-threat data into a basis for clear and well-founded management decisions.

Thus, the existing studies provide a theoretical foundation for understanding the technological, security and ethical aspects of artificial intelligence application. At the same time, the public administration dimension of this issue remains insufficiently explored, particularly the impact of AI on the overall capacity of Ukraine's security and defence forces to perform information and analytical, monitoring, forecasting, planning, coordination and other management functions.

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the role of artificial intelligence in enhancing the management capacity of Ukraine's security and defence forces, to systematise its key management functions and areas of application, and to identify the organisational and institutional conditions for the effective use of AI technologies in monitoring, forecasting, planning, coordination, and management decision-making support processes.

Presentation of the main results. The study of artificial intelligence as a tool for enhancing the management capacity of security and defence forces requires, first and foremost, clarification of the meaning of the concept of "management capacity". In the academic literature, capacity is generally associated with a particular actor's possession of the necessary powers, organisational structure, and human, financial, informational and technical resources that enable the achievement of defined objectives and the performance of assigned tasks [9].

Management capacity cannot be reduced exclusively to the formally established competence of a particular authority. The existence of legally defined powers does not in itself guarantee the ability to exercise them effectively in practice. Such capacity depends on the quality of management processes, the professionalism of personnel, access to reliable information, the speed of communication, the effectiveness of interagency cooperation, and the ability to adopt and implement decisions in a timely manner.

Management in the security and defence sector is distinctive because it is carried out under conditions of increased risk, time constraints, incomplete information,

adversarial interference and rapidly changing operational environments [10]. Errors or delays in management processes may cause not only organisational or material losses but also directly affect human lives, the resilience of state institutions, territorial integrity and national defence capability.

Security forces and defence forces constitute interconnected but functionally distinct components of the security and defence sector. Pursuant to the Law of Ukraine "On the National Security of Ukraine" [3], security forces comprise law enforcement and intelligence agencies, state bodies with special-purpose law enforcement functions, civil protection forces and other bodies entrusted with ensuring national security. Defence forces include the Armed Forces of Ukraine, as well as other military formations, law enforcement and intelligence agencies entrusted with ensuring national defence [3].

Differences in the functional purposes of these actors determine the specific nature of their management needs. For some actors, the identification of military threats, operational planning and command and control are of primary importance; for others, the principal priorities include state border protection, counterterrorism, public security, civil protection, intelligence or counterintelligence activities [12]. Nevertheless, all of them require timely information, threat forecasting, coordinated action and the proper substantiation of management decisions.

Within this study, the management capacity of Ukraine's security and defence forces is proposed to be understood as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. This definition represents the authors' interpretation developed within the present study. Management capacity encompasses not only the availability of resources to the relevant actors but also their functional ability to transform information into specific management decisions and practical actions.

Based on the proposed definition, the following interrelated components should be distinguished within the structure of the management capacity of security and defence forces:

1. Institutional capacity – the existence of clearly defined powers, an appropriate organisational structure and mechanisms of interaction among the relevant actors.

2. Information and analytical capacity – the ability to collect, verify, systematise, process and analyse information obtained from various sources.

3. Forecasting capacity – the ability to identify trends, assess risks and forecast possible developments in the security and operational environment.

4. Planning capacity – the ability to define objectives, develop courses of action, allocate forces, assets and resources, and adjust plans in response to changes in the operational environment.

5. Coordination capacity – the ability to ensure the coherence of actions undertaken by different components of the security and defence sector, facilitate information exchange and support the joint performance of tasks.

6. Capacity for decision-making and implementation – the ability to select a substantiated course of action in a timely manner, communicate decisions to those responsible for their execution, organise their implementation and monitor the results.

7. Adaptive capacity – the ability to modify structures, procedures, tactics and management approaches in response to emerging threats, new technologies and acquired practical experience/

The proposed components do not function in isolation. The quality of a management decision depends on the completeness of the available information;

100-110
v.38 (2026)
https://smart-scm.org

forecasting results influence planning, while the implementation of plans requires coordination and control. Therefore, management capacity should be regarded as an integrated system in which the weakening of one component may reduce the effectiveness of the entire management process [14].

Artificial intelligence affects management capacity primarily by expanding the possibilities for working with information [7]. Algorithmic systems can process large volumes of structured and unstructured data, identify hidden relationships, compare information obtained from various sources, and present analytical results in a form suitable for use by public officials and military command authorities.

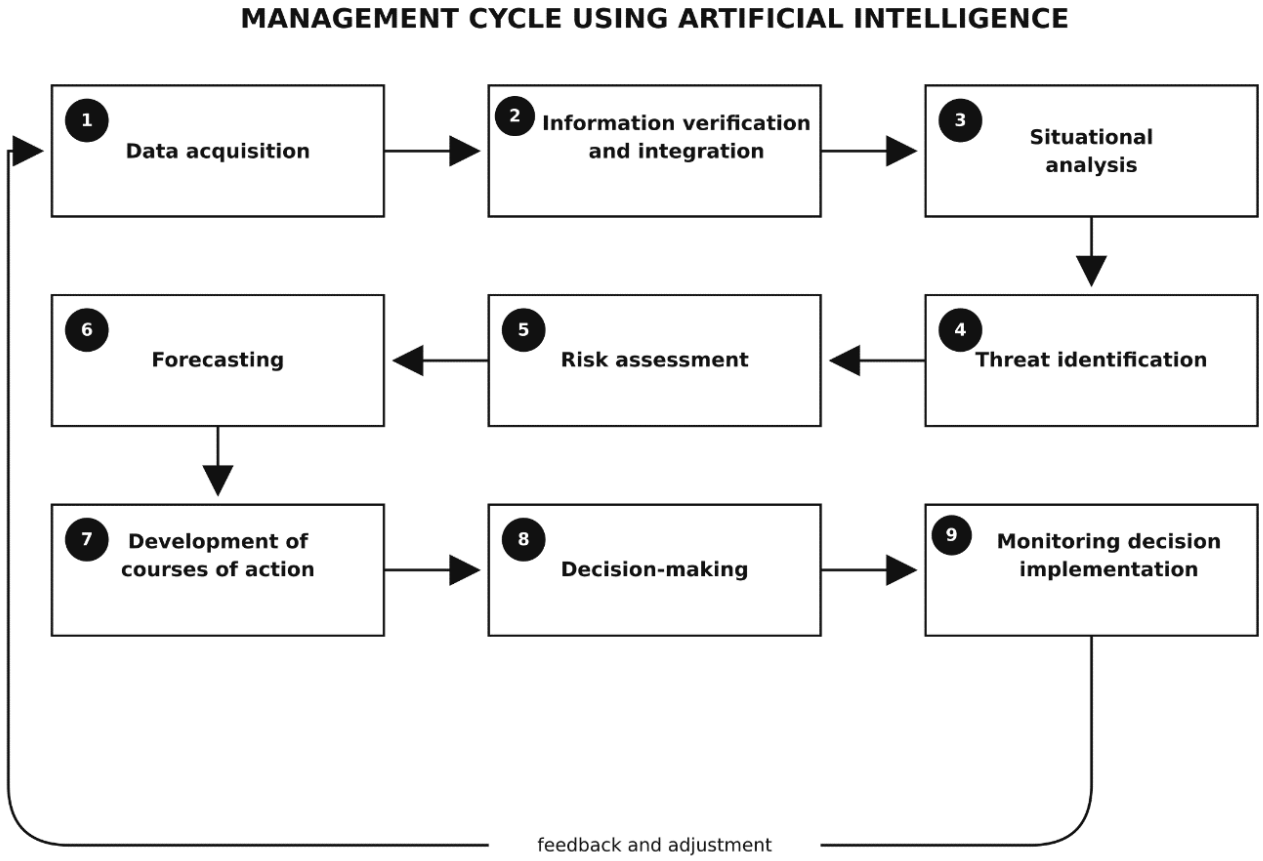


Figure 1. Management cycle using artificial intelligence
Source: Developed by the authors based on their own research.

At each of these stages, artificial intelligence can perform a supporting function by filtering information, detecting anomalies, forecasting possible developments, comparing alternative scenarios and identifying deviations during decision implementation. As a result, the time between receiving information and initiating a management response is reduced, situational awareness is enhanced, and conditions are created for a more substantiated allocation of forces and resources.

Therefore, AI should be regarded not as an autonomous management actor but as an information, analytical and forecasting tool supporting the activities of authorised actors. It can prepare data, identify relationships, propose courses of action and forecast their possible consequences. However, the final decision and responsibility for it must remain with the competent official.

100-110
v.38 (2026)
https://smart-scm.org

These steps do not involve replacing a human manager with an algorithmic system. Instead, they provide for the development of a human–machine interaction model in which the technological capabilities of AI are combined with professional experience, contextual understanding, critical thinking and human legal responsibility [11]. Only under these conditions can the use of artificial intelligence genuinely enhance, rather than merely complicate, the management capacity of Ukraine's security and defence forces [8]

Further examination of the role of artificial intelligence requires the systematisation of its functions in the activities of Ukraine's security and defence forces. In this context, AI functions should be defined not according to the technical characteristics of algorithmic systems but according to their influence on the content, speed and effectiveness of management processes [6].

Based on the conducted research, it is proposed to distinguish the information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions of artificial intelligence, as well as its decision-support function, in the activities of Ukraine's security and defence forces (Table 1).

Table 1. Management functions of artificial intelligence in the activities of Ukraine's security and defence forces

Management function	Content of AI application	Impact on management capacity
Information and analytical	Collection, systematisation, processing and comparison of structured and unstructured data obtained from different sources	Increasing the completeness and speed of information processing; reducing the workload on analytical units
Monitoring	Continuous monitoring of changes in the security and operational environment, detection of anomalies and deviations from specified parameters	Improving situational awareness and ensuring the timely detection of changes in the operational environment
Forecasting	Identification of trends, assessment of the probability of threats and modelling of possible scenarios	Increasing the validity of forecasts and enabling preventive management responses
Planning	Development and comparison of alternative courses of action, modelling of their potential consequences and adjustment of plans	Improving the quality of strategic, operational and tactical planning
Coordination	Integration of information from different agencies, support for information exchange and coordination of joint actions	Strengthening interagency cooperation and reducing delays in transmitting management information
Resource optimisation	Analysis of resource requirements, logistical flows, technical conditions and possible options for allocating forces and assets	Improving the efficiency of the use of personnel, material, technical, financial and time resources
Decision support	Preparation of analytical conclusions, prioritisation of threats and development of alternative courses of action	Reducing the time required to prepare decisions and improving their informational validity

Control	Monitoring the implementation of decisions, comparison of actual results with established objectives and identification of deviations	Ensuring feedback, timely adjustment of actions and increasing executive discipline

Source: Developed by the authors based on their own research

The proposed systematisation demonstrates that artificial intelligence can be applied at all major stages of the management process. At the same time, the content of each function is determined by the competence of the relevant actor, the nature of its assigned tasks, the level of management and the conditions of the operational environment.

The information and analytical function consists in expanding the capacity of security and defence forces to work with large volumes of heterogeneous information. Such data may include text messages, intelligence data, geospatial information, photographic and video materials, information obtained from technical surveillance systems, data concerning the availability and condition of resources, and other information required for situational assessment [4]. The application of AI makes it possible to accelerate the systematisation of these data, identify recurring patterns and develop a comprehensive information picture.

The monitoring function involves continuously monitoring changes in the security and operational environment. Algorithmic systems can detect anomalous events, atypical changes in indicators, potential signs of emerging threats or deviations from established parameters [5]. This entails shifting the emphasis from responding to events that have already occurred to their timely identification and prevention.

The forecasting function involves using accumulated data to identify trends and model possible developments. AI can assist in assessing the probability of specific threats, forecasting changes in the operational environment, determining the possible consequences of adopted decisions and identifying factors that may affect the achievement of established objectives [2]. At the same time, algorithmic forecasts should not be regarded as indisputably reliable predictions but as one of the informational elements used in preparing management decisions.

The planning function consists in using AI to develop, model and compare possible courses of action. Algorithmic systems can assist in assessing resource requirements, time constraints, potential risks and the expected outcomes of each scenario. This contributes to improving the validity of strategic, operational and tactical planning but does not eliminate the need for the professional assessment of proposed options by authorised officials.

The coordination function is reflected in ensuring the coherence of actions undertaken by different actors within the security and defence sector. Artificial intelligence can facilitate the integration of information received from different authorities and units, detect inconsistencies in data, identify shared priorities and promptly communicate the necessary information to the relevant actors [13]. However, the implementation of this function depends on the interoperability of information systems, the availability of common data standards and a legally established procedure for interagency information exchange.

The resource optimisation function encompasses the analysis of requirements for forces, assets, material and technical resources, transport, communications, medical support and other components of security and defence activities. Algorithmic systems can contribute to forecasting requirements, identifying critical shortages,

optimising logistics routes, monitoring the technical condition of equipment and ensuring a more rational allocation of available resources.

The management decision-support function is integrative because it combines the results of the information and analytical, monitoring, forecasting and planning functions. AI can synthesise information, prioritise threats, compare alternative courses of action and forecast their possible consequences. Nevertheless, an algorithmic recommendation should not automatically become a management decision. It must be verified with due regard to the operational context, the reliability of source data, legal restrictions and potential consequences.

The control function is implemented by comparing actual results with the established objectives, indicators and parameters of decision implementation. Algorithmic systems can promptly identify deviations, determine factors hindering task performance and provide information on the need to adjust existing plans. This ensures feedback between an adopted decision, the process of its implementation and subsequent management responses.

The management potential of artificial intelligence lies not in performing a single isolated function but in combining different capabilities within an integrated management cycle. Information obtained through monitoring is used for analysis and forecasting; forecasting results provide the basis for planning; developed courses of action are used in decision-making; and monitoring decision implementation generates new data for further analysis and activity adjustment.

At the same time, the introduction of artificial intelligence does not imply the complete transfer of the relevant functions to algorithmic systems. Rather, it involves the technological enhancement of management activities, whereby AI supports information processing, modelling and the preparation of recommendations, while goal setting, the assessment of legal and societal consequences, the selection of the final course of action and responsibility for its implementation remain with humans [1].

Conclusions.

The conducted research demonstrates that artificial intelligence should be considered not only as a technological innovation but also as an important tool for enhancing the management capacity of Ukraine's security and defence forces. Under conditions of increased risk, time constraints, incomplete information, adversarial interference and rapidly changing operational environments, AI technologies can improve the speed of data processing, situational awareness, threat forecasting, activity planning, interagency coordination and the informational validity of management decisions.

The management capacity of Ukraine's security and defence forces is defined as the comprehensive ability of the relevant authorities, military formations and other actors within the security and defence sector to exercise their statutory powers through the timely acquisition and analysis of information, risk assessment, threat forecasting, activity planning, coordination, and the adoption and implementation of management decisions. This capacity includes institutional, information and analytical, forecasting, planning, coordination and adaptive components, as well as the capacity to adopt and implement decisions. These components form an integrated system in which the effectiveness of each element influences the overall quality of management.

The study establishes that artificial intelligence can support all stages of the management cycle: data acquisition, information verification and integration, situational analysis, threat identification, risk assessment, forecasting, the development of courses of action, decision-making and monitoring of decision implementation. The use of AI can reduce the time between receiving information and initiating a

management response, identify patterns and anomalies in large datasets, compare alternative courses of action and facilitate the rational allocation of forces and resources.

The principal management functions of artificial intelligence in the activities of Ukraine's security and defence forces have been systematised. They include information and analytical, monitoring, forecasting, planning, coordination, resource optimisation and control functions, as well as the decision-support function. The management potential of AI lies not in the isolated performance of individual operations but in integrating these functions within a continuous management cycle supported by feedback and the adjustment of actions.

At the same time, the implementation of artificial intelligence should not result in the transfer of management authority to algorithmic systems. AI should be regarded as an information, analytical and forecasting tool that assists authorised actors in preparing and implementing decisions. Algorithmic recommendations require professional assessment based on the operational context, the reliability and completeness of source data, legal restrictions, potential risks and the possible consequences of the proposed actions.

Effective AI application requires the development of a human–machine interaction model in which technological capabilities are combined with professional experience, critical thinking and contextual understanding. Goal setting, assessment of legal and societal consequences, selection of the final course of action and responsibility for its implementation must remain with the competent official. Preserving meaningful human oversight is therefore a fundamental condition for the responsible use of artificial intelligence by security and defence forces.

Further research should focus on developing criteria and indicators for assessing the impact of AI on management capacity, identifying the specific features of its application by different actors within Ukraine's security and defence sector, improving interagency data exchange and information-system interoperability, and establishing organisational safeguards for human oversight and accountability. Addressing these issues will facilitate the responsible integration of AI into management processes and strengthen the adaptability, resilience and effectiveness of Ukraine's security and defence forces.

References

1. Alon-Barkat, S., & Busuioc, M. (2023). Human–AI interactions in public sector decision making: "Automation bias" and "selective adherence" to algorithmic advice. Journal of Public Administration Research and Theory, 33(1), 153–169. https://doi.org/10.1093/jopart/muac007 [in English].

2. Alon-Barkat, S., & Busuioc, M. (2024). Public administration meets artificial intelligence: Towards a meaningful behavioral research agenda on algorithmic decision-making in government. Journal of Behavioral Public Administration, 7. https://doi.org/10.30636/jbpa.71.261 [in English].

3. Verkhovna Rada of Ukraine. (2018). On the National Security of Ukraine: Law of Ukraine No. 2469-VIII of June 21, 2018. Vidomosti Verkhovnoi Rady Ukrainy, 31, Art. 241. https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian].

4. Harmash, O. M., Fedorenko, T. V., & Hvozdova, O. O. (2026). Corporate cyber risk governance as a factor in the economic security of defence-industrial enterprises. Actual Problems of Innovative Economy and Law, 3, 57–64. https://doi.org/10.36887/2524-0455-2026-3-9 [in Ukrainian].

5. Ilina, A. O. (2025). Artificial intelligence in public authorities as a pathway to the formation of innovative institutions. Scientific Perspectives, 2(56), 823–847. https://doi.org/10.52058/2708-7530-2025-2(56)-823-847 [in Ukrainian].

6. Karpenko, O. V., & Karpenko, Yu. V. (2021). Artificial intelligence as a tool for public administration of socio-economic development: Smart infrastructure, digital business analytics systems and transfers. Public Administration: Improvement and Development, 10. URL: http://www.dy.nayka.com.ua/?op=1&z=2257 [in Ukrainian].

7. Kyrych, N. (2024). The influence of digitalization on modern management processes. In Business Transformation for a Sustainable Future: Research, Digitalization and Innovation: A Monograph (pp. 363–372). Ternopil: Ternopil Ivan Puluj National Technical University. URL: https://elartu.tntu.edu.ua/handle/lib/46660 [in Ukrainian].

8. Morgan, F. E., Boudreaux, B., Lohn, A. J., Ashby, M., Curriden, C., Klima, K., & Grossman, D. (2020). Military applications of artificial intelligence: Ethical concerns in an uncertain world. RAND Corporation. https://doi.org/10.7249/RR3139-1 [in English].

9. Nikoliuk, O. V., Rodina, O. V., & Savchenko, T. V. (2023). Problems and advantages of artificial intelligence as an effective institution for the development of management solutions in public administration. Scientific Notes of V. I. Vernadsky Taurida National University. Series: Public Administration and Management, 34(73), 3, 124–130. URL: https://surl.li/pjenta [in Ukrainian].

10. Sporyshev, K. (2024). Analysis of the regulatory framework for information and analytical support of the security forces of Ukraine: aspects of public administration. Honor and Law, (1 (88), 142–149. https://doi.org/10.33405/2078-7480/2024/1/88/302293

11. Pshenychna, T. V. (2024). Integration of artificial intelligence technologies into public administration at the local level: New horizons and challenges. Efficiency of Public Administration, 3(80/81), 94–104. https://doi.org/10.36930/508013 [in Ukrainian].

12. Pustovit, Ya. B. (2026). State policy on the use of artificial intelligence technologies in the defence sector of Ukraine. Actual Problems of Innovative Economy and Law, 3, 191–195. https://doi.org/10.36887/2524-0455-2026-3-36 [in Ukrainian].

13. Sposato, M., & Dittmar, E. C. (2026). The AI-powered future of digital transformation: Enhancing organizations and leadership development. Journal of Work-Applied Management. https://doi.org/10.1108/JWAM-02-2025-0039 [in English].

14. Zakhmi, K. (2023). AI and integrity: Balancing innovation with ethical responsibility beyond the algorithm. Journal of Artificial Intelligence, Machine Learning and Data Science, 3(2), 2. URL: https://urfjournals.org/open-access/ai-and-integrity-balancing-innovation-with-ethical-responsibilitybeyond-the-algorithm.pdf [in English].

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

111-121
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-8

UDC 351.746.1
JEL Classification: F52, H56, O33.

Received: 2026-07-21
Accepted: 2026-08-26
Published: 2026-08-30

Sorokivska O.A. Doctor of Economics, Professor, Ternopil Ivan Puluj National Technical University Ternopil (Ukraine)

ORCID – 0000-0001-8549-2910
Researcher ID HKO-6132-2023
Scopus author id: – 57148526900
E-Mail: sorokivska_o@tntu.edu.ua

INTERNATIONAL INFORMATION SECURITY IN THE CONTEXT OF THE EMERGENCE OF A GLOBAL INFORMATION SOCIETY

Olena Sorokivska "International information security in the context of the emergence of a global information society" *This article examines the theoretical and methodological foundations for ensuring international information security in the context of the emerging global information society. It is argued that the rapid development of digital technologies, the globalization of information flows, and the spread of artificial intelligence, big data, cloud computing, digital platforms, and cross-border communications are significantly transforming the international security environment, creating not only new opportunities for the development of states and societies but also a wide range of information risks and threats. It is determined that the information space is increasingly becoming an independent sphere of international confrontation, where, alongside traditional instruments, information and psychological operations, cyberattacks, digital espionage, manipulation of public opinion, disinformation, and other forms of hybrid influence are employed. This paper analyzes current trends in the development of the global information society and their impact on the transformation of international information security. It examines the activities of international organizations and integration associations aimed at establishing mechanisms for international cooperation in the field of information security, developing global digital security standards, and countering cybercrime, information operations, and transnational information threats. This paper identifies the key factors influencing the state of international information security in the context of the global information society. It substantiates conceptual directions for improving the international information security system, including: the development of international digital diplomacy; the creation of integrated mechanisms for monitoring information threats; improving strategic communications systems; implementing intelligent technologies for analyzing the information space; developing international information exchange regarding cyber incidents; establishing uniform standards for digital trust and information resilience; and strengthening partnerships among states, international organizations, research institutions, and the private sector in the field of protecting the global information space.*

Keywords: information security, globalization, information society, threats, national security, cyberspace, international cooperation, digital technologies

Олена Сороківська «Міжнародна інформаційна безпека в контексті формування глобального інформаційного суспільства». *У статті досліджено теоретико-методологічні*

111-121
v.38 (2026)
https://smart-scm.org

засади забезпечення міжнародної інформаційної безпеки в умовах формування глобального інформаційного суспільства. Обґрунтовано, що стрімкий розвиток цифрових технологій, глобалізація інформаційних потоків, поширення штучного інтелекту, великих даних, хмарних обчислень, цифрових платформ і транскордонних комунікацій суттєво трансформують міжнародне безпекове середовище, створюючи не лише нові можливості для розвитку держав і суспільств, а й широкий спектр інформаційних ризиків та загроз. Визначено, що інформаційний простір дедалі більше перетворюється на самостійну сферу міжнародного протиборства, де поряд із традиційними інструментами використовуються інформаційно-психологічні операції, кібератаки, цифрове шпигунство, маніпулювання громадською думкою, дезінформація та інші форми гібридного впливу. Проаналізовано сучасні тенденції розвитку глобального інформаційного суспільства та їх вплив на трансформацію міжнародної інформаційної безпеки. Досліджено діяльність міжнародних організацій та інтеграційних об'єднань щодо формування механізмів міжнародного співробітництва у сфері інформаційної безпеки, розвитку глобальних стандартів цифрової безпеки, протидії кіберзлочинності, інформаційним операціям і транснаціональним інформаційним загрозам. У роботі визначено основні чинники, що впливають на стан міжнародної інформаційної безпеки в умовах глобального інформаційного суспільства. Обґрунтовано концептуальні напрями вдосконалення системи міжнародної інформаційної безпеки, серед яких: розвиток міжнародної цифрової дипломатії; створення інтегрованих механізмів моніторингу інформаційних загроз; удосконалення систем стратегічних комунікацій; впровадження інтелектуальних технологій аналізу інформаційного простору; розвиток міжнародного обміну інформацією щодо кіберінцидентів; формування єдиних стандартів цифрової довіри та інформаційної стійкості; зміцнення партнерства між державами, міжнародними організаціями, науковими установами й приватним сектором у сфері захисту глобального інформаційного простору.

Ключові слова: інформаційна безпека, глобалізація, інформаційне суспільство, загрози, національна безпека, інформаційний простір, міжнародне співробітництво, цифрові технології..

Introduction. The emergence of a global information society is one of the defining trends in contemporary global development, accompanied by the rapid spread of digital technologies, an increase in the volume of information exchange, and growing interdependence among nations. The digitization of international relations opens up new opportunities for economic development, international cooperation, and innovative governance, while simultaneously creating new challenges in the field of international information security. Threats related to cyberattacks, disinformation, information and psychological operations, interference in the internal affairs of states through the information space, and the use of digital technologies as a tool of geopolitical influence are of particular concern. In today's world, the information space is increasingly becoming a distinct dimension of international competition, where information serves as both a strategic resource and an object requiring protection. The transnational nature of information threats significantly complicates individual states' ability to detect and neutralize them in a timely manner. This necessitates strengthening international cooperation, developing mechanisms for collective response, and improving international legal regulation in the field of information security. At the same time, the rapid pace of development in digital technologies is far outpacing the adaptation of existing international institutional and legal mechanisms, which reduces the effectiveness of efforts to counter modern information threats. Under these conditions,

the search for new conceptual approaches to ensuring international information security—based on the principles of international partnership, digital resilience, and information trust—becomes particularly relevant. Research into current trends in the development of international information security in the context of the formation of a global information society is an important prerequisite for improving international policy in the field of protecting the global information space and ensuring the sustainable development of the global community.

Analysis of recent research and publications. Issues related to international information security, the development of the global information society, digital transformation, and countering modern information threats are the focus of the domestic scientific community. Research by Ukrainian scholars covers the legal, managerial, institutional, technological, and international-political aspects of ensuring information security, which attests to the interdisciplinary nature of this field.

The scholarly works of O. A. Baranov, V. G. Pylypchuk, and I. M. Doronin are devoted to the development of the theoretical and legal foundations of information security, the improvement of information legislation, the formulation of state policy in the field of cybersecurity and information law, as well as the harmonization of the national information protection system with European and international standards. The researchers pay particular attention to issues related to the legal framework for digital transformation, combating cybercrime, and developing mechanisms to protect Ukraine's information space.

The research by O. P. Dzoban, I. V. Aristova, and K. I. Belyakov focuses on issues of public administration in the field of information security, the development of state information policy, the functioning of mechanisms for ensuring information security in government agencies, and the improvement of the organizational and legal framework for state regulation in the context of digitalization. The authors' works justify the need to integrate modern digital technologies, international experience, and European approaches into the development of the information security system.

At the same time, issues related to ensuring international information security—specifically in the context of the formation of a global information society, the development of international digital diplomacy, the improvement of international coordination mechanisms, countering cross-border information threats, and the establishment of unified international standards for digital trust—remain insufficiently studied in a comprehensive manner. This necessitates further scholarly examination of the conceptual foundations for the development of international information security, taking into account contemporary processes of digital transformation, the globalization of the information space, and the growing role of international cooperation in countering the latest information challenges.

The formulation of the goals of the article to study the theoretical foundations of international information security in the context of the emergence of a global information society, to identify contemporary information threats, and to justify priority areas for improving international mechanisms for ensuring information security.

Presentation of the main results. The emergence of a global information society is a natural consequence of the development of digital technologies, international integration, and the intensive exchange of information, which is fundamentally transforming contemporary social and international processes. Under these conditions, ensuring international information security has become one of the top priorities of international policy, as the resilience of the global information space

directly affects the stability of states, international institutions, and the global security system.

The rapid development of digital technologies is fundamentally changing the modern system of international relations, contributing to the formation of a global information society in which information and digital data are becoming strategic resources. The globalization of information flows enables an unprecedented speed of cross-border information exchange and expands opportunities for international cooperation, economic integration, e-governance, and the development of the digital economy. At the same time, the widespread adoption of artificial intelligence, big data analytics, cloud computing, and digital platforms significantly enhances the efficiency of management processes, automated decision-making, risk forecasting, and the operation of critical infrastructure. At the same time, digitalization significantly increases the dependence of states, international organizations, and society on information and communications infrastructure, making it a potential target for external influence [1].

The transformation of the international security environment is reflected in the changing nature of contemporary threats, which are increasingly of an informational and cyber nature. The use of digital technologies creates conditions for large-scale cyberattacks, information and psychological operations, the spread of disinformation, the manipulation of public opinion, interference in electoral processes, digital espionage, and disruptions to critical information infrastructure. A particular danger is posed by the use of artificial intelligence for the automated creation of disinformation content, deepfake technologies, personalized information campaigns, and the refinement of cyberattack tools. Furthermore, the cross-border nature of digital communications significantly complicates the identification of sources of information attacks, the determination of jurisdiction, and the prosecution of actors engaged in unlawful activities in the global information space [2].

Thus, modern digital technologies serve simultaneously as a powerful driver of social development and a source of new information risks, which necessitates the improvement of international mechanisms for ensuring information security, the development of international cooperation, the harmonization of legal regulations, and the establishment of an effective system for collectively countering global information threats.

It is worth noting that the information space is increasingly becoming a distinct arena of international competition, within which states, international organizations, and non-state actors employ a wide range of instruments of influence; therefore, it is appropriate to classify them into traditional and modern categories [3]:

1. Traditional instruments of international information competition

- diplomatic information influence—the use of official statements, international negotiations, diplomatic channels, and public diplomacy to advance national interests;
- propaganda and counterpropaganda—the systematic dissemination of information aimed at shaping the desired international image of a state or discrediting an opponent;
- informational and psychological influence—the targeted influence on public consciousness and the moral and psychological state of the population, the military, and political elites;
- activities of traditional mass media—the use of television, radio, print media, and international news agencies to shape public opinion;
- political and economic communication—the use of information resources during international negotiations, the implementation of sanctions policies, and the execution of foreign policy strategies.

2. Modern tools of international information warfare:

111-121
v.38 (2026)
https://smart-scm.org

- cyberattacks – unauthorized interference with information systems, government information resources, and critical information infrastructure;

- digital espionage – the illegal acquisition of confidential information through the use of cyber tools, malware, and digital data collection channels;

- disinformation and the dissemination of fake content – the deliberate spread of false or manipulative information to achieve political, military, or economic goals;

- manipulation of public opinion through digital platforms – the use of social media, recommendation algorithms, bot networks, targeted advertising, and other digital technologies to influence public sentiment.

- next-generation information and psychological operations—the comprehensive use of digital technologies, social media, artificial intelligence, and big data technologies to exert targeted informational influence;

- artificial intelligence and deepfake technologies—the automated creation of realistic audio, video, and text content for the purpose of disinformation, discrediting, or misleading a target audience;

- hybrid information operations—a combination of cyber tools, information and psychological influence, economic pressure, political instruments, and diplomatic measures within a unified strategy to achieve geopolitical goals.

Thus, modern international information warfare is characterized by the integration of traditional and digital tools of influence. While traditional methods were primarily aimed at shaping international public opinion through classic communication channels, modern technologies enable high-speed, large-scale, personalized, and often covert influence on the information space, which significantly complicates efforts to ensure international information security and requires the development of new mechanisms for international cooperation and collective response.

The emergence of a global information society is accompanied by a large-scale digital transformation of the global landscape, which is changing the nature of international interaction, economic development, public administration, and security processes. Modern digital technologies not only provide new opportunities for the integration of states and the development of international cooperation but also give rise to fundamentally new challenges in the field of international information security. In this regard, it is advisable to analyze the key trends in the development of the global information society and determine their impact on the transformation of the international security environment [4]:

Table 1 – Current trends in the development of the global information society and their impact on the transformation of international information security

Current Trends in the Development of the Global Information Society	Characteristics of the Trend	Impact on International Information Security
The Globalization of the Information Space	The rapid growth of cross-border information flows, digital communications, and international information exchange.	It strengthens the interdependence of nations, but at the same time increases the risks of cross-border cyberattacks, disinformation, and information interference.
Digital Transformation of Public Administration	Active implementation of e-government, digital services, and interagency information sharing.	It improves the efficiency of public administration while highlighting the need to protect government information resources and critical digital infrastructure.

111-121
v.38 (2026)
https://smart-scm.org

The Spread of Artificial Intelligence and Big Data Technologies	The use of intelligent algorithms to automate processes, analyze information, and support management decisions.	It expands the capabilities for predicting and monitoring threats, but creates risks related to the automation of cyberattacks, information manipulation, and the use of deepfake technologies
The Dominance of Digital Platforms and Social Media	Digital platforms are becoming the primary medium for international communication and the dissemination of information.	They facilitate the global exchange of information, but they also create the conditions for the widespread dissemination of disinformation, information and psychological operations, and the manipulation of public opinion.
Digitalization of Critical Infrastructure	The integration of digital technologies into the operations of the energy sector, transportation, the financial system, healthcare, and the public sector.	It improves the efficiency of managing critical systems, but also increases their vulnerability to international cyberattacks and cyberterrorism.
Strengthening International Cooperation in the Field of Cybersecurity	The development of international mechanisms for coordination, information exchange, and the harmonization of information security standards.	It lays the groundwork for a collective response to global information threats, strengthens digital resilience, and improves the international information security system.

Source: compiled by the author based on data from [5]

Consequently, current trends in the development of the global information society are significantly transforming the international information environment, altering both the nature of international interaction and the nature of information threats. Digitalization, the development of artificial intelligence, global digital platforms, cloud technologies, and cross-border information communications are creating new opportunities for the sustainable development of states, but at the same time are increasing the vulnerability of the international information space to cyber threats, disinformation, and hybrid influences. Under these conditions, international information security takes on a multifaceted character, necessitating the improvement of international legal mechanisms, the development of interstate coordination, the strengthening of digital resilience, and the establishment of an effective system for collective response to contemporary information threats.

Current trends in the development of the global information society indicate that information threats are increasingly taking on a cross-border nature, extending beyond the jurisdiction of individual states and posing risks to international security. Under these conditions, effectively ensuring international information security can no longer rely solely on national mechanisms but requires the consolidation of the international community's efforts, the harmonization of regulatory and legal approaches, and the development of institutional mechanisms for international cooperation. In this regard, the activities of international organizations and integration associations take on particular significance, as they shape the modern architecture of international information security, develop global digital security standards, and coordinate joint measures to counter cybercrime, information operations, and transnational information threats [6-8]:

1) The United Nations (UN)—establishing international legal principles for responsible state behavior in cyberspace and fostering global dialogue on information security. The work of the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG); the development of voluntary norms for responsible state behavior in cyberspace; and the promotion of

international cooperation in the field of cybersecurity.

2) NATO—integration of cybersecurity and information security into the collective defense system; development of member states' cyber resilience. Recognition of cyberspace as a distinct operational domain; activities of the Cooperative Cyber Defense Center of Excellence (CCDCOE) in Tallinn; conduct of the international exercises Locked Shields and Cyber Coalition; exchange of information on cyber threats.

3) European Union (EU) – harmonization of digital legislation; enhancing the cyber resilience of member states; protecting the digital market and critical infrastructure. Adoption of the NIS2 Directive, the DORA Regulation, the Cybersecurity Act, and the Cyber Solidarity Act; activities of ENISA; creation of a CSIRT network for rapid response to cyber incidents.

4) Council of Europe – combating cybercrime and improving international cooperation in criminal law. The Convention on Cybercrime (Budapest Convention) and the Second Additional Protocol on Electronic Evidence; international cooperation among law enforcement agencies during cybercrime investigations.

5) Organization for Security and Cooperation in Europe (OSCE) – reducing the risks of conflict in the digital environment and building trust among states regarding the use of ICT. Implementation of Confidence-Building Measures (CBMs) in cyberspace; consultations among states on the prevention of cyber incidents; mechanisms for transparency and information sharing.

6) International Telecommunication Union (ITU) – development of global digital infrastructure and international standards for information and communication technologies. Global Cybersecurity Agenda (GCA); Global Cybersecurity Index (GCI); development of international technical standards and support for the development of states' cybersecurity capabilities.

7) International Criminal Police Organization (INTERPOL) — coordination of the international fight against cybercrime and transnational digital crimes. The work of the Cybercrime Directorate; international operations against ransomware, botnets, and online fraud; and the operations of the Global Complex for Innovation in Singapore.

An analysis of the activities of international organizations shows that the modern system of international information security is based on multilevel cooperation, within which each institution performs specialized functions. The UN defines general principles of international law governing states' conduct in cyberspace; NATO ensures the development of collective cyber defense and cyber resilience; the European Union establishes a comprehensive regulatory framework for digital security; the Council of Europe coordinates international efforts to combat cybercrime, the OSCE develops confidence-building mechanisms in cyberspace, the ITU establishes global technical standards, and Interpol facilitates international cooperation among law enforcement agencies in the fight against transnational cybercrime.

This comprehensive approach demonstrates that ensuring international information security can no longer be achieved solely at the national level, but requires constant coordination among states, international organizations, the scientific community, and the private sector, as well as the harmonization of international legal, organizational, and technological mechanisms for responding to modern information threats.

However, despite the active development of international cooperation in the field of information security and the improvement of international legal mechanisms to counter modern threats, the global information environment continues to undergo dynamic transformation under the influence of technological, political, and social processes. This gives rise to new factors that

111-121
v.38 (2026)
https://smart-scm.org

shape the current state of international information security, alter the nature of information confrontation, and require constant updating of approaches to ensuring the resilience of the global information space (Table 2).

Table 2 – Key factors influencing the state of international information security in the context of the global information society

Factor	Manifestations in the Current Context
1. The digital transformation of society	The widespread digitization of public administration, the economy, education, the financial system, and critical infrastructure improves the efficiency of societal processes, but at the same time increases the number of potential targets for cyberattacks and unauthorized access to information.
2. The development of artificial intelligence	The use of AI for information analysis, the automation of management processes, cybersecurity, and risk forecasting is accompanied by the potential for its use in the automated creation of disinformation, cyberattacks, personalized information influence, and deepfake technologies.
3. The intensification of information wars and hybrid conflicts	The information space is used as a separate arena of international confrontation, where information and psychological operations are combined with military, political, economic, and cyber instruments of influence.
4. The spread of cyberterrorism and transnational cybercrime	There has been an increase in the number of attacks on government agencies, critical infrastructure, financial institutions, the energy sector, and international information networks using ransomware, malware, and other cyber tools.
5. The use of deepfake technologies and the automation of information and psychological influence	Realistically generated audio, video, and text content, automated bot networks, and generative AI algorithms are being used to manipulate public opinion, discredit political leaders, and destabilize the information environment.
6. The use of algorithmic systems and digital interdependence among nations	The algorithms of digital platforms determine the dissemination of information and shape the information agenda, while the high level of integration of digital infrastructures and global services leads to the rapid spread of information threats across nations and heightens the need for international coordination.

Source: compiled by the author based on data from [9-10]

Thus, the current state of international information security is determined by a complex of interrelated technological, political, and security factors that are significantly transforming the nature of the global information environment. Digital transformation, the development of artificial intelligence, the intensification of information warfare, cyberterrorism, deepfake technologies, the automation of information and psychological influence, the algorithmization of digital platforms, and the growing digital interdependence of states are shaping a new architecture of international information security. This indicates that modern information threats are complex and transnational in nature, and their effective prevention is possible only through a combination of technological innovations, international legal regulation, interstate coordination, and the development of mechanisms for collectively ensuring information resilience.

An analysis of current trends in the development of the global information society and the key factors influencing international information security shows that modern information threats are complex and transnational in nature, as their emergence, spread, and consequences are not limited by national borders. The rapid development of digital technologies, the global integration of information systems, and the high level of digital interdependence among states

contribute to the rapid spread of cyber threats, disinformation, information and psychological operations, and other forms of hybrid influence, which can simultaneously affect multiple countries and regions.

Under these circumstances, effectively preventing and countering cyberattacks, information and psychological operations, disinformation, digital espionage, cyberterrorism, manipulation of public opinion, the use of deepfake technologies, and other forms of hybrid information influence requires a systematic international approach based on the coordination of efforts by states, international organizations, the private sector, and the scientific community; the harmonization of international legal norms; the development of mechanisms for the rapid exchange of information; a coordinated response to cyber incidents; and the strengthening of global digital resilience.

At the same time, the deepening digital transformation of the global community, the growing number of cross-border information threats, and the insufficient effectiveness of existing international response mechanisms necessitate the improvement of the international information security system. Under current conditions, its development must be based on a comprehensive combination of legal, organizational, technological, and institutional mechanisms aimed at ensuring the resilience of the global information space. In this regard, it is appropriate to identify the following conceptual directions for improving international information security [11]:

1) Development of international digital diplomacy—this involves expanding international dialogue to develop common approaches to regulating the digital space, coordinating information security policies, and preventing international information conflicts;

2) Creating integrated mechanisms for monitoring information threats—establishing international platforms for the early detection of information threats will ensure the timely exchange of analytical data, risk forecasting, and the coordination of joint actions to mitigate them;

3) Improving strategic communications systems—developing international cooperation in the field of strategic communications will help increase the effectiveness of countering disinformation, information and psychological operations, and other forms of hybrid influence;

4) Implementation of intelligent technologies for analyzing the information space—the use of artificial intelligence, Big Data, and machine learning will enable the automation of detecting information attacks, analyzing trends in the spread of disinformation, and forecasting potential threats;

5) Developing international information sharing on cyber incidents—establishing effective mechanisms for the rapid exchange of information among states, international organizations, and national response centers will facilitate the swift containment of cyber incidents and minimize their consequences;

6) establishing uniform standards for digital trust and information resilience—the harmonization of international regulatory, legal, and technical standards will help enhance the security of digital infrastructure, foster the development of a secure digital environment, and strengthen trust among participants in international cooperation;

7) Strengthening partnerships among states, international organizations, research institutions, and the private sector—consolidating the resources and expertise of all stakeholders will ensure a comprehensive approach to developing innovative solutions, training specialists, conducting joint research, and establishing an effective international information security system.

Thus, improving the international information security system requires a shift from a predominantly reactive response to information threats to a proactive model of international governance based on risk forecasting, international coordination, and

the widespread use of digital innovations. The priority areas for such development include strengthening international digital diplomacy, implementing smart technologies for monitoring and analyzing the information space, improving strategic communications systems, harmonizing international digital security standards, and deepening partnerships among states, international organizations, the scientific community, and the private sector. Implementing these priorities will contribute to the development of a resilient, adaptive, and effective international information security system capable of ensuring an adequate level of protection for the global information space amid ongoing digital transformation and the rise of transnational information threats.

Conclusions.

Thus, the emergence of a global information society is fundamentally transforming the international security environment, turning the information space into one of the key dimensions of international interaction and confrontation. The rapid development of digital technologies, the spread of artificial intelligence, the globalization of information flows, and the growth of digital interdependence among states—along with new opportunities—are giving rise to a complex set of transnational information threats that cannot be effectively countered at the national level alone. This study has confirmed the decisive role of international organizations in shaping the modern architecture of international information security, while also demonstrating the need for further improvement of mechanisms for international cooperation. Under current conditions, the development of international digital diplomacy, the harmonization of international digital security standards, the implementation of intelligent technologies for monitoring the information space, the improvement of strategic communications, and the strengthening of partnerships among states, international organizations, the scientific community, and the private sector have become priorities. Implementing these priorities will contribute to the formation of an effective, adaptive, and resilient system of international information security capable of ensuring the protection of the global information space in the face of contemporary civilizational challenges.

References

1. Pylypchuk, V. H., Baranov, O. A., Hyliaka, O. S. (2022). The problem of legal regulation in the field of artificial intelligence in the context of the development of European Union legislation. Bulletin of the National Academy of Legal Sciences of Ukraine. Available at: https://visnyk.kh.ua/uk/author/oleksandr-andriyovich-baranov.

2. Pylypchuk, V. H., Doronin, I. M. (2018). National security law and military law: theoretical and applied foundations of formation and development in Ukraine. Information and Law, Vol. 2(25), pp. 62–72. Available at: https://ippi.org.ua/pilipchuk-vg-doronin-im-pravo-natsionalnoi-bezpeki-ta-viiskove-pravo-teoretichni-ta-prikladni-zasadi.

3. Aristova, I. V., Baranov, O. A., Dzoban, O. P., et al.; Bieliakov, K. I. (Ed.). (2019). Legal liability for offenses in the information sphere and the foundations of information delictology. Kyiv: KVITs. 344 p.

4. Bieliakov, K. I. (2018). Legislation in the information security sector: technological and legal analysis. In: Current Issues of Information Security Management of the State: Proceedings of the IX All-Ukrainian Scientific and Practical Conference. Kyiv, pp. 15–19.

5. Kohut, Yu. I. (2024). A new type of hybrid warfare as a threat to national security of the state. Kyiv: DAKOR Publishing House. 348 p.

6. Pavlov, D. M., Mykytiuk, M. A. (2020). Legal and organizational principles of critical infrastructure protection in the context of the formation of Ukraine's new security paradigm. Chest i Zakon, Vol. 4(75), pp. 69–77.

7. Bezverkhniuk, T. M. (2024). Strategic communications for ensuring the synchronization of programs and projects of Ukraine's post-war recovery plan. Public Administration and Administration in Ukraine, Vol. 39, pp. 57–63. Available at: https://pagjournal.iei.od.ua/39-2024.

8. Makovetska, I. M., Yuhov, V. Yu. (2021). Communication management in enterprises. Economics. Management. Business, Vol. 2(36). pp. 32-36. Available at: https://doi.org/10.31673/2415-8089.2021.023338.

9. Onyshchenko, O. V. (2026). Information security as a component of the international system of counter-terrorism. Scientific Bulletin of Uzhhorod National University. Series: Law, Issue 93, Part 5. DOI: https://doi.org/10.24144/2307-3322.2026.93.5.52.

10. Dovhan, O. D., Tkachuk, T. Yu. Legal support of state information security as a sub-branch of information law: theoretical discourse. Available at: https://ippi.org.ua/dovganod-tkachuk-tyu-pravove-zabezpechennya-informatsiinoi-bezpeki-derzhavi-yak-pidgaluzinformatsi.

11. Kylymnyk, I. I. (2023). Information society and information security. New challenges and ways to overcome information threats. Scientific Bulletin of Uzhhorod National University. Series: Law, Vol. 2, No. 76. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.8.

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

122-147
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-9

UDC 338.4:330.322:005.334(477)
JEL Classification: C53, D81, H54, O18

Received: 2026-07-24
Accepted: 2026-08-25
Published: 2026-08-30

Trushkina N.V. Ph.D. (in Economics), Senior Researcher, Senior Research Officer of the Sector of Industrial Policy and Innovative Development of the Department of Industrial Policy and Energy Security, Research Center for Industrial Problems of Development of the NAS of Ukraine (Ukraine)

ORCID – 0000-0002-6741-7738
Researcher ID AAO-9802-2020
Scopus author id: – 57210808778
E-Mail: nata_tru@ukr.net

SCENARIO MODELLING OF INVESTMENT NEEDS FOR THE RESILIENT RECOVERY OF UKRAINE'S CRITICAL INFRASTRUCTURE: STRATEGIC PATHWAYS UNDER WARTIME AND POST-WAR RISKS

Nataliia Trushkina. "Scenario Modelling of Investment Needs for the Resilient Recovery of Ukraine's Critical Infrastructure: Strategic Pathways under Wartime and Post-War Risks". *The article substantiates a scenario-based approach to assessing investment needs for the resilient recovery of Ukraine's critical infrastructure under wartime and post-war risks. The empirical basis of the study comprises the results of RDNA1–RDNA5, which were used to systematise the dynamics of direct damage, economic losses, and recovery needs and to construct an analytical infrastructure block. The methodological framework combines systems and comparative analysis, scenario and simulation modelling, and multi-criteria assessment. Investment needs are treated as a dynamic variable that changes under the influence of new and repeated damage, project implementation rates, financial and institutional constraints, the selected recovery standard, and the capacity of investments to reduce future risks. Four strategic pathways are proposed – minimal-recovery, functional-adaptive, Build Back Better modernisation, and resilience-transformational – together with three types of risk environment, integrated into a scenario matrix. Under the specified scenario assumptions and a baseline value of USD 218.9 billion, the estimated residual needs in 2030 amount to USD 253.8, 197.9, 171.1, and 142.4 billion, respectively. The findings demonstrate that minimising initial capital expenditure is not equivalent to minimising long-term investment needs and systemic risk. The scientific novelty lies in distinguishing strategic choice from the external risk environment, interpreting investment needs dynamically, and linking resource constraints with functional outcomes. The practical significance of the proposed approach lies in its applicability to scenario testing, prioritisation, and portfolio formation of critical infrastructure projects*

Keywords: critical infrastructure, resilient recovery, investment needs, scenario modelling, strategic pathways, wartime risks, post-war recovery, Build Back Better, investment prioritisation, external threats

Наталія Трушкіна. "Сценарне моделювання інвестиційних потреб для резильєнтного відновлення критичної інфраструктури України: стратегічні траєкторії в умовах воєнних і

122-147
v.38 (2026)
https://smart-scm.org

повоєнних ризиків". *У статті обґрунтовано сценарний підхід до оцінювання інвестиційних потреб для резильєнтного відновлення критичної інфраструктури України в умовах воєнних і повоєнних ризиків. Емпіричну основу дослідження становлять результати RDNA1–RDNA5, за якими систематизовано динаміку прямої шкоди, економічних втрат і потреб у відновленні та сформовано аналітичний інфраструктурний блок. Методичний інструментарій поєднує системний і порівняльний аналіз, сценарне та імітаційне моделювання, багатокритеріальне оцінювання. Інвестиційні потреби розглянуто як динамічну величину, що змінюється під впливом нової і повторної шкоди, темпів реалізації проєктів, фінансових та інституційних обмежень, обраного стандарту відновлення і здатності інвестицій знижувати майбутній ризик. Запропоновано чотири стратегічні траєкторії – мінімально-відновну, функціонально-адаптивну, модернізаційну Build Back Better та резильєнтно-трансформаційну – і три типи ризикового середовища, поєднані у сценарну матрицю. За заданих сценарних припущень і базового значення 218,9 млрд дол. США розрахунковий залишок потреб у 2030 р. становить відповідно 253,8; 197,9; 171,1 і 142,4 млрд дол. Встановлено, що мінімізація початкових капітальних витрат не тотожна мінімізації довгострокових потреб і системного ризику. Наукова новизна полягає у розмежуванні стратегічного вибору та зовнішнього ризикового середовища, динамічному трактуванні інвестиційних потреб і поєднанні ресурсних обмежень із функціональним результатом. Практичне значення підходу полягає у можливості його використання для сценарного тестування, пріоритизації та формування портфеля проєктів критичної інфраструктури.*

Ключові слова: критична інфраструктура, резильєнтне відновлення, інвестиційні потреби, сценарне моделювання, стратегічні траєкторії, воєнні ризики, повоєнне відновлення, Build Back Better, інвестиційна пріоритизація, зовнішні загрози.

Introduction. The full-scale war has changed not only the scale of destruction inflicted on Ukraine's critical infrastructure but also the underlying economic logic of its recovery. Under the conventional post-crisis model, damage assessment, needs estimation, and the development of reconstruction programmes generally take place after the destructive event has ended. The situation in Ukraine is fundamentally different. Recovery activities are being carried out while the military threat persists, meaning that already repaired facilities may suffer repeated damage, the spatial distribution of population and economic activity continues to change, the cost of equipment and construction works rises, logistics chains become increasingly complicated, and requirements for physical, technological, and digital security are continuously tightened. As a result, recovery can no longer be regarded as a one-time reconstruction of lost assets. Instead, it becomes a prolonged process of managing infrastructure functionality, vulnerability, and investment needs under conditions of uncertainty [1–5].

The quantitative parameters of reconstruction confirm the systemic nature of this challenge. According to the five consecutive Rapid Damage and Needs Assessments, from RDNA1 to RDNA5, direct damage to Ukraine increased from 97.4 billion to 195.1 billion United States dollars, economic losses from 252.0 billion to 666.7 billion United States dollars, and ten-year recovery needs from 348.5 billion to 587.7 billion United States dollars [6–11]. At the same time, economic losses accumulated substantially faster than physical damage. Between 2022 and 2025, economic losses increased by 164.6 percent, compared with an increase of 100.3 percent in direct damage, while the ratio of losses to damage rose to 3.42. This indicates that the economic consequences of infrastructure destruction arise not only at the moment when an asset is

physically damaged. A considerable share of these consequences accumulates throughout the period in which critical functions remain disrupted, taking the form of foregone revenues, additional operating costs, shortages of essential services, reduced production activity, and secondary effects transmitted across interdependent sectors.

An important structural feature of the recovery process is the increasing role of the infrastructure component. For analytical purposes, an infrastructure block was constructed on the basis of the Rapid Damage and Needs Assessments, comprising energy and extractive industries, transport, telecommunications and digital infrastructure, water supply and sanitation, and municipal services. The estimated recovery needs of this block increased from 98.9 billion United States dollars in RDNA1 to 218.9 billion United States dollars in RDNA5 [6–11]. It accounted for approximately 50.2 percent of the overall increase in recovery needs between the first and fifth assessments, and for 77.2 percent of the increase between RDNA4 and RDNA5. At the same time, this analytical aggregate should not be equated with Ukraine's legally defined critical infrastructure system. Its analytical value lies primarily in its ability to trace the dynamics of sectors whose functioning directly determines the continuity of basic services and the resilience of other components of the economic system. For this reason, allocating resources solely according to sectoral affiliation or the scale of physical destruction is insufficient. Investment decisions must also take into account the criticality of the function performed, the number of dependent users, the possibility of substitution, the facility's position within the network, and its potential to trigger cascading failures.

This leads to a distinction that is fundamental to investment planning: direct damage, recovery needs, and the amount of investment actually required are not equivalent concepts. The value of a damaged asset reflects the scale of the physical loss, but it does not automatically determine either the cost of restoring the critical function or the target configuration of the recovered system. An estimated recovery need, in turn, is not equivalent to the volume of financing that can be mobilised and effectively utilised within a given period. Likewise, the formal completion of construction or repair works does not necessarily mean that the required level of functionality and resilience has been achieved [1; 6–14]. This distinction is particularly pronounced in network infrastructure. Physical damage of the same monetary value may produce substantially different consequences depending on the systemic role of the damaged node, the availability of alternative routes and reserve capacities, the duration of disruption, and the possibility of rapid substitution. The initial capital cost of a project therefore cannot, by itself, serve as a sufficient criterion for determining its investment viability.

A further constraint arises from the gap between the scale of long-term needs and the actual capacity to transform financial resources into completed projects that deliver functional outcomes. The problem extends well beyond a shortage of financing. Investment feasibility depends on the availability of a sufficiently prepared project pipeline, feasibility studies and design documentation, secure access to infrastructure facilities, contractor and production capacity, access to equipment, procurement timelines, institutional coordination, and the capacity to operate and maintain newly created or restored facilities. Consequently, the path from total estimated recovery needs to the actual restoration of a critical function involves not one but several successive gaps: financial, project preparation, implementation, technical, functional, and resilience gaps. Treating these gaps as a single issue creates the misleading impression that mobilising the required amount of funding automatically means that recovery has been completed.

The choice of the infrastructure condition that investment is intended to achieve is equally important. Restoring pre-war technical characteristics may be justified when the immediate objective is to return specific functions to operation, but it is not always rational from a life-cycle perspective. If reconstruction reproduces the previous territorial concentration of capacities, technological obsolescence, insufficient interchangeability, or single points of failure, it simultaneously preserves some of the vulnerabilities embedded in the pre-existing system. An alternative approach is to incorporate modernisation, physical and digital protection, redundancy, decentralisation, autonomy, spatial dispersion of critical nodes, and improved maintainability into investment decisions. This is precisely where the difference between restoring an asset and ensuring the resilient recovery of a system becomes apparent. Higher expenditure at the initial stage may be economically justified if it shortens the duration of future disruptions, reduces the scale of repeated damage, and lowers expected losses over the infrastructure life cycle [2–4; 7–11].

The challenge of financing critical infrastructure therefore has not only a quantitative dimension but also structural and temporal dimensions. The key issue becomes the choice among different ways of allocating scarce resources: rapidly replacing damaged assets; prioritising the restoration of critical functions through temporary, mobile, and reserve solutions; undertaking technological modernisation in line with new standards; or pursuing a deeper transformation of the infrastructure system aimed at reducing future risk. These alternatives differ not only in their initial costs but also in implementation timelines, financing requirements, their effects on system functionality, and their capacity to prevent the renewed accumulation of recovery needs.

The need to make such choices will persist even after the intensity of direct hostilities declines. A post-war environment will not automatically imply a transition to risk-free reconstruction. Accumulated damage and the territorial unevenness of destruction will be compounded by limited availability of long-term capital, changes in the spatial distribution of population and economic activity, shortages of certain types of equipment and specialised expertise, cyber and technological threats, and the need to align new infrastructure with the requirements of European integration, decarbonisation, energy efficiency, and resource efficiency. Accordingly, decisions taken under the pressure of urgent wartime needs will have long-term consequences. They may either create the foundation for structural modernisation or lock the system into technological and spatial configurations whose subsequent modification would require substantial additional expenditure.

Against this background, the scientific problem lies in the need to reconcile the dynamic formation of investment needs with the choice of a strategic trajectory for critical infrastructure recovery in a changing risk environment. A static estimate of reconstruction costs does not capture the fact that future needs depend on new and repeated damage, the pace of project implementation, the level of available financing, the selected recovery standard, and the capacity of completed investments to reduce subsequent vulnerability. Nor does such an estimate allow the economic consequences of alternative decisions to be compared adequately, ranging from minimum repair to functional adaptation, technological modernisation, and the resilient transformation of the infrastructure system.

Investment justification for critical infrastructure therefore requires a shift away from searching for a single "cost of reconstruction" towards analysing a range of possible recovery trajectories. Each trajectory

is shaped by a particular combination of the external risk environment, the target condition of the infrastructure, the pace of project implementation, resource constraints, and the expected effect of risk reduction. Scenario modelling within this framework makes it possible to assess not only the amount of investment required but also the consequences of choosing different recovery models over time. The rationality of an investment decision is therefore determined not by the minimisation of initial expenditure as such, but by the relationship between investment, function, time, risk, and avoided losses. This relationship makes it possible to connect the cost of reconstruction with its ultimate outcome: the capacity of critical infrastructure to sustain vital functions and adapt to wartime and post-war risks.

Analysis of recent research and publications. Scientific approaches to the study of critical infrastructure have undergone a marked evolution over recent decades. While earlier research focused primarily on the physical protection of individual assets and on minimising the probability of their damage, contemporary scholarship increasingly relies on a systemic understanding of infrastructure as a set of interconnected networks, functions, and services whose disruption may generate much broader economic and social consequences. At the same time, international and Ukrainian researchers have developed this understanding under different institutional and security conditions, which has resulted in certain differences in the focus of analysis, methodological tools, and the interpretation of recovery priorities.

In the international literature, the resilience-oriented approach has become one of the leading perspectives. A. Mentges et al. [1] demonstrate that the meaning of resilience is context-dependent and that no universal interpretation can be applied equally to different types of critical infrastructure. W. Liu et al. [15] understand infrastructure resilience as the capacity of a system to prepare for disruptive events, absorb their consequences, restore its functioning, and adapt to changed conditions. The systematic reviews by M. Sathurshan et al. [16] and B. Rathnayaka et al. [17] confirm the growing use of multidimensional approaches to resilience assessment, in which physical reliability is considered alongside functionality, recovery time, adaptability, cross-sectoral interdependencies, and changes in the state of the system after a shock. Criticality in the international research discourse is therefore increasingly determined not only by the physical characteristics of an asset but by the function it performs within the wider system.

Ukrainian scholarship initially followed a somewhat different research logic. The development of the national critical infrastructure protection system led to the predominance of security-oriented, regulatory, legal, and public governance approaches. However, following the beginning of the Russo-Ukrainian war, and particularly after the full-scale invasion, the scope of research expanded considerably. O. Sukhodolia [18] examines critical infrastructure resilience through its capacity to maintain vital functions and services, which effectively brings the Ukrainian approach closer to the international functional paradigm of resilience. O. Shpatakova, R. Ivanenko, and M. Pohrebytskyi [19] focus on the specific challenges of restoring critical infrastructure in de-occupied territories, where reconstruction is directly connected with the restoration of territorial integrity, economic activity, and the basic conditions required for everyday life. V. Mykytenko [20], in turn, interprets the post-war recovery of critical infrastructure as part of its reconstructive development, implying a transition towards qualitatively new parameters of system functioning.

The distinction between these two research traditions is therefore gradually diminishing. International research historically shifted earlier from the protection

of individual assets towards the preservation of critical functions, whereas the Ukrainian discourse has evolved from a security and institutional interpretation of critical infrastructure towards an integrated understanding that combines protection, functional resilience, recovery, and long-term development. At the same time, the Ukrainian approach understandably retains a stronger emphasis on military conditions, territorial considerations, and public governance.

A second important area of comparison concerns the interpretation of risk. International research generally conceptualises critical infrastructure as a highly interdependent system in which the failure of one node may trigger a chain of secondary disruptions. This perspective shifts the focus of analysis away from immediate physical damage towards the functional and economic consequences generated as disruption propagates through the system. S. Hallegatte, J. Rentschler, and J. Rozenberg [21] demonstrate that the economic significance of infrastructure resilience is determined not only by reducing the value of physical damage but also by shortening service disruptions and limiting the associated welfare losses. S.-A. Mitoulis et al. [2] adapt this logic to conflict environments, where functional interdependencies, cascading effects, and the restoration of critical services become integral elements of a broader conflict-resilience framework.

Ukrainian research on risk has largely developed around the identification of specific military threats and the determination of protection priorities. A representative example is the study by R. Murasov and Ya. Melnyk [22], which applies expert assessment to quantitatively prioritise threats to critical infrastructure under missile and drone attacks. This methodological orientation directly reflects Ukraine's current needs, while also illustrating an important difference between the two research traditions: international scholarship focuses more extensively on the behaviour of interconnected systems after a shock, whereas Ukrainian studies devote considerable attention to identifying and ranking the sources of danger themselves. For the purposes of investment justification for resilient recovery, however, these approaches should not be regarded as mutually exclusive; rather, they are complementary.

The most visible difference remains the degree of quantitative formalisation. Alongside indicator-based systems, international research makes extensive use of probabilistic, network-based, multi-criteria, and dynamic models. H. O. Caetano et al. [3], for example, employ dynamic Bayesian networks to assess critical infrastructure resilience and to model the propagation of evidence across system components. The studies reviewed by M. Sathurshan et al. [16] and B. Rathnayaka et al. [17] assess resilience using indicators of functional performance, recovery time, vulnerability, adaptability, and other parameters. Such approaches make it possible to move beyond recording the current state of infrastructure towards analysing how an infrastructure system may behave under different conditions.

Ukrainian studies more commonly employ systemic, institutional, expert-based, comparative, and structural-logical methods. Their principal advantage lies in their ability to capture national specificities, actual constraints on public governance, and the distinctive characteristics of the wartime environment. At the same time, some studies already demonstrate a movement towards greater formalisation of risk assessment [22]. This creates the basis for the further development of scenario-based and dynamic modelling, in which the object of analysis should extend beyond the level of threat or resilience observed at a particular point in time to include changes in recovery and investment needs over time.

The Build Back Better concept forms a separate methodological dimension. In international approaches, it fundamentally changes the relationship between damage

and recovery needs. According to the guidance provided by the Global Facility for Disaster Reduction and Recovery [12] and the study by S. Hallegatte, J. Rentschler, and B. Walsh [13], reconstruction should not reproduce pre-existing vulnerabilities but should use post-crisis recovery as an opportunity to strengthen infrastructure systems, accelerate their recovery, and increase their inclusiveness. From an economic perspective, this means that required investment may exceed the cost of simply replacing a damaged asset because it also incorporates expenditure on modernisation, redundancy, protection, autonomy, and other characteristics that contribute to future resilience.

In Ukrainian research, a similar idea acquires a specific meaning because recovery and development need to be pursued simultaneously. V. Mykytenko [20] directly links the reconstruction of critical infrastructure with improvements in its quality and reliability, while O. Lazor, I. Yunyk, and A. Zabolotnyi [23] consider post-war recovery within the framework of a national strategy that should encompass not only the reconstruction of damaged facilities but also the modernisation of vital sectors and the identification of appropriate financing sources. Thus, the international approach more explicitly formalises the principle of "building back better", whereas the Ukrainian perspective adds the question of whether and how such a transition can be implemented institutionally under conditions of extensive destruction, resource constraints, and an uncertain security environment.

The investment dimension of recovery is also interpreted differently, although the two perspectives are becoming increasingly aligned. In the international discourse [12; 13; 21], investment in resilience is evaluated according to its capacity to reduce future disruptions and losses rather than solely by the volume of capital expenditure. T. Becker et al. [14], when examining the prospects for Ukraine's reconstruction, emphasise the need to combine external financing with institutional reforms, modernisation, and European integration. The OECD [24] additionally highlights the importance of a clear prioritisation framework, the availability of implementation-ready projects, efficient use of resources, and consistency between reconstruction efforts and long-term digitalisation and decarbonisation objectives.

Historical studies of post-war recovery further reinforce this argument. B. Eichengreen [4] demonstrates the importance of institutional coordination, investment, and structural adaptation for Europe's post-war economic growth. R. Mallett and A. Pain [25], in their analysis of post-conflict recovery, draw attention to the role of markets, the private sector, and infrastructure linkages in restoring economic activity. The outcome of reconstruction, therefore, is determined not simply by whether capital has been mobilised, but by how those resources are transformed into a new functional and institutional configuration of the economy.

The Ukrainian context fundamentally complicates this logic because investment decisions have to be made before the principal destructive factor has ceased to operate. A reconstructed facility may be damaged again, while the actual level of need may continue to change even as the investment portfolio is being designed and implemented. The works of Ukrainian researchers [18–20; 22–23] convincingly demonstrate the importance of functional resilience, territorial specificities, military threats, public-sector coordination, and the strategic nature of post-war recovery. At the same time, a particularly important task for the Ukrainian academic discourse is to move beyond assessing what has been damaged and to what extent, towards determining how much should be invested, in what sequence, and towards what target state of the system in order for such investment to be economically justified.

The comparative analysis therefore points not to a fundamental opposition between international and Ukrainian research approaches, but rather to their potential methodological complementarity. A major strength of the international discourse lies in its high degree of formalisation of resilience, its analysis of cross-sectoral interdependencies and cascading effects, and its attention to the dynamics of system functioning. Ukrainian studies, by contrast, provide a deeper reflection of the specific characteristics of the wartime environment, territorial heterogeneity, institutional and resource constraints, and the need to address protection, recovery, and modernisation simultaneously. Combining these research perspectives provides a theoretical and methodological foundation for moving from a static assessment of reconstruction costs towards scenario-based analysis of investment needs and strategic trajectories for the resilient recovery of Ukraine's critical infrastructure.

Identification of previously unresolved parts of the overall problem. Despite substantial progress in research on critical infrastructure resilience, risk management, post-war recovery, and the principles of Build Back Better, the investment dimension of this field remains methodologically fragmented. In most existing approaches, the assessment of physical damage, the estimation of recovery needs, the analysis of resilience, and the justification of investment decisions are treated as relatively independent analytical tasks. As a result, the transition from the estimated cost of recovery to the determination of an investment volume and structure capable of ensuring not only asset reconstruction but also the restoration of critical functions, the reduction of future vulnerability, and the achievement of a target level of resilience remains insufficiently formalised.

A separate unresolved issue is the predominantly static interpretation of investment needs. Conventional approaches to damage and needs assessment are useful for establishing a baseline estimate of the scale of reconstruction, but they are considerably more difficult to apply in an environment where the level of need itself changes during the implementation of recovery measures. This is particularly important for Ukraine, where new and repeated destruction, revisions of existing assessments, changes in the cost of works and equipment, different rates of financing utilisation, and limited project readiness may simultaneously increase or reduce residual needs. Investment needs should therefore be viewed not as a one-off estimate, but as a dynamic outcome of the interaction between accumulated damage, newly incurred losses, the pace of project implementation, and the characteristics of the selected recovery model. In the present study, this interdependence is treated as a key property of the object of scenario modelling.

The combined consideration of the external risk environment and the strategic choice concerning the target state of infrastructure also remains insufficiently developed. Existing studies generally examine either the impact of threats on system resilience or the advantages of particular recovery and modernisation models. Yet the same strategy may have very different economic consequences under stabilisation, prolonged military pressure, or the escalation of compound threats. Similarly, at the same level of risk, minimum recovery, functional adaptation, modernisation, and resilient transformation may generate different trajectories of capital requirements and residual vulnerability. It is therefore essential to distinguish analytically between external conditions that are beyond the control of the decision-maker and the strategic trajectory that results from a deliberate management choice. Such a distinction makes it possible to compare alternative strategies under the same level of risk exposure and to avoid conflating external

uncertainty with the parameters of the recovery strategy itself.

Another research gap concerns the insufficient distinction between long-term needs, the priority project portfolio, committed financing, investments actually implemented, and the functional outcomes ultimately achieved. A financing gap is only one of the barriers to recovery. Even when financial resources are formally available, incomplete projects, equipment shortages, limited contractor capacity, security constraints, or a mismatch between the selected technical solution and the critical function may create additional project preparation, implementation, physical, functional, and resilience gaps. Consequently, assessing reconstruction performance solely in terms of funds mobilised or spent does not reveal the extent to which systemic vulnerability has actually been reduced. For this reason, investment analysis needs to move beyond the value of a damaged asset towards the broader logic of "investment – function – time – risk – avoided losses."

A comprehensive approach that simultaneously links the dynamics of investment needs, alternative strategic recovery trajectories, changes in the wartime and post-war risk environment, implementation capacity, and the economic effects of increased resilience therefore remains insufficiently developed. Overcoming this methodological fragmentation requires a scenario-based formulation of the problem in which investment needs are assessed not in isolation, but as the outcome of the interaction between external risks and managerial choices concerning the future configuration of critical infrastructure.

Formulation of the article's objectives. The aim of the study is to develop and test a scenario-based approach to assessing investment needs and substantiating strategic trajectories for the resilient recovery of Ukraine's critical infrastructure, taking into account the dynamics of their formation, implementation capacity, financial constraints, and the changing wartime and post-war risk environment.

Achieving this aim requires addressing the following tasks: to systematise the dynamics of direct damage, economic losses, and recovery needs based on the results of RDNA1–RDNA5 and determine the role of the infrastructure component within their overall structure; to distinguish between direct damage, estimated recovery needs, the required volume of investment, committed financing, investments actually implemented, and the functional outcomes achieved; to develop a system of strategic trajectories reflecting alternative target states of critical infrastructure, ranging from minimum restoration of damaged assets to the resilient transformation of the system; to identify types of external risk environments and integrate them with strategic alternatives into a single scenario matrix; to conduct simulation-based assessment of the dynamics of residual investment needs for 2026–2030 under different combinations of scenario parameters; to determine how the pace of investment implementation, additional expenditure on resilience enhancement, and reductions in future risk affect the long-term dynamics of required resources; and to substantiate criteria for selecting a strategic trajectory on the basis of the relationship between "investment – function – time – risk – avoided losses".

The methodological foundation of the study comprises systemic, functional, risk-oriented, resilience-based, and scenario-based approaches. The research employs methods of analysis, synthesis, and scientific generalisation; comparative and structural-logical analysis; systematisation and dynamic analysis of RDNA1–RDNA5 data; scenario and simulation modelling; and multi-criteria assessment to substantiate the selection of strategic trajectories for the resilient recovery of critical infrastructure.

Within this study, scenario modelling is not regarded as a tool for producing a

122-147
v.38 (2026)
https://smart-scm.org

deterministic forecast of reconstruction costs, but rather as a means of comparing alternative management decisions under different combinations of external risks and recovery parameters. This approach makes it possible to assess not only the scale of the resources required but also the long-term consequences of choosing among minimum-restoration, functional-adaptive, modernisation, and resilience-transformation trajectories for the recovery of critical infrastructure.

Presentation of the main research material. Scenario-based assessment of critical infrastructure investment needs should not be structured around the search for a single final "cost of reconstruction", but rather around a sequence of decisions that transform assessed damage into a restored critical function. This approach is particularly important for Ukraine, where reconstruction is taking place under conditions of a continuing military threat, repeated damage, restricted access to certain territories, changing price conditions, and uneven capacity to implement projects. The PDNA and Disaster Recovery Framework methodologies provide the basic framework for distinguishing between damage, losses, needs, and priorities, while the Build Back Better approach adds the requirement not to reproduce pre-existing vulnerabilities, but to reduce future risk [5–6; 12–13].

For investment analysis, it is essential to distinguish between five categories: direct damage, estimated recovery needs, the required volume of investment taking into account the target state of the infrastructure, investments actually implemented, and the functional outcome achieved. Treating these categories as equivalent distorts management decisions: the availability of financing does not yet mean that implementation has taken place, the completion of construction works does not guarantee the restoration of the service, and the physical reconstruction of an asset does not necessarily reduce systemic risk. In a concise form, this relationship can be expressed as:

$$D_{i,t} \not\equiv N_{i,t} \not\equiv I_{i,t}^{req} \not\equiv I_{i,t}^{impl} \not\equiv R_{i,t}^{func}, \quad (1)$$

where $D_{i,t}$ denotes the direct damage to asset or system i in period t; $N_{i,t}$ denotes estimated recovery needs; $I_{re}q_{i,t}$ denotes the required investment taking into account the target state of the infrastructure; $I^{impl}{}_{i,t}$ denotes investment actually implemented; $R^{func}{}_{i,t}$ denotes the achieved level of functional recovery. Equation (1) is conceptual in nature: it represents different stages of a single process rather than an arithmetic inequality between indicators.

The empirical basis of the calculations consists of five consecutive Rapid Damage and Needs Assessments – RDNA1–RDNA5 [7–11]. They are used as a system of interconnected analytical snapshots rather than as a homogeneous statistical time series. The assessments were prepared as of different dates, cover different durations of the war, and incorporate revisions to sectoral boundaries, price assumptions, and needs that had already been met. RDNA5 is therefore used as the baseline for the scenario simulation, while the preceding assessments are employed to identify structural changes, verify the direction of observed dynamics, and establish sensitivity ranges.

The consecutive assessments demonstrate not only an expansion in the scale of destruction, but also a substantial change in the relationship between physical damage and the economic consequences of disrupted functions. Between RDNA1 and RDNA5, direct damage increased from USD 97.4 billion to USD 195.1 billion, approximately doubling, whereas economic losses rose from USD 252.0 billion to USD

122-147
v.38 (2026)
https://smart-scm.org

666.7 billion, an increase of 164.6%. Ten-year recovery needs increased from USD 348.5 billion to USD 587.7 billion (Table 1) [7–11].

Table 1 – Dynamics of the Overall RDNA1–RDNA5 Estimates

Indicator	RDNA1	RDNA2	RDNA3	RDNA4	RDNA5	Change, RDNA1–RDNA5, %
Direct damage, USD billion	97.4	134.7	152.5	176.1	195.1	100.3
Economic losses, USD billion	252.0	289.1	499.3	588.8	666.7	164.6
Recovery needs, USD billion	348.5	410.6	486.2	523.6	587.7	68.6
Losses / damage, times	2.59	2.15	3.27	3.34	3.42	32.0
Recovery needs / damage, times	3.58	3.05	3.19	2.97	3.01	-15.9

Note: Relative changes were calculated using the values reported in the respective assessments; minor discrepancies may occur due to rounding.

Source: systematised and calculated by the author based on [7–11].

The most important finding is that economic losses have increased faster than direct damage. The rise in the losses-to-damage ratio to 3.42 indicates that the economic cost of the war accumulates not only through the destruction of assets, but also through prolonged disruptions, additional operating costs, foregone revenues, and services that could not be provided. At the same time, the relative stability of the recovery-needs-to-damage ratio at around three after RDNA2 does not justify the use of a universal coefficient for converting damage into recovery needs. The aggregate ratio conceals substantial sectoral differences and depends on the selected recovery standard, the structure of prices, and methodological revisions.

For the purposes of this article, energy and extractive industries, transport, telecommunications and digital infrastructure, water supply and sanitation, and municipal services are combined into an analytical "RDNA infrastructure block" (Table 2). This grouping is used solely to ensure comparability across the five assessments and should not be equated with the legally defined list of critical infrastructure sectors. When moving from aggregate assessment to individual projects, priority should instead be determined by the criticality of the function, the number and scope of affected users, substitutability, cross-sectoral interdependencies, and cascading potential.

Table 2 – Dynamics of the RDNA Infrastructure Block across RDNA1–RDNA5

Indicator	RDNA1	RDNA2	RDNA3	RDNA4	RDNA5
Damage to the infrastructure block, USD billion	37.3	52.5	55.2	66.9	78.5
Share of total damage, %	38.3	39.0	36.2	38.0	40.2
Losses of the infrastructure block, USD billion	49.8	70.9	115.4	140.9	172.2
Share of total losses, %	19.8	24.5	23.1	23.9	25.8
Recovery needs of the infrastructure block, USD billion	98.9	156.4	148.0	169.4	218.9
Share of total recovery needs, %	28.4	38.1	30.4	32.4	37.2
Energy sector recovery needs, USD billion	10.4	47.0	47.1	67.8	90.6

Source: systematised and calculated by the author based on [7–11].

The recovery needs of the infrastructure block increased by USD 120.0 billion and accounted for approximately half of the overall increase in recovery needs between RDNA1 and RDNA5. The most recent interval between assessments is particularly illustrative: out of the USD 64.1 billion increase in total recovery needs,

approximately USD 49.5 billion, or 77.2%, was attributable to the infrastructure block. This indicates that the infrastructure component is becoming increasingly important not only as a consequence of physical destruction, but also as a source of prolonged functional losses.

Moving from aggregate recovery needs to an investment decision requires decomposition according to economic content. Within the proposed framework, basic physical restoration is separated from the costs of restoring service delivery, preparatory works, technological modernisation, and the resilience premium. Such a hierarchy reduces the risk of double counting while also making it possible to compare alternative target states of the system.

$$N_{r,s,t}^{(k)} = N_{r,s,t}^{base,(k)} + N_{r,s,t}^{serv,(k)} + N_{r,s,t}^{enable,(k)} + \Delta N_{r,s,t}^{mod,(k)} + \Delta N_{r,s,t}^{res,(k)}, \quad (2)$$

where r denotes the territory; s denotes the sector or critical function; t denotes the period; k denotes the scenario; N^{base} denotes basic physical restoration or replacement; N^{serv} denotes the costs of restoring service delivery and operational capacity; N^{enable} denotes demining, access provision, dismantling, design, and other preparatory activities; ΔN^{mod} denotes the additional cost of a modern technological equivalent; ΔN^{res} denotes expenditure on protection, redundancy, autonomy, decentralisation, cyber resilience, and the reduction of systemic risk.

A key property of the model is the dynamic nature of residual recovery needs. Even when investments are being implemented, residual needs may increase if new and repeated damage, reassessment effects, price changes, and higher recovery standards exceed the volume of completed works. This fundamentally distinguishes wartime recovery from one-off post-crisis reconstruction:

$$N_{i,t+1}^{resid} = N_{i,t}^{resid} + N_{i,t+1}^{new} + N_{i,t+1}^{repeat} + N_{i,t+1}^{reval} + N_{i,t+1}^{price} + N_{i,t+1}^{standard} + \Delta N_{i,t+1}^{res} - I_{i,t}^{impl} \quad (3)$$

Equation (3) shows that changes in residual needs result from two opposing flows. Residual needs increase as a result of new and repeated damage, reassessment, rising costs, new standards, and the resilience component, while they decrease through works actually implemented. Consequently, an increase in residual recovery needs does not in itself indicate an absence of reconstruction, just as a decline in residual needs does not necessarily demonstrate the full restoration of a critical function.

A second constraint is implementation capacity. Committed financial resources can be utilised only when there is an adequately prepared project portfolio, access to the facility, available equipment, contractors, and effective management coordination. The maximum volume of actual implementation is expressed as:

$$I_{i,t}^{impl} = \min\{I_{i,t}^{req}, CF_{i,t}, V_{i,t}^{ready}, C_{i,t}^{delivery}\} \cdot \varphi_{i,t}, \qquad 0 \le \varphi_{i,t} \le 1, \quad (4)$$

where $CF_{i,t}$ denotes committed financing; $V^{ready}_{i,t}$ denotes the value of the implementation-ready project portfolio; $C^{delivery}_{i,t}$ denotes the physical and institutional delivery capacity; $\varphi_{i,t}$ denotes a coefficient reflecting the impact of security,

122-147
v.38 (2026)
https://smart-scm.org

procurement, logistics, and coordination constraints. The use of the minimum operator prevents the model from assuming that resources can be utilised beyond any of the actual implementation limits.

The strategic trajectory determines not the pace at which funds are spent, but the target state that the recovery process is intended to achieve. The study identifies four alternatives (Table 3), forming a progression from the short-term restoration of basic operability to the transformation of the system configuration in order to reduce future risk. These alternatives should not be interpreted as interchangeable "better" or "worse" scenarios. The rationality of each depends on the criticality of the function, the decision horizon, the security environment, and implementation capacity

Table 3 – Comparative Characteristics of Strategic Trajectories for Resilient Recovery

Characteristic	Minimum-Restoration	Functional-Adaptive	BBB Modernisation	Resilience-Transformation
Objective	Rapid restoration of basic operability	Restoration of the critical function and reduction of downtime	Modern technological equivalent	New system configuration with lower systemic risk
Object of investment	Damaged asset	Function, reserve capacities, and temporary solutions	Asset + technological modernisation	System, network, interdependencies, and life cycle
Priority	Minimum CapEx, rapid repair	Critical loads, recovery time, substitutability	Efficiency, digitalisation, EU standards	Protection, decentralisation, redundancy, autonomy
Spatial logic	Predominantly the previous location	Selective relocation or mobile solutions	Reconsideration of location based on future demand	Dispersion of critical nodes and elimination of single points of failure
Financial logic	Emergency and budget financing	Blended financing for critical projects	International financial institutions, programme funding, private capital	Portfolio financing, guarantees, insurance, public-private partnerships
Expected outcome	Asset restored, with part of the previous vulnerability retained	More resilient operational function	Higher performance and compliance with standards	Lower future losses and greater system adaptability
Time horizon	Short term; emergency phase	Short- and medium-term; phased recovery	Medium- and long-term	Long-term; multi-phase transformation
Key performance criterion	Time required to restore basic operability	Share of the critical function restored and reduction in TTR	Life-cycle costs, efficiency, and technological outcomes	Reduction in expected losses, cascading risk, and residual vulnerability
Main risk of inappropriate application	Preservation of pre-existing vulnerability and repeated financing	Temporary solutions becoming permanent and fragmentation of the system	Technological overcomplication, delayed commissioning, and mismatch with future demand	Excessive capital intensity, coordination complexity, and system design errors

Source: developed by the author based on [5–14; 21; 24; 26; 27–29].

The proposed strategic trajectories should be interpreted not as four mutually exclusive stages of a single process, but as ideal-type investment regimes that define

different target states of the system and different logics for allocating scarce resources. At the national or sectoral portfolio level, they may be applied simultaneously, while for an individual facility they may replace one another sequentially. For example, the emergency restoration of a service may initially be achieved through a minimum-restoration or functional-adaptive solution, whereas capital modernisation or transformation may be undertaken after security and project conditions have stabilised. This approach reduces the risk of artificially selecting a single universal scenario for different sectors and territories [5; 12–13; 26].

Minimum-restoration trajectory. Its economic logic is based on minimising the time required to restore basic operability and the initial CapEx. It is rational for localised damage, emergency works, facilities with limited cascading potential, or as a temporary bridge towards a more sophisticated solution. At the same time, restoring a particular asset should not become an end in itself. If the critical function can be provided more effectively through another technological solution, relocated to another site, or integrated into a different network, the managed non-restoration of an obsolete asset may be economically more justified than mechanically reproducing the pre-war configuration [14; 24].

The principal risk associated with this trajectory arises from path dependence. Rapid repair of a centralised node, insufficient redundancy, or the repeated use of unique equipment may preserve previous vulnerabilities and create technological lock-in. Where the probability of repeated damage is high, a cheaper initial solution may generate higher expected costs of future repairs and service interruptions. The minimum-restoration regime should therefore be concluded not only with the commissioning of the facility, but also with an explicit assessment of residual risk and the conditions under which a transition to an adaptive, modernisation, or transformation model becomes necessary [5; 7–11; 21].

Functional-adaptive trajectory. Unlike the first model, its primary object is the critical service rather than a particular asset. The investment portfolio is formed from permanent, reserve, mobile, and organisational solutions that make it possible to reduce the functional deficit even before capital reconstruction has been completed. In the energy sector, such solutions may include mobile substations, distributed generation, or microgrids; in water supply, reserve sources and modular systems; and in digital infrastructure, duplicated communication channels, autonomous power supply, and backup data centres. Under conditions of prolonged wartime risk, this trajectory effectively allows investment not merely in physically restored assets, but in time and continuity of critical functions [5; 18; 21].

Its weakness lies in the risk that temporary solutions may become permanent. The accumulation of incompatible equipment, differing donor standards, and local bypass arrangements may reduce the future manageability of the system and increase operating costs. The functional-adaptive model therefore requires a predefined exit trajectory, including interoperability standards, rules for integrating temporary assets into the target architecture, and triggers for transition to modernisation. The key indicators in this case are the share of critical load restored, TTR, the availability of reserve capacity, and the duration of service interruptions, rather than the number of repaired facilities [20; 21].

Build Back Better modernisation trajectory. This model assumes that reconstruction should create a modern technological equivalent rather than a replica of the damaged asset. The investment decision incorporates life-cycle costs, energy and resource efficiency, digitalisation of management, maintainability, compatibility with European Union standards, and alignment with the expected structure of

future demand. Its application is most justified where the future function is expected to remain consistently necessary, the project has a sufficiently long operating horizon, and the operator has the capacity to maintain a technologically more complex solution [12–14; 24; 26].

At the same time, Build Back Better should not be equated with maximising technical complexity. Overdesign, a prolonged project cycle, or dependence on uncertain future demand may increase the losses associated with delayed commissioning. Moreover, new equipment does not in itself eliminate systemic vulnerability: a highly efficient but excessively centralised node without adequate redundancy may remain a single point of failure. The modernisation trajectory is therefore economically justified when the life-cycle and technological benefits exceed the cost of delayed commissioning and when the project simultaneously meets minimum thresholds for security, autonomy, and maintainability [5; 12–13].

Resilience-transformation trajectory. Its defining feature is that it changes not an individual asset, but the configuration of the infrastructure system itself. It is most justified for functions characterised by high criticality, low substitutability, substantial cross-sectoral interdependencies, and a high probability of repeated or compound impacts. Investment is directed towards alternative routes, the spatial dispersion of critical nodes, consumer autonomy, physical and cyber protection, decentralised capacity, and rapid reconnection mechanisms. In this case, the resilience premium cannot be defined as a single percentage of the value of damage. Its economic meaning depends on the extent to which additional investment reduces expected future losses and shortens the duration of functional deficits [12–13; 21; 26].

The transformation model places the greatest demands on data, project preparation, and coordination, because a system design error may be more costly than a local repair error. At the same time, it does not necessarily imply restoring a larger number of assets. Some obsolete or excessively vulnerable nodes may be replaced by alternative technologies, relocated, or excluded from the future system configuration. The performance of this trajectory should therefore be assessed not by the amount of CapEx utilised, but by the reduction in residual systemic risk, shorter TTR, the magnitude of avoided losses, and a reduction in cascading potential [5; 14; 21; 26].

In practice, the choice of trajectory should be regarded as conditional rather than prescriptive. As the criticality of a function, the recurrence of threats, and cascading potential increase, and as substitutability declines, the case for functional-adaptive and resilience-transformation solutions becomes stronger. Conversely, high urgency combined with low project readiness increases the role of minimum-restoration and adaptive measures. In a stabilisation and post-war environment, when the inflow of new damage declines and the planning horizon becomes longer, part of the portfolio will naturally shift towards modernisation and systemic transformation. The strategic trajectory is therefore a controllable variable of investment policy rather than a direct function of the fact of destruction itself.

For a methodologically sound scenario analysis, the strategic choice must be separated from the external environment. A scenario is defined as a combination of a strategic trajectory and a risk environment:

$$S_k = T_q \times E_p, \quad (5)$$

where Tq denotes the strategic trajectory and Ep denotes the external risk environment. This two-dimensional framework separates the controllable strategic choice from

122-147
v.38 (2026)
https://smart-scm.org

conditions that arise beyond the boundaries of a specific project.

Table 4 – Characteristics of External Risk Environments

Risk Environment	Security Characteristics	Macroeconomic and Financial Conditions	Data and Access	Implications for the Model
Stabilisation and post-war transition	Substantial decline in the intensity of attacks; persistence of localised, mine-related, cyber, and technological risks	More predictable funding flows, but persistently high demand for capital and reconstruction resources	Improved access and verification; territorial and demographic uncertainties remain	Lower inflow of new damage; greater scope for longer-term integrated projects; increasing share of modernisation
Prolonged wartime risks	Regular attacks on particular sectors and territories	Limited availability of long-term capital; high dependence on international support	Uneven access; periodic revision of data	Phased implementation, mobile solutions, redundancy, and priority given to rapid restoration of critical functions
Escalation and compound threats	Intensive repeated attacks; cyber and cascading impacts	Higher risk premium, more expensive resources, and tight fiscal constraints	Significant areas of uncertainty and restricted access	Increase in new and repeated damage; higher protection costs; preference for autonomous and spatially dispersed solutions

Source: developed by the author taking into account [7–11; 14; 24].

Table 5 – "Strategic Trajectory – Risk Environment" Matrix

Strategic Trajectory	Stabilisation / Post-War Transition	Prolonged Wartime Risks	Escalation and Compound Threats
Minimum-restoration	Selective repair only where modernisation is economically unjustified or the function has low criticality	Rapid emergency repairs with a high risk of repeated financing	Limited to the urgent restoration of local vital functions
Functional-adaptive	Transitional model leading to subsequent modernisation; reserve capacities serve as a contingency layer	Core approach based on mobility, redundancy, phased implementation, and rapid restoration of functions	Autonomous and mobile solutions for critical loads become predominant
BBB modernisation	Principal mode of technological renewal and alignment with European Union standards	Phased modernisation of the most implementation-ready and adequately protected projects	Applied selectively to facilities where a longer implementation cycle does not create an unacceptable service deficit
Resilience-transformation	System-level redesign of networks, elimination of critical dependencies and single points of failure	Selective transformation of nodes with high cascading potential	Highest relevance for critical systems, but also the most demanding in terms of protection, financing, and coordination

Source: proposed and developed by the author based on the analysis of reports by international organisations and analytical centres and the findings of previous studies [27–29].

The risk environment (Table 4) determines the intensity of new and repeated damage, the risk premium, access to capital, and the level of informational uncertainty, whereas the strategic trajectory determines the target state, the additional modernisation

122-147
v.38 (2026)
https://smart-scm.org

or resilience component, the pace of actual implementation, and the mechanism through which future risk is reduced.

The matrix should therefore not be interpreted as a set of twelve independent forecasts, but rather as a stress-testing architecture (Table 5). It makes it possible to compare alternative management decisions under the same level of external pressure and to test the robustness of a particular strategy as the external environment changes.

For the purpose of testing the proposed scenario framework, the recovery needs of the RDNA5 infrastructure block, amounting to USD 218.9 billion as of 31 December 2025, were used as the baseline [11]. The numerical simulation is conducted under a single assumed baseline level of external pressure approximating a prolonged wartime risk environment. This assumption deliberately holds the external component constant in order to isolate the effect of strategic choice itself. The full matrix is subsequently used as a framework for stress-testing the parameters under stabilisation or escalation conditions. The calculation is methodological in nature and should not be interpreted as a statistical forecast or an official estimate of financing requirements. Its purpose is to demonstrate the direction of change in residual needs under different combinations of the rate of new damage, additional expenditure on modernisation and resilience, the effect of future risk reduction, and the actual capacity to implement investment projects.

The simplified equation describing the simulation dynamics is expressed as:

$$N_{t+1}^{(s)} = N_t^{(s)}\left(1 + g_r - \alpha_s + \pi_{s,t} - m_s\right), \quad (6)$$

where N^s_t denotes the residual need under trajectory s at the beginning of year t; g^r denotes the exogenous rate of increase resulting from new damage, reassessment, and price changes; α_s denotes the effect of reducing future risk; $\pi_{s,t}$ denotes the additional modernisation or resilience component; m_s denotes the share of the initial recovery need that can actually be implemented during the year. For the methodological simulation, g^r is assumed to be 8% for all trajectories, while the remaining parameters are differentiated according to the substantive characteristics of the respective strategies (Tables 6, 7).

Table 6 – Simulation Parameters under the Baseline Risk Environment

Parameter	Minimum-Restoration	Functional-Adaptive	BBB Modernisation	Resilience-Transformation
Exogenous growth in needs g^r, %	8	8	8	8
Future risk reduction effect α_s, percentage points	0	2	4	6
Additional component $\pi_{s,t}$ in 2026–2027, %	0	2	4	8
Additional component $\pi_{s,t}$ in 2028, %	0	2	4	4
Additional component $\pi_{s,t}$ in 2029–2030, %	0	2	2	2
Share of actual implementation m_s, %	5	10	12	15
Net rate in 2026–2027, %	+3	-2	-4	-5
Net rate in 2028, %	+3	-2	-4	-9
Net rate in 2029–2030, %	+3	-2	-6	-11

Note: The parameters represent scenario assumptions used for methodological testing and should be subject to sensitivity analysis.

Source: author's assumptions based on the dynamics of RDNA1–RDNA5 [7–11].

122-147
v.38 (2026)
https://smart-scm.org

Table 7 – Simulated Dynamics of Residual Recovery Needs of the Infrastructure Block, USD Billion

Trajectory	2025, baseline	2026	2027	2028	2029	2030
Minimum-Restoration	218.9	225.5	232.2	239.2	246.4	253.8
Functional-Adaptive	218.9	214.5	210.2	206.0	201.9	197.9
BBB Modernisation	218.9	210.1	201.7	193.7	182.0	171.1
Resilience-Transformation	218.9	208.0	197.6	179.8	160.0	142.4

Source: calculated by the author using Equation (6).

The results presented in Table 8 reveal fundamentally different patterns of long-term dynamics. The minimum-restoration option does not offset the inflow of new damage and reassessment effects: under the specified parameters, residual needs increase to USD 253.8 billion by 2030. The functional-adaptive trajectory shifts the system towards a moderate reduction in residual needs, bringing them down to USD 197.9 billion. Despite a higher additional component in the initial years, the BBB modernisation trajectory reduces residual needs to USD 171.1 billion, while the resilience-transformation trajectory lowers them further to USD 142.4 billion.

Table 8 – Summary Results of the Simulation for 2026–2030

Trajectory	Estimated Investment Implemented over 5 Years, USD Billion	Residual Needs in 2030, USD Billion	Change from the 2025 Baseline, %	Dominant Outcome
Minimum-Restoration	58.1	253.8	+15.9	Substantial volume of repairs without reversing the accumulation of residual needs
Functional-Adaptive	105.2	197.9	-9.6	Stabilisation of residual needs and faster restoration of critical functions
BBB Modernisation	120.8	171.1	-21.8	Technological upgrading and sustained reduction in residual needs
Resilience-Transformation	144.6	142.4	-34.9	System-wide reduction in vulnerability and cascading risk

Note: The amounts of investment implemented are elements of the scenario simulation rather than a budget forecast.

Source: calculated by the author.

This result does not imply that the most expensive trajectory is automatically preferable for every facility. Rather, it demonstrates a nonlinear trade-off: higher initial expenditure on protection, redundancy, and system reconfiguration may reduce the future accumulation of needs and shorten the duration of functional disruptions. A comparison based solely on current CapEx therefore systematically undervalues alternatives whose economic benefits emerge over the infrastructure life cycle.

For the practical selection of a scenario, the residual level of investment needs alone is insufficient. It is advisable to consider simultaneously the volume of investment, the functional outcome achieved, the recovery time, the increase in resilience, and the present value of avoided losses. A composite criterion may be expressed as:

122-147
v.38 (2026)
https://smart-scm.org

$$Score_s = w_1(1 - \tilde{I}_s) + w_2\tilde{R}_s^{func} + w_3\left(1 - \widetilde{TTR}_s\right) + w_4\widetilde{RG}_s + w_5\widetilde{AL}_s, \quad (7)$$

where the normalised indicators represent, respectively, the investment burden, the degree of functional restoration, the time required to restore the function, the increase in resilience, and avoided future losses; w_j denotes the weight assigned to criterion jj, with the sum of all weights equal to one. The weights should be determined on a sector-specific basis: for energy, water supply, or emergency medical infrastructure, greater importance should be assigned to speed and continuity of service, whereas for long-term transport projects, life-cycle costs, capacity, and network effects should carry greater weight.

Scenario-based assessment of investment needs should also be linked to the actual capacity to transform long-term needs into an annual project portfolio (Table 9). The RDNA2–RDNA5 data reveal a substantial gap between ten-year recovery estimates and the scale of annual priorities. During 2023–2026, annual priorities accounted for only 2.59–3.43% of long-term recovery needs, while committed financing in 2024–2026 covered less than half of the identified annual priorities [8–11].

Table 9 – Long-Term Recovery Needs, Annual Priorities, and Financial Provision

Indicator	RDNA2 / 2023	RDNA3 / 2024	RDNA4 / 2025	RDNA5 / 2026
Long-term recovery needs, USD billion	410.6	486.2	523.6	587.7
Annual priorities, USD billion	14.1	15.3	17.32	15.245
Annual priorities / long-term recovery needs, %	3.43	3.15	3.31	2.59
Committed financing, USD billion	n/a	approximately 5.5	7.37	5.765
Financing gap, USD billion	n/a	approximately 9.5	9.96	9.48
Coverage of annual priorities, %	n/a	approximately 35.9	42.6	37.8

Note: Due to rounding and differences in financing categories, the sum of committed resources and the financing gap may not exactly equal the annual priority.

Source: systematised and calculated by the author based on [8–11].

The financing gap is defined as the difference between the annual priority need and committed financing:

$$FG_t = N_t^{priority} - CF_t. \quad (8)$$

However, this indicator captures only one component of the overall shortfall. Even full financial coverage does not eliminate shortages of implementation-ready projects, equipment, contractor capacity, permits, secure access, and operational capability. Portfolio formation should therefore distinguish at least between financial, project preparation, implementation, technical, functional, and resilience gaps.

Project prioritisation cannot be based solely on the value of the damaged asset or the extent of its physical destruction. To compare alternatives, a multi-criteria index is proposed (Table 10), combining function criticality, functional deficit, population coverage, cross-sectoral interdependencies,

122-147
v.38 (2026)
https://smart-scm.org

substitutability, recovery time, resilience gains, avoided losses, project readiness, financial feasibility, and implementation capacity:

$$PRI_i = \sum_{j=1}^{m} w_j z_{ij}, \qquad \sum_{j=1}^{m} w_j = 1, \qquad w_j \geq 0, \tag{9}$$

where z_{ij} denotes the normalised value of criterion j for project i, and w_j denotes the weight assigned to that criterion. For indicators where a lower value is preferable, such as recovery time or substitutability when interpreted in terms of high irreplaceability, inverse normalisation is applied. The weights should be transparent, tested for sensitivity, and, where possible, determined separately for different sectoral groups.

Table 10 – Criteria for Prioritising Critical Infrastructure Investment Projects

Criterion	Economic Rationale	Preferred Direction	Example Indicator
Criticality	Importance of the function for vital societal needs and security	Maximum	Composite criticality index
Functional deficit	Scale of the service that is unavailable or provided at a reduced level	Maximum	Share of lost capacity, %
Coverage	Population and organisations dependent on the function	Maximum	Number of users
Cross-sectoral impact	Number and strength of dependent functions	Maximum	Interdependency / cascading potential index
Substitutability	Possibility of providing the service through alternative means	Minimum	Switching time and share of demand that can be redirected
Recovery time	Time required to restore the target function	Minimum	Days / months
Resilience gain	Reduction in vulnerability after project implementation	Maximum	Change in expected risk
Avoided losses	Expected economic benefit	Maximum	Discounted value of avoided losses
Project readiness	Availability of documentation, permits, and procurement readiness	Maximum	Readiness stage, %
Financial feasibility	Realism of financing sources and cost of capital	Maximum	Share of committed financing
Implementation capacity	Ability to implement and subsequently operate the project	Maximum	Capacity coefficient

Source: proposed by the author based on the analysis of [5; 7–11; 18; 22; 26; 27–29].

A unified scenario logic does not imply the use of identical parameters across all sectors. Energy, transport, digital infrastructure, water supply, and municipal systems differ in the duration of project cycles, the nature of network interdependencies, the potential for private financing, and the consequences of functional deficits. For this reason, applying a universal resilience premium or assuming the same implementation rate across sectors would be methodologically unjustified.

In the energy sector, priority is determined by available capacity, critical loads, redundancy, and the effects on dependent systems; in transport, by route capacity, the availability of alternatives, and network bottlenecks; in digital infrastructure, by network availability, power autonomy, channel redundancy, and cyber resilience; in water supply, by the ability to localise failures, the availability of reserve sources, and dependence on energy supply; while for municipal infrastructure, territorial differentiation, migration-related changes,

and the capacity of local communities become particularly important. The value of a damaged asset should therefore be supplemented by functional and systemic criteria.

A separate limitation concerns the RDNA data. The five assessments do not constitute a regular statistical time series, and their values reflect not only new physical damage but also reassessment effects, price and exchange-rate changes, revisions to classifications, and partial accounting for completed recovery works [7–11]. The simulation for 2026–2030 should therefore be interpreted as a scenario experiment rather than a forecast. A transition to autoregressive or other forms of statistical forecasting would require the construction of a harmonised quarterly or monthly time series in constant prices, consistent sectoral boundaries, a clear distinction between gross and residual needs, and the inclusion of explanatory variables capturing new damage, financing, implementation, risk, and price dynamics.

Taking these limitations into account, the proposed approach should be regarded as a tool for economic and portfolio-level decision-making prior to detailed engineering design. Its practical value lies in the possibility of comparing alternatives within a common analytical framework without reducing reconstruction performance to the amount of funds disbursed. The decisive criterion becomes the relationship between "investment – function – time – risk – avoided losses." A trajectory can be considered justified when, given the criticality of the function, the acceptable duration of service disruption, and actual resource constraints, it provides the best balance between the speed of service restoration and the reduction in the expected cost of future disruptions.

Conclusions.

The study has shown that investment needs for the recovery of Ukraine's critical infrastructure cannot be treated as a fixed value derived directly from the monetary scale of physical destruction. Under conditions of an ongoing war, these needs evolve dynamically under the influence of accumulated, new, and repeated damage; economic losses resulting from disruptions to critical functions; changes in the cost of works and equipment; the selected recovery standard; the availability of financing; project readiness; and the actual capacity to implement investment projects. Economically justified assessment should therefore be based not only on the value of the damaged asset, but also on the functional condition that the infrastructure system needs to achieve and the level of future risk that can be considered acceptable.

The analysis of RDNA1–RDNA5 confirmed that economic losses have accumulated faster than direct damage. Between the first and fifth assessments, direct damage increased by 100.3%, economic losses by 164.6%, and ten-year recovery needs by 68.6%. Under RDNA5, the needs of the infrastructure block constructed for the purposes of this study reached USD 218.9 billion, accounting for 37.2% of total estimated recovery needs. This indicates that the economic consequences of infrastructure destruction are determined not only by the physical loss of assets, but also by the duration of service disruptions, the scale of functional deficits, and the cascading transmission of adverse effects across interdependent sectors.

The proposed scenario framework is based on four strategic trajectories: minimum-restoration, functional-adaptive, Build Back Better modernisation, and resilience-transformation. These trajectories differ primarily in the target condition of the infrastructure, ranging from the rapid restoration of basic operability to a deeper transformation of the system configuration aimed at reducing future losses and systemic vulnerability. Importantly, these trajectories are not treated as a universal sequence or a rigid hierarchy. The rationality of each depends on the criticality of the function, time constraints, available resources, the level of

threats, substitutability, and cascading potential.

One of the key results of the study is the development of a two-dimensional scenario architecture based on the relationship "strategic trajectory – risk environment." The matrix combines four management alternatives with three types of external conditions: a stabilisation and post-war transition environment, a prolonged wartime risk environment, and an environment characterised by the escalation of compound threats. This distinction makes it possible to separate controllable recovery parameters from exogenous conditions and, consequently, to compare alternatives more accurately under the same level of external pressure or to assess the robustness of a particular trajectory under different scenarios for the evolution of the security environment.

The simulation exercise based on the RDNA5 needs of the infrastructure block demonstrated substantially different dynamics of residual investment needs. Under the adopted scenario assumptions, the minimum-restoration trajectory does not offset the inflow of new damage and reassessment effects, causing residual needs to increase to USD 253.8 billion by 2030. Under the functional-adaptive trajectory, residual needs decline to USD 197.9 billion; under the modernisation trajectory, to USD 171.1 billion; and under the resilience-transformation trajectory, to USD 142.4 billion. These values should not be interpreted as forecasts of future budget expenditure or financing. Their analytical significance lies elsewhere: higher initial expenditure may be economically justified if it slows the accumulation of new needs, shortens the duration of functional disruptions, and reduces expected losses over the infrastructure life cycle.

A further result concerns the distinction between long-term needs, annual priorities, committed financing, realised investment, and the actual functional outcome achieved. During 2023–2026, annual priorities represented only about 2.6–3.4% of long-term needs, while in 2024–2026 committed financing covered less than half of the identified priorities. At the same time, insufficient capital is not the only limiting factor. Between estimated needs and the level of functionality ultimately achieved, financial, project preparation, implementation, technical, functional, and resilience gaps may emerge successively. The amount of financing mobilised or actually utilised therefore cannot be treated as a self-sufficient indicator of reconstruction performance.

The scientific novelty of the results lies in the further development of a scenario-based approach to assessing critical infrastructure investment needs through the integration of several analytical components: distinguishing the strategic trajectory as the outcome of a management decision from the risk environment as an exogenous condition; constructing a matrix of twelve scenario combinations; representing residual investment needs as a dynamic variable that changes under the influence of new and repeated damage, realised investment, and the modernisation and resilience components; and incorporating financial, project preparation, and implementation capacity into the transition from estimated needs to the achieved functional outcome. The approach to evaluating investment alternatives has also been further developed through the relationship "investment – function – time – risk – avoided losses," which shifts the selection criterion away from minimising initial expenditure towards assessing outcomes over the entire life cycle.

The practical significance of the proposed approach lies in its potential application at the stages of scenario testing, investment portfolio formation, and preliminary project prioritisation before proceeding to detailed feasibility assessment and engineering design. Depending on the level of governance, the following targeted recommendations can be proposed:

– The Cabinet of Ministers of Ukraine and central executive authorities should complement the criterion based on the scale of physical destruction with indicators of function criticality, the duration of functional deficit, substitutability, cascading potential, and the expected reduction in future risk.

– Sectoral ministries and critical infrastructure operators should establish sector-specific requirements for acceptable recovery time, redundancy, autonomy, physical and cyber protection, and should justify the resilience component of investment not through a universal coefficient, but on the basis of the characteristics of the specific function and infrastructure system concerned.

– Regional military administrations and local self-government authorities should align infrastructure projects with territorial planning, demographic changes, the spatial relocation of population and businesses, future demand, and the actual operational capacity of territories.

– International financial institutions, donors, and development banks should distinguish between financing for emergency recovery, functional adaptation, modernisation, and systemic transformation, while linking financial support to project readiness, expected functional outcomes, and the capacity of the project to reduce long-term risk.

– Private investors, banks, and insurance institutions should assess infrastructure projects with due consideration of life-cycle costs, the risk of repeated damage, mechanisms for guarantees and war-risk insurance, and the economic effects arising from reduced future losses.

The study has several limitations that define the boundaries within which its results should be interpreted. RDNA1–RDNA5 represent successive analytical snapshots rather than a homogeneous statistical time series: the assessments were prepared as of different dates, cover different durations of the war, and incorporate changes in sectoral boundaries, price parameters, and the treatment of needs that had already been met. The simulation parameters used in the study therefore serve a methodological rather than forecasting purpose. The RDNA infrastructure block constructed for the analysis was used solely to ensure comparability over time and should not be regarded as equivalent to Ukraine's legally defined critical infrastructure system. The proposed model also does not replace engineering analysis of individual facilities and, at this stage, does not incorporate a fully parameterised matrix of cross-sectoral interdependencies, empirically estimated probabilities of repeated damage, or sector-specific functions of avoided losses.

Future research should focus on testing the proposed scenario model using actual data from individual sectors of Ukraine's critical infrastructure. This will require the development of comparable dynamic data series reflecting the scale of damage, residual investment needs, volumes of financing, actual project implementation, and changes in the intensity of risks. Such an empirical database would make it possible to gradually replace conditionally specified scenario parameters with empirically grounded estimates and to determine more precisely how different strategic recovery trajectories affect the scale and dynamics of investment needs over the long term.

Use of artificial intelligence

During the preparation of this manuscript, the author used ChatGPT (OpenAI, GPT-5.6 Sol) to assist with the translation of the manuscript from Ukrainian into English and for subsequent language editing and stylistic refinement, including improvements in grammar, academic wording, clarity, consistency, and readability. Artificial intelligence was used exclusively as a language-support tool and was not used to formulate the research problem, research design, methodology, analytical framework, or scientific hypotheses; to perform data

analysis, calculations, modelling, or statistical procedures; to generate or interpret the research results; or to develop the scientific conclusions. All AI-assisted translations and language revisions were carefully reviewed and verified by the author to ensure their accuracy and consistency with the original scientific meaning. The author takes full responsibility for the content and final version of the manuscript.

References

1. Mentges, A., Halekotte, L., Schneider, M., Demmer, T., & Lichte, D. (2023). A resilience glossary shaped by context: Reviewing resilience-related terms for critical infrastructures. International Journal of Disaster Risk Reduction, 96, 103893. https://doi.org/10.1016/j.ijdrr.2023.103893

2. Mitoulis, S.-A., Argyroudis, S., Panteli, M., Fuggini, C., Valkaniotis, S., Hynes, W., & Linkov, I. (2023). Conflict-resilience framework for critical infrastructure peacebuilding. Sustainable Cities and Society, 91, 104405. https://doi.org/10.1016/j.scs.2023.104405

3. Caetano, H. O., Desuó, N. L., Fogliatto, M. S. S., & Maciel, C. D. (2024). Resilience assessment of critical infrastructures using dynamic Bayesian networks and evidence propagation. Reliability Engineering & System Safety, 241, 109691. https://doi.org/10.1016/j.ress.2023.109691

4. Eichengreen, B. (2007). The European economy since 1945: Coordinated capitalism and beyond. Princeton University Press.

5. Global Facility for Disaster Reduction and Recovery. (2020). Disaster recovery framework guide (Revised version) [Report]. World Bank Group. https://www.gfdrr.org/en/publication/disaster-recovery-framework-guide

6. United Nations Development Group, World Bank, & European Union. (2013). Post-disaster needs assessments: Volume A: Guidelines [Report]. World Bank Group. https://www.gfdrr.org/en/publication/post-disaster-needs-assessments-guidelines-volume-2013

7. World Bank, Government of Ukraine, & European Commission. (2022). Ukraine rapid damage and needs assessment, August 2022 [Report]. World Bank. https://doi.org/10.1596/37988

8. World Bank Group, Government of Ukraine, European Commission, & United Nations. (2023). Ukraine rapid damage and needs assessment: February 2022–February 2023 [Report]. World Bank Group. https://documents1.worldbank.org/curated/en/099184503212328877/pdf/P1801740d1177f03c0ab180057556615497.pdf

9. World Bank Group, Government of Ukraine, European Commission, & United Nations. (2024). Ukraine third rapid damage and needs assessment: February 2022–December 2023 [Report]. World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099021324115085807

10. World Bank Group, Government of Ukraine, European Union, & United Nations. (2025). Ukraine fourth rapid damage and needs assessment: February 2022–December 2024 [Report]. World Bank Group. https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099022025114040022

11. World Bank Group, Government of Ukraine, European Union, & United Nations. (2026). Ukraine fifth rapid damage and needs assessment: February 2022–December 2025 [Report]. World Bank Group. https://documents1.worldbank.org/curated/en/099022026094036395/pdf/P514499-22f93f3a-4278-42bc-b907-db9553d12069.pdf

12. Global Facility for Disaster Reduction and Recovery. (2017). Building back better in post-disaster recovery: Guidance note [Guidance note]. https://www.gfdrr.org/sites/default/files/Disaster%20Recovery%20Guidance%20Series-%20Building%20Back%20Better%20in%20Post-Disaster%20Recovery.pdf

13. Hallegatte, S., Rentschler, J., & Walsh, B. (2018). Building back better: Achieving resilience through stronger, faster, and more inclusive post-disaster reconstruction. World Bank. https://doi.org/10.1596/29867

14. Becker, T., Eichengreen, B., Gorodnichenko, Y., Guriev, S., Johnson, S., Mylovanov, T., Rogoff, K., & Weder di Mauro, B. (2022). A blueprint for the reconstruction of Ukraine. CEPR Press.

15. Liu, W., Shan, M., Zhang, S., Zhao, X., & Zhai, Z. (2022). Resilience in infrastructure systems: A comprehensive review. Buildings, 12(6), 759. https://doi.org/10.3390/buildings12060759

16. Sathurshan, M., Saja, A., Thamboo, J., Haraguchi, M., & Navaratnam, S. (2022). Resilience of critical infrastructure systems: A systematic literature review of measurement frameworks. Infrastructures, 7(5), 67. https://doi.org/10.3390/infrastructures7050067

17. Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., & Setunge, S. (2022). Improving the resilience of critical infrastructures: Evidence-based insights from a systematic literature review. International Journal of Disaster Risk Reduction, 81, 103123. https://doi.org/10.1016/j.ijdrr.2022.103123

18. Sukhodolia, O. M. (2023). Stiikist krytychnoi infrastruktury ta zhyttievo vazhlyvykh funktsii i posluh: formalizatsiia zavdan i zmistu dii subiektiv zabezpechennia. Stratehichna panorama, 2, 5–20. https://doi.org/10.53679/2616-9460.2.2023.01

19. Shpatakova, O. L., Ivanenko, R. O., & Pohrebytskyi, M. L. (2022). Perspektyvy vidnovlennia krytychnoi infrastruktury na deokupovanykh terytoriiakh Ukrainy. Ekonomika ta suspilstvo, 40. https://doi.org/10.32782/2524-0072/2022-40-5

20. Mykytenko, V. V. (2023). Povoienne vidnovlennia ta rozvytok krytychnoi infrastruktury Ukrainy. Visnyk ekonomichnoi nauky Ukrainy, 1(44), 124–138. https://doi.org/10.37405/1729-7206.2023.1(44).124-138

21. Hallegatte, S., Rentschler, J., & Rozenberg, J. (2019). Lifelines: The resilient infrastructure opportunity. World Bank. https://documents1.worldbank.org/curated/en/111181560974989791/pdf/Lifelines-The-Resilient-Infrastructure-Opportunity.pdf

22. Murasov, R. K., & Melnyk, Ya. V. (2023). Rezultaty otsiniuvannia zahroz krytychnii infrastrukturi metodom ekspertnoho otsiniuvannia. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 48(3), 83–88. https://doi.org/10.33099/2311-7249/2023-48-3-83-88

23. Lazor, O. Ya., Yunyk, I. H., & Zabolotnyi, A. V. (2024). Derzhavna stratehiia povoiennoho vidnovlennia ta rozvytku krytychnoi infrastruktury v Ukraini. Derzhavne upravlinnia: udoskonalennia ta rozvytok, 4, 1–19. https://doi.org/10.32702/2307-2156.2024.4.2

24. OECD. (2022). The architecture of infrastructure recovery in Ukraine. OECD Publishing. https://doi.org/10.1787/d768a2e4-en

25. Mallett, R., & Pain, A. (2018). Post-war recovery and the role of markets: Policy insights from six years of research. Global Policy, 9(2), 264–275. https://doi.org/10.1111/1758-5899.12560

26. OECD. (2026). Infrastructure policy review of Ukraine. OECD Publishing. https://doi.org/10.1787/eeef2059-en

27. Khaustova, V. Ye., & Trushkina, N. V. (2025). Zahrozy rozvytku krytychnoi infrastruktury: sutnist i klasyfikatsiia. Problemy ekonomiky, 3, 89–104. https://doi.org/10.32983/2222-0712-2025-3-89-104

28. Kyzym, M. O., Khaustova, V. Ye., & Trushkina, N. V. (2026). Kompleksnyi pidkhid do upravlinnia ryzykamy rozvytku krytychnoi infrastruktury rehioniv Ukrainy v umovakh zovnishnikh zahroz. Infrastruktura rynku, 88, 70–78. https://doi.org/10.32782/infrastruct88-11

29. Kyzym, M. O., Kozyrieva, O. V., & Trushkina, N. V. (2026). Mizhnarodni instrumenty povoiennoi vidbudovy krytychnoi infrastruktury ta yikh adaptatsiia dlia rehioniv Ukrainy. Efektyvna ekonomika, 1. https://doi.org/10.32702/2307-2105.2026.1.22

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

148-161
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-10

UDC 351.78:004.9
JEL Classification: H83, O33, R50

Received: 2026-07-24
Accepted: 2026-08-28
Published: 2026-08-30

Sporyshev K. O. Doctor of Science in Public Administration, Associate Professor, Deputy Head of the Educational and Scientific Institute for Training of Management Personnel in Scientific Work – Head of the Scientific and Research Laboratory of Construction and Operational Application of the National Guard of Ukraine, National Academy of the National Guard of Ukraine, (Ukraine)

ORCID – 0000-0003-4737-9698
Researcher ID J-5960-2018
Scopus author id: – 59047032200
E-Mail: spor_kos@ukr.net

Bondarenko O. H. Doctor of Science in Public Administration, Associate Professor Head of the Logistics Management Department of the Educational and Scientific Institute for Management Training National Academy of the National Guard of Ukraine (Ukraine)

ORCID – 0000-0003-1755-3333
Researcher ID J-5705-2018
Scopus author id: – 57687413400
E-Mail: Alexanderbondarenko77@gmail.com

"SAFE CITY" AS A SECURITY COMPONENT OF THE SMART CITY CONCEPT: PUBLIC AND MANAGEMENT ASPECT

Sporyshev Kostyantyn, Bondarenko Oleksandr "Safe City" as a security component of the Smart City concept: public and management aspect". *The article examines the Safe City concept in the context of Smart City development and determines its public governance dimension in the conditions of digital transformation of the urban environment. It is substantiated that the contemporary understanding of Smart City is gradually moving beyond a purely technological approach and increasingly encompasses the efficiency of public governance, sustainable development, the quality of urban services, human and social capital, and the implementation of data-driven governance. The key components of Smart City – Smart Governance, Smart Economy, Smart Mobility, Smart Environment, Smart People, and Smart Living – are analyzed, with particular attention paid to their security dimension. It is established that security has a cross-cutting nature and includes the protection of information systems and data, cybersecurity, transport and public safety, economic and infrastructure resilience, prevention of environmental and technological threats, and the development of a public safety culture.*

The evolution and transformation of the Safe City concept are examined. A gradual transition is identified from local video surveillance and crime-recording systems towards the integrated use of digital technologies, intelligent video analytics, geographic information systems, Internet of Things devices, big data, and interagency information exchange tools. Particular attention is paid to the changing role of data in urban

148-161
v.38 (2026)
https://smart-scm.org

security governance and its use for monitoring, threat detection, risk assessment, forecasting, and decision-making support.

The public governance dimension of the Safe City system is determined through a combination of monitoring, information and analytical, coordination, organizational, preventive, and control functions, as well as the function of supporting managerial decision-making. It is demonstrated that the digitalization of urban security creates the prerequisites for a transition from a predominantly reactive model of responding to hazardous events towards preventive and risk-oriented governance. It is emphasized that the effectiveness of the Safe City system should be assessed not by the number of surveillance technologies deployed, but by its capacity to ensure timely threat detection, information exchange, interagency coordination, well-grounded managerial decisions, and rapid response while simultaneously respecting human rights and freedoms.

***Keywords**:* Smart City, Safe City, public governance, digitalization, urban security, digital technologies, data-driven governance, managerial decision-making, security risks, urban environment, national security

Костянтин Споришев, Олександр Бондаренко. «Безпечне місто» як безпекова складова концепції Smart City: публічно-управлінський аспект». *У статті досліджено концепцію «Безпечне місто» у контексті розвитку Smart City та визначено її публічно-управлінський зміст в умовах цифрової трансформації міського середовища. Обґрунтовано, що сучасне розуміння Smart City поступово виходить за межі технологічного підходу та охоплює питання ефективності публічного управління, сталого розвитку, якості міських послуг, використання людського і соціального капіталу та впровадження управління, заснованого на даних. Проаналізовано основні складові Smart City: Smart Governance, Smart Economy, Smart Mobility, Smart Environment, Smart People та Smart Living – та визначено їх безпековий вимір. Встановлено, що безпека має наскрізний характер та охоплює захист інформаційних систем і даних, кібербезпеку, транспортну та громадську безпеку, економічну й інфраструктурну стійкість, попередження екологічних і техногенних загроз, а також формування культури безпеки населення.*

Досліджено становлення та трансформацію концепції Safe City («Безпечне місто»). Встановлено поступовий перехід від використання локальних систем відеоспостереження та фіксації правопорушень до комплексного застосування цифрових технологій, інтелектуальної відеоаналітики, геоінформаційних систем, пристроїв Інтернету речей, великих масивів даних та засобів міжвідомчого інформаційного обміну. Особливу увагу приділено зміні ролі даних у системі забезпечення міської безпеки та їх використанню для моніторингу, виявлення загроз, оцінювання ризиків, прогнозування та підтримки прийняття управлінських рішень.

Визначено публічно-управлінський зміст системи «Безпечне місто» через сукупність моніторингової, інформаційно-аналітичної, координаційної, організаційної, превентивної, контрольної функцій та функції підтримки прийняття управлінських рішень. Доведено, що цифровізація міської безпеки створює передумови для переходу від переважно реактивної моделі реагування на небезпечні події до превентивного та ризик-орієнтованого управління. Наголошено, що ефективність системи «Безпечне місто» повинна визначатися не кількістю технічних засобів спостереження, а здатністю забезпечувати своєчасне виявлення загроз, інформаційну взаємодію, міжвідомчу координацію, обґрунтованість управлінських рішень та оперативність реагування з одночасним дотриманням прав і свобод людини.

Ключові слова: Smart City, Safe City, «Безпечне місто», публічне управління, цифровізація, міська безпека, цифрові технології, data-driven governance, управлінські рішення, безпекові ризики, національна безпека.

148-161
v.38 (2026)
https://smart-scm.org

Introduction. The rapid development of digital technologies, urbanisation processes and the increasing complexity of managing modern territorial communities are driving the transformation of traditional approaches to the organisation of urban space. Digitalisation is gradually encompassing not only the provision of administrative services and communication between public authorities and citizens but also transport, housing and communal services, energy, environmental protection, infrastructure management, public order, civil protection and emergency response. Consequently, cities increasingly function as complex information and communication systems whose management is based on the collection, integration, processing and use of large volumes of data.

The Smart City model has emerged as a conceptual reflection of these transformations. It involves the comprehensive application of digital, information and communication, and analytical technologies to improve the effectiveness of urban governance, the quality of public services, the efficient use of resources and the living conditions of the population. At the same time, the technological development of the urban environment creates new requirements for ensuring its security. The increasing number of digital systems, information flows, critical and municipal infrastructure facilities, transport networks and public spaces highlights the need to move from fragmented responses to individual threats towards integrated urban security management.

In this context, the Safe City concept is becoming particularly important. It is gradually evolving from a local video surveillance and public-order control system into an integrated information and analytical mechanism for ensuring the security of the urban environment. Modern Safe City systems may combine video surveillance networks, intelligent video analytics technologies, geographic information systems, Internet of Things (IoT) sensors and devices, automated traffic-control systems, situation centres, public warning systems, information resources of law enforcement and emergency services, as well as data analysis and risk-forecasting tools.

At the same time, the proliferation of digital security technologies is transforming not only the technological support available to public authorities but also the public governance model itself. Data obtained from different urban subsystems provide an informational basis for situational monitoring, risk identification, coordination among different actors, operational response and management decision-making. Thus, a gradual transition is taking place from a predominantly reactive urban security management model, focused on responding to events that have already occurred, towards a preventive and analytical model aimed at the early identification of potential threats and the mitigation of their consequences.

These processes are particularly relevant to Ukraine, where the digital transformation of territorial communities is taking place alongside the need to ensure the resilience of the urban environment under martial law, heightened security risks, threats to critical infrastructure and the need for the operational coordination of local self-government bodies, law enforcement agencies, emergency services and other actors within the security sector. Under such conditions, Safe City is becoming not merely a local-level technological project but also a component of the public governance system for ensuring the security and resilience of territorial communities.

Nevertheless, the Smart City and Safe City concepts are frequently examined separately in academic and practical discourse. Smart City is predominantly considered through the lens of the digitalisation of urban governance, infrastructure development, electronic services, mobility and sustainable

148-161
v.38 (2026)
https://smart-scm.org

development, whereas Safe City is often reduced to the use of video surveillance systems, public-order control and law enforcement activities. Such an approach does not fully reflect the contemporary nature of the relationship between a city's digital development and the provision of its security.

In view of the above, it is important to develop a public governance approach according to which Safe City should be regarded as a functional security component of the Smart City concept. This component ensures the integration of digital technologies, data, institutions and management processes to prevent threats, respond to them promptly and ensure the safe and resilient functioning of the urban environment.

Analysis of recent research and publications. The development of the Smart City concept and the integration of security components into contemporary urban governance have been addressed by both international and Ukrainian scholars. A. Caragliu, C. Del Bo, and P. Nijkamp examine Smart City through the interconnection between technological infrastructure, human and social capital, and sustainable urban development. V. Albino, U. Berardi, and R. M. Dangelico systematize the main approaches to defining Smart City, its dimensions, and development criteria. The use of urban data and digital technologies in public governance has been explored by S. Barns, J. R. Gil-Garcia, M. Gasco-Hernandez, T. A. Pardo, J. Kandt, M. Batty, E. Przeybilovicz, M. A. Cunha, and others.

A separate area of research focuses on the relationship between Smart City and Safe City. M. Lacinák and J. Ristvej emphasize the importance of strengthening the safety and security dimension of Smart City and examine the potential of modern technologies for ensuring urban safety. J. Ristvej, M. Lacinák, and R. Ondrejka further develop this approach by considering Smart City and Safe City as interconnected concepts and identifying the areas in which they overlap.

Among Ukrainian scholars, particular aspects of the Safe City system have been studied by I. S. Drok, O. V. Zinchenko, T. I. Kadlubovych, and M. O. Karpenko, with a focus on transport safety, emergency response, protection of state sovereignty, and the implementation of Safe City projects at the national level. At the same time, the public governance dimension of the Safe City system and its role in Smart City development require further research, particularly regarding the use of digital data, interagency cooperation, risk prevention, and support for managerial decision-making.

The formulation of the goals of the article. The purpose of the article is to provide a theoretical substantiation of the place and functional role of the "Safe City" concept within the Smart City framework, define its public administration content, and reveal the mechanisms for integrating digital security technologies into the management system of the modern urban environment.

Presentation of the main results. The formation of the Smart City concept is a natural consequence of the transformation of the modern urban environment under the influence of urbanization, the development of information and communication technologies, the digitalization of public governance, and the growing public demand for improved quality of urban services [16]. The increasing complexity of modern cities, population growth, growing pressure on transport, energy, and utility infrastructure, as well as the need to ensure environmental sustainability and security, have created a need to search for new approaches to organizing urban development governance.

The concept of Smart City became widely used in academic and governance discourse at the beginning of the 21st century. At the same time, its formation was associated with earlier processes of urban informatization and the development of the concepts of the digital city, information city, sustainable city, and e-governance [17].

One of the important approaches to understanding Smart City is presented by A. Caragliu, C. Del Bo, and P. Nijkamp, who associate the development of a smart city not only with the availability of physical and technological infrastructure but also with human and social capital [4]. The researchers emphasize the importance of information and communication technologies for enhancing the efficiency and competitiveness of modern cities. Thus, technology is viewed not as an end in itself in Smart City development, but as one of the instruments for the comprehensive development of the urban environment.

This approach is particularly important for examining Smart City from the perspective of public governance, as it makes it possible to move beyond its narrow interpretation as merely a set of digital technologies. The availability of sensors, video surveillance cameras, digital platforms, automated transport systems, or other technological solutions does not in itself constitute a smart city. What is decisive is how these technologies are integrated into the urban governance system and used to address socially significant issues, improve the efficiency of public authorities, and enhance the quality of life of the population.

V. Albino, U. Berardi, and R. M. Dangelico emphasize the multidimensional nature of the Smart City concept. Based on an analysis of academic literature and documents issued by international institutions, the researchers draw attention to the absence of a single universal definition of Smart City and to the diversity of components used to characterize the "smartness" of a city [1]. Therefore, Smart City should be regarded not as a separate technology or a local digital project, but as a comprehensive direction of urban development encompassing various spheres of city functioning.

In this context, digital technologies primarily perform an instrumental function. Their application enables the collection and processing of data on the condition of urban infrastructure, traffic flows, energy consumption, environmental conditions, the functioning of utility systems, the state of public spaces, and other urban processes. Based on such data, public authorities are able to assess situations more promptly, identify problematic areas, forecast the needs of the territorial community, and make appropriate governance decisions.

Thus, Smart City development is directly associated with the spread of data-driven governance. Under this approach, information obtained from various urban subsystems is transformed into a resource for public governance. First and foremost, the nature of governance activities changes: alongside traditional administrative mechanisms, digital monitoring, analytical data processing, forecasting, automated data exchange, and interagency information interaction are becoming increasingly important.

Importantly, the contemporary understanding of Smart City is gradually moving beyond a purely technological approach. One of the key criteria for smart city development is becoming the ability of digital solutions to deliver tangible improvements in the functioning of urban services and the quality of life of the population. This approach is reflected, in particular, in the international standard ISO 37122:2019 "Sustainable cities and communities – Indicators for smart cities", which associates Smart City development with the improvement of urban services and quality of life and establishes a system of indicators for assessing progress in this area [8].

Currently, academic discourse demonstrates a gradual transition from a technology-oriented understanding of Smart City towards a comprehensive governance approach. While at the initial stages considerable attention was focused on the development of information and communication infrastructure and the implementation of digital technologies, Smart City is increasingly associated with governance efficiency, sustainable

148-161
v.38 (2026)
https://smart-scm.org

development, human and social capital, the quality of public services, and the capacity of public authorities to use data for managerial decision-making [18].

Table 1 – Key Components of Smart City and Their Security Dimension

Smart City Component	Content of the Component	Public Governance Aspect	Security Dimension
Smart Governance	Digitalization of governance processes, e-services, open data, and digital interaction between public authorities and citizens	Improving governance responsiveness; using data for decision-making; interagency information exchange	Protection of information systems and data; cybersecurity; rapid exchange of threat-related information; coordination among security actors
Smart Economy	Innovation, digital economy, entrepreneurship, technological development, and urban competitiveness	Creating an enabling environment for innovation; digitalization of economic processes; support for technological development	Economic resilience of the city; protection of digital economic infrastructure; ensuring the continuity of businesses and essential services
Smart Mobility	Intelligent transport systems, traffic management, and digital mobility services	Monitoring traffic flows; traffic management; optimization of transport infrastructure	Road safety; detection of accidents and hazardous situations; emergency response; monitoring and management of traffic flows
Smart Environment	Environmental monitoring, energy efficiency, resource and waste management	Collection and analysis of environmental data; management of natural and energy resources; planning of environmental policy measures	Early detection of environmental and technological hazards; monitoring of risk indicators; prevention of emergencies
Smart People	Human and social capital, digital competencies, education, and civic participation	Citizen engagement in urban governance; development of digital literacy; e-participation and communication	Development of a safety culture; public information on threats; digital channels for reporting hazardous events; citizen participation in ensuring urban safety
Smart Living	Quality of life, healthcare, culture, housing, education, social infrastructure, and safety	Ensuring the accessibility and quality of urban services; creating a comfortable and resilient urban environment	Public and personal safety; protection of public spaces; video surveillance; emergency response; civil protection; crime prevention

Source: systematized by the author based on: [1, 6].

The analysis of the Smart City components (Table 1) demonstrates that security is not limited exclusively to the Smart Living component, within which it has traditionally been associated with the quality of life of the population. In fact, the security dimension is cross-cutting and is manifested across all components of a smart city: from cybersecurity and the protection of governance data within Smart Governance, to transport safety within Smart Mobility, economic resilience within Smart Economy, the prevention of environmental and technological threats within Smart Environment, and the development of a safety culture within Smart People. Thus, the role of security within the Smart City structure is gradually expanding, creating grounds for a separate examination of Safe City as a

security-oriented dimension of the digital development of the modern city.

For the purposes of this study, the Smart Living component is of particular importance, since the quality of urban life directly depends not only on the accessibility of services, housing conditions, mobility, or the state of the environment, but also on the level of personal and public safety. At the same time, the security component is not confined to a single area of Smart City. Transport system safety is associated with Smart Mobility, the protection of digital infrastructure with Smart Governance, the resilience of energy and utility systems with Smart Environment, while the ability of public authorities to identify threats in a timely manner and coordinate response measures directly depends on the quality of digital governance.

Therefore, security should be regarded as one of the cross-cutting prerequisites for the effective functioning of Smart City. The higher the level of digital integration of the urban environment, the greater the importance of timely threat detection, protection of the population and infrastructure, coordination of relevant services, emergency response, and the use of information to prevent potential risks.

In this context, within the broader development of Smart City, a distinct security-oriented direction is gradually emerging, associated with the use of digital technologies for monitoring urban spaces, preventing offences and emergencies, protecting infrastructure, and providing information and analytical support for the activities of public authorities. Its development creates the prerequisites for the formation and expansion of the Safe City concept.

Ensuring the safety of the population is one of the fundamental prerequisites for the sustainable functioning and development of the modern city. Urban population growth, the increasing complexity of transport and utility infrastructure, the concentration of numerous economic and social facilities, the growing intensity of information flows, and the emergence of new technological risks significantly broaden the range of threats faced by the urban environment. Under these conditions, security is gradually ceasing to be regarded exclusively as the responsibility of law enforcement agencies and is acquiring a comprehensive character, encompassing public, transport, technological, information, cyber, infrastructure, and other interconnected dimensions of security.

These processes have directly influenced the development of the Smart City concept. The digitalization of the urban environment has created new opportunities not only for optimizing traffic flows, managing energy resources, or providing public services, but also for monitoring the state of urban spaces, detecting hazardous situations, preventing offences, coordinating the activities of relevant services, and ensuring rapid response to threats. As a result, security issues have gradually become one of the important areas of smart city development.

The relationship between the technological development of Smart City and the provision of urban security is reflected in the works of international researchers. In particular, K. T. Chui, P. Vasant, and R. W. Liu, examining urban monitoring and surveillance systems, draw attention to the potential of information and communication infrastructure, sensor devices, cameras, and big data analytics technologies for protecting people and property. At the same time, the use of such technologies is accompanied by a number of challenges related to data quality, privacy, information security, and relevant public policy [5]. Thus, the digitalization of urban security creates not only new governance instruments but also new objects and risks of public regulation.

The gradual emergence of a distinct security-oriented dimension of urban digital development contributed to the spread of the Safe City concept. At the initial stages, its practical implementation was largely associated with maintaining public order,

preventing crime, and using video surveillance systems. Surveillance cameras made it possible to continuously monitor specific areas of urban space, record events, and use the information obtained in law enforcement activities. However, the development of information and communication technologies has gradually expanded the capabilities of such systems.

An important direction of this transformation has been the use of data not only to record offences that have already occurred but also to prevent them. Research in the field of urban security demonstrates the potential for combining crime-related information with data on the characteristics of the urban environment, land use, population movements, and other factors. On this basis, digital systems can be used as decision-support tools in the formulation and implementation of urban security policies.

In the academic literature, Safe City is considered one of the directions for developing a secure urban environment through the application of modern technologies. In particular, a systematic review devoted to the development of a conceptual Safe City model associates a safe city with the use of technologies by public authorities, communities, and other stakeholders to reduce crime risks and create an environment in which the population can feel safe. At the same time, security is identified as one of the essential aspects of Smart City development.

At the same time, the relationship between the concepts of Smart City and Safe City is not interpreted uniformly in contemporary academic literature. Some approaches consider Safe City as a separate functional component of Smart City, primarily focused on ensuring public safety. Other studies emphasize the much broader scope of urban security, which does not allow Safe City to be fully subordinated to the Smart City concept.

The position of J. Ristvej, M. Lacinák, and R. Ondrejka is particularly illustrative in this context. The researchers note that at the early stages of their research they considered Safe City as one of the systems within Smart City; however, they subsequently concluded that such an approach did not cover the entire spectrum of urban security issues [14]. As a result, they proposed considering Smart City and Safe City as independent but partially interconnected concepts. This position demonstrates the complexity of establishing a clear hierarchy between a "smart" and a "safe" city and indicates the gradual expansion of the scope of the Safe City concept.

From a public governance perspective, this transformation in the functional content of Safe City is of particular importance. While traditional urban security systems were primarily focused on surveillance, event recording, and subsequent response by relevant services, modern digital technologies make it possible to establish a significantly more complex system of information support for governance. Video surveillance is complemented by intelligent video analytics, geographic information systems, sensors and Internet of Things devices, automated recognition of specific objects and events, big data analytics, digital public warning systems, and interagency information exchange tools.

Accordingly, the role of data in the urban security system is also changing. Data can be used not only as a source of information about events that have already occurred, but also to identify high-risk areas, detect patterns, forecast possible developments, and select the most appropriate governance measures. This creates the prerequisites for a transition from a predominantly reactive approach to urban security towards more preventive and risk-oriented governance.

Along with the technological expansion of Safe City, the range of actors involved in ensuring urban security is also broadening. While law enforcement agencies and emergency services traditionally played the primary role in this field, the functioning of a

modern digitalized city requires interaction among local self-government bodies, state authorities, police, rescue and medical services, urban infrastructure operators, transport enterprises, municipal services, and other actors. Consequently, the issue of urban security is acquiring a distinct interagency and cross-sectoral character.

At the same time, the technological advancement of security should not be equated with the unlimited expansion of surveillance systems. Contemporary research increasingly focuses on risks related to privacy, personal data protection, cybersecurity, algorithmic data analysis, and the possibility of excessive surveillance of urban spaces. Therefore, the effectiveness of Safe City is determined not only by the number of installed cameras, sensors, or other digital tools, but also by the existence of appropriate organizational, legal, and governance mechanisms regulating their use.

Thus, the development of Safe City is characterized by a gradual transition from local surveillance and monitoring technologies to the comprehensive use of digital data in urban security processes. This transformation simultaneously broadens the scope of public governance: alongside maintaining public order, it increasingly encompasses risk prevention, infrastructure protection, information exchange, coordination among relevant services, data protection, and ensuring the resilient functioning of the urban environment.

In this regard, the study of Safe City in the context of Smart City requires a shift from a purely technological interpretation towards an analysis of its governance dimension. Of particular importance is the question of how information obtained through the city's digital infrastructure is integrated into the activities of public authorities, transformed into governance decisions, and used to prevent and minimize security risks.

The development of Safe City systems highlights the need to consider them not merely as a set of technical tools for surveillance, event recording, and data analysis, but as an element of the contemporary system of public governance of urban security. Technological infrastructure alone does not ensure the security of the urban environment [2]. Its practical value is determined by the capacity of public authorities to use the data obtained to identify problems, assess risks, coordinate the activities of relevant services, make governance decisions, and organize timely responses.

This approach corresponds with contemporary research on smart urban governance. E. Przeybilovicz and M. A. Cunha consider the digital transformation of the urban environment as a factor contributing to the emergence of new dynamic models of urban governance, within which the nature of interaction among public authorities, information and communication technologies, and citizens directly influences the mechanisms through which governance functions are performed [12]. In turn, S. Ranchordás and A. Klop associate the development of data-driven governance in Smart City with the use of big data, artificial intelligence, the Internet of Things, and predictive analytics to improve the efficiency of public services and managerial decision-making. The combination of these components makes it possible to understand Safe City more broadly than traditional video surveillance systems or automated monitoring of individual areas of urban space [13].

In the traditional model of urban security, information about an offence, accident, emergency, or other hazardous event is generally received by the relevant authority or service only after the event has occurred. Subsequent governance actions are aimed at containing the event, mitigating its consequences, establishing the circumstances, and restoring the normal functioning of the affected area or facility. Such an approach is predominantly reactive,

as the governance system responds to a threat that has already materialized.

The digitalization of the urban environment creates the prerequisites for a gradual transformation of this model. The continuous flow of information from various sources enables public authorities and relevant services to obtain data on the condition of individual facilities and processes in near real time. As a result, information can be used not only to record an event but also to detect deviations, identify potentially hazardous situations, assess risks, and take appropriate measures in advance.

In this context, one of the key elements of the public governance dimension of Safe City is the information and analytical function. Large volumes of information obtained from various sources acquire governance value only when they are systematized, compared, and analyzed [3]. Therefore, what becomes fundamentally important is not the accumulation of data itself, but its transformation into information suitable for use in managerial decision-making.

At the same time, the effective use of data requires their integration. Information on the condition of public spaces, transport infrastructure, road traffic, municipal facilities, or emergencies may be generated by different authorities, services, and information systems. The isolated use of such information limits the possibilities for a comprehensive assessment of the situation. In contrast, effective information exchange makes it possible to develop a more comprehensive understanding of the state of the urban environment and the nature of existing risks.

This leads to another important function of the Safe City system – the coordination function. Ensuring the security of a modern city extends beyond the competence of any single public authority. Responding to different types of threats may simultaneously require the involvement of local self-government bodies, law enforcement agencies, civil protection authorities and units, emergency medical services, municipal enterprises, transport services, and other actors [7]. Under such conditions, governance effectiveness depends not only on the powers of each actor but also on the speed of information exchange and the coordination of joint actions.

The monitoring function also plays an important role in the operation of Safe City and involves systematic observation of the urban environment and individual processes relevant to security. Unlike the episodic receipt of information, digital monitoring makes it possible to generate continuous information flows, track changes in relevant indicators, and promptly identify developments requiring governance intervention.

The preventive function is directly related to the monitoring and information and analytical functions. The use of accumulated data and the results of their analysis creates opportunities to identify recurring patterns, determine high-risk areas or facilities, and plan measures aimed at preventing or reducing the likelihood of adverse events. Thus, governance activities gradually shift from responding to consequences towards preventing threats.

The managerial decision-support function is of particular importance. Given the large number of simultaneous information flows, an official or public authority may not always be able to process the entire volume of available information promptly. Digital analytical tools make it possible to structure data, identify priority events, reveal interrelationships, and provide an information basis for selecting appropriate governance decisions [9]. At the same time, technology should not replace the competent public authority: it performs a supporting role, while responsibility for decision-making remains with the relevant authority or official.

Today, digital technologies are changing the nature of information support for public governance. In the traditional governance

model, information was largely received through citizens' appeals, reports from relevant services, statistical reporting, and other documented sources. In the digitalized urban environment, these sources are supplemented by automated data flows that can be generated continuously and characterize the current state of particular processes. As a result, the time between the emergence of a hazardous situation, its detection, and the initiation of a governance response is reduced.

The public governance dimension of the Safe City system is also manifested through its organizational function. The integration of digital technologies into security processes requires the identification of responsible actors, the delineation of their competencies, the establishment of procedures for access to information resources, information exchange, and response algorithms. Therefore, the technological integration of information resources should be accompanied by the corresponding organizational integration of the activities of public governance actors.

Equally important is the control function, which is associated with the possibility of evaluating the outcomes of governance decisions and measures implemented. The accumulation of data makes it possible to compare the state of the urban environment before and after the implementation of relevant decisions, assess the response time of services, identify recurring problems, and adjust governance measures accordingly [11]. This creates a feedback mechanism linking information collection, decision-making, implementation, and evaluation of results.

At the same time, the digitalization of urban security governance gives rise to a number of new governance and legal challenges. The concentration of large volumes of information, including data on individuals' movements and behavior, creates risks of unlawful interference with privacy, unauthorized access to information, data leakage, or the use of data for purposes other than those for which they were originally collected [15]. The use of algorithmic analytical systems further raises issues concerning the transparency of technological solutions, non-discrimination, the limits of automated data processing, and accountability for decisions made with the use of such technologies.

Therefore, the public governance effectiveness of Safe City cannot be assessed solely by the number of installed cameras and sensors, established situation centers, or the volume of accumulated data. It should be determined by the system's capacity to ensure timely threat detection, effective information exchange, coordination among relevant actors, well-grounded governance decisions, rapid response, and respect for human rights and freedoms [10].

Thus, from a public governance perspective, the Safe City system is characterized by a combination of monitoring, information and analytical, coordination, organizational, preventive, and control functions, as well as the managerial decision-support function. Their implementation enables the transformation of digital data on the state of the urban environment into a public governance resource and creates the prerequisites for improving the responsiveness and soundness of public authorities' activities in the field of urban security.

Accordingly, the fundamental difference between the contemporary Safe City system and traditional technical surveillance systems lies not so much in the number or technological complexity of the tools employed, but rather in the integration of the data obtained through these tools into the full public governance cycle – from problem identification and risk assessment to decision-making, organization of response measures, and evaluation of their effectiveness. It is this aspect that makes it possible to consider the development of Safe City systems as part of the broader processes of the digital transformation of public governance of the urban environment.

148-161
v.38 (2026)
https://smart-scm.org

Conclusions.

In the context of the digital transformation of the urban environment, security is becoming one of the key dimensions of Smart City development. At the same time, its role cannot be limited exclusively to the Smart Living domain, since security-related objectives are, to varying degrees, integrated into all major components of a smart city. The protection of information resources, transport safety, urban infrastructure resilience, prevention of technological and environmental threats, maintenance of public order, and development of a public safety culture constitute an interconnected set of tasks that requires the coordinated use of digital and governance instruments.

The development of the Safe City concept demonstrates a gradual transformation of the approach to ensuring urban security. A Safe City can no longer be identified solely with video surveillance systems, technical recording of events, or monitoring of public spaces. Its contemporary content is primarily determined by the capacity to integrate various sources of information and use the data obtained for timely threat detection, risk assessment, forecasting of possible developments, and the organization of coordinated response measures. Accordingly, the technological development of Safe City is gradually evolving into a broader transformation of urban security governance.

A key outcome of this transformation is the changing role of information in the governance process. Data no longer serve exclusively as a means of recording events but are increasingly becoming a resource for public governance. Their systematic collection, integration, and analytical processing make it possible to reduce the time between the emergence of a threat, its detection, and the initiation of a governance response. This creates the conditions for a gradual transition from a predominantly reactive security model to preventive and risk-oriented governance of the urban environment.

The governance effectiveness of the Safe City system therefore depends not on the number of cameras, sensors, information platforms, or other technical tools, but on the extent to which they are integrated into the activities of public authorities and relevant services. Of decisive importance is the system's capacity to ensure continuous monitoring, analytical processing of information, effective interagency data exchange, coordination among relevant actors, support for managerial decision-making, and control over the results of implemented decisions. Therefore, technological integration should be accompanied by organizational and governance integration.

At the same time, the expansion of the technological capabilities of Safe City creates a new set of risks for public governance. The accumulation of large volumes of data, the increasing use of intelligent video analytics, and algorithmic data processing raise important issues related to personal data protection, privacy, cybersecurity, transparency in the use of digital technologies, and accountability for decisions made with their assistance. Therefore, the further development of Safe City should be based on a combination of technological efficiency, appropriate legal and organizational frameworks, and respect for human rights and freedoms.

Thus, the prospective development of Safe City systems should focus not on simply expanding digital infrastructure, but on establishing an integrated mechanism for urban security governance in which technologies provide the information basis for monitoring, threat prevention, coordination, and decision-making. It is precisely the capacity to transform digital data into timely and well-grounded governance actions that will determine the actual effectiveness of Safe City as a security-

oriented dimension of contemporary Smart City development.

References

1. Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. Journal of Urban Technology, 22(1), 3–21. DOI: 10.1080/10630732.2014.942092.

2. Barns, S. (2018). Smart cities and urban data platforms: Designing interfaces for smart governance. City, Culture and Society, 12, 5–12. DOI: 10.1016/j.ccs.2017.09.006.

3. Bui, M. (2025). Toward a community-driven approach to urban data-driven governance. International Communication Gazette, 87(1). DOI: 10.1177/17480485241261572.

4. Caragliu, A., Del Bo, C., & Nijkamp, P. (2011). Smart cities in Europe. Journal of Urban Technology, 18(2), 65–82. DOI: 10.1080/10630732.2011.601117.

5. Chui, K. T., Vasant, P., & Liu, R. W. (2019). Smart city is a safe city: Information and communication technology-enhanced urban space monitoring and surveillance systems: The promise and limitations. In Smart Cities: Issues and Challenges (pp. 111–124). Elsevier.

6. Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanović, N., & Meijers, E. (2007). Smart Cities: Ranking of European Medium-Sized Cities. Vienna: Centre of Regional Science, Vienna University of Technology.

7. Gil-Garcia, J. R., Gasco-Hernandez, M., & Pardo, T. A. (2022). Governance rules for managing smart city information. Urban Governance, 2(1), 221–231. DOI: 10.1016/j.ugj.2022.05.003.

8. International Organization for Standardization. (2019). ISO 37122:2019. Sustainable cities and communities Indicators for smart cities. Geneva: ISO. 95 p. https://www.iso.org/standard/69050.html.

9. Kandt, J., & Batty, M. (2021). Smart cities, big data and urban policy: Towards urban analytics for the long run. Cities, 109, Article 102992. DOI: 10.1016/j.cities.2020.102992.

10. Lacinák, M., & Ristvej, J. (2017). Smart city, safety and security. Procedia Engineering, 192, 522–527. DOI: 10.1016/j.proeng.2017.06.090.

11. OECD. (2023). Smart City Data Governance: Challenges and the Way Forward. OECD Urban Studies. Paris: OECD Publishing. 185 p. DOI: 10.1787/e57ce301-en. https://doi.org/10.1787/e57ce301-en.

12. Przeybilovicz, E., & Cunha, M. A. (2024). Governing in the digital age: The emergence of dynamic smart urban governance modes. Government Information Quarterly, 41(1), Article 101907. DOI: 10.1016/j.giq.2023.101907.

13. Ranchordás, S., & Klop, A. (2024). Data-driven regulation and governance in smart cities. In V. Mak et al. (Eds.), Research Handbook in Data Science and Law (2nd ed., pp. 251–276). Edward Elgar Publishing. DOI: 10.4337/9781035316458.00019.

14. Ristvej, J., Lacinák, M., & Ondrejka, R. (2020). On smart city and safe city concepts. Mobile Networks and Applications, 25, 836–845. DOI: 10.1007/s11036-020-01524-4.

15. Drok, I. S. (2025). The "Safe City" system as a tool for monitoring compliance with transport legislation. Analytical and Comparative Jurisprudence, 2, 244–249. [in Ukrainian].

16. Zinchenko, O. V. (2024). "Safe City" as a factor of rapid response to emergencies in the context of the development of a digital society. Collection of Scientific Works of the State Research Institute of the Ministry of Internal Affairs of Ukraine, 4(12). [in Ukrainian].

17. Kadlubovych, T. I. (2026). The "Safe City" concept as a tool for protecting state sovereignty. Forum Prava, 87(3), 190–198. DOI: 10.32631/fp.2026.3.18. [in Ukrainian].

18. Karpenko, M. O. (2023). Substantiation of the implementation of "Safe City" projects at the state level in Ukraine. Investments: Practice and Experience, 11, 45–51. [in Ukrainian].

The electronic scientifically and practical journal
"INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT",
ISSN 2708-3195

162-168
v.38 (2026)
https://smart-scm.org

DOI: https://doi.org/10.46783/smart-scm/2026-38-11

UDC 005.932:355.01
JEL Classification: C61, D81, F15, F51, R41

Received: 2026-07-26
Accepted: 2026-08-26
Published: 2026-08-30

Grabovskiy D.Y. Postgraduate Student National University "Kyiv Aviation Institute" (Ukraine)

ORCID – 0009-0005-8861-6006
Researcher ID
Scopus author id: –
E-Mail: dimka_92@ukr.net

Bugayko D.O. Doctor of Science (Economics), Professor, Academician of the Academy of Economic Sciences of Ukraine, Corresponding Member of the Transport Academy of Ukraine, Instructor of ICAO Institute, Leading Researcher, Professor (Full) of the Logistics Department National University "Kyiv Aviation Institute" (Ukraine)

ORCID – 0000-0002-3240-2501
Researcher ID ABF-5564-2021
Scopus author id: – 57216582348
E-Mail: bugaiko@kai.edu.ua

OPTIMIZATION OF UKRAINE–EU LOGISTICS ROUTES UNDER WARTIME RISKS

Danylo Grabovsky, Dmytro Bugayko. "Optimization of Ukraine–EU Logistics Routes Under Wartime Risks". *The full-scale war has fundamentally transformed freight flows between Ukraine and the European Union, restricted the use of traditional maritime routes, and substantially increased pressure on road, rail, and inland waterway corridors. Under these conditions, logistics route selection cannot be based solely on minimizing distance or transportation costs. It must also account for delivery time, infrastructure capacity, border-crossing delays, technical interoperability, disruption probability, and security risks. The purpose of this study is to substantiate approaches to optimizing logistics routes between Ukraine and the EU under wartime risks and to identify the factors determining the choice of an efficient, reliable, and resilient route. The methodological framework combines a systems approach, comparative analysis of the principal transport corridors, synthesis of multimodal transport practices, and a multi-criteria approach to logistics decision-making. The study proposes a conceptual objective function incorporating transportation cost, delivery time, risk level, and delay probability, with the weight assigned to each criterion depending on the type, urgency, and value of the cargo. The Polish, Slovak, Hungarian, Romanian, and Danube corridors are examined. The findings indicate that logistics resilience cannot be ensured by a single universally optimal route; instead, it requires a portfolio of interchangeable primary, backup, and supplementary corridors. The principal constraints on route optimization include insufficient capacity at individual border crossings, border queues, incompatibility between the Ukrainian and European railway gauges, limited terminal capacity, and the risk of transport infrastructure disruption or damage. The study substantiates the need to expand multimodal transportation,*

162-168
v.38 (2026)
https://smart-scm.org

develop logistics hubs in western Ukraine, extend European-standard railway infrastructure, and strengthen the Danube transport corridor. Digital platforms, GPS and geographic information systems, transport management systems, and artificial intelligence tools are shown to provide a foundation for forecasting delays and dynamically adjusting routes in response to changing operational conditions. The practical significance of the results lies in their potential application by logistics companies and public authorities when designing resilient transport networks, planning alternative corridors, and improving the continuity of Ukraine's foreign trade. The proposed approach links operational efficiency with supply chain resilience and treats route redundancy as an essential component of logistics optimization under wartime uncertainty.

***Keywords**:* route optimization, transport logistics, wartime risks, transport corridors, multimodal transportation, supply chain resilience, logistics digitalization

Данило Грабовський, Дмитро Бугайко. «Оптимізація логістичних маршрутів між Україною та ЄС в умовах воєнних ризиків». *Повномасштабна війна докорінно змінила структуру вантажних потоків між Україною та Європейським Союзом, обмежила використання традиційних морських маршрутів і суттєво підвищила навантаження на автомобільні, залізничні та річкові транспортні коридори. За таких умов вибір логістичного маршруту не може ґрунтуватися виключно на мінімізації відстані або вартості перевезення, оскільки необхідно одночасно враховувати час доставки, пропускну здатність інфраструктури, тривалість проходження кордону, технічну сумісність транспортних систем, імовірність затримок і безпекові ризики. Метою дослідження є обґрунтування підходів до оптимізації логістичних маршрутів між Україною та ЄС в умовах воєнних ризиків і визначення чинників, які впливають на вибір ефективного, надійного та стійкого маршруту. Методологічну основу дослідження становлять системний підхід, порівняльний аналіз основних транспортних коридорів, узагальнення практики мультимодальних перевезень і багатокритеріальний підхід до прийняття логістичних рішень. Запропоновано концептуальну цільову функцію вибору маршруту, яка враховує транспортні витрати, тривалість доставки, рівень ризику та ймовірність затримки, а вагомість кожного критерію визначається видом, терміновістю і цінністю вантажу. Проаналізовано польський, словацький, угорський, румунський і Дунайський коридори та встановлено, що стійкість логістичної системи забезпечується не одним універсально оптимальним маршрутом, а портфелем взаємозамінних основних, резервних і додаткових напрямів. Визначено ключові обмеження маршрутної оптимізації: недостатню пропускну здатність окремих пунктів пропуску, черги на кордоні, відмінність ширини залізничної колії України та ЄС, обмежені можливості терміналів і ризики пошкодження транспортної інфраструктури. Обґрунтовано доцільність розвитку мультимодальних перевезень, логістичних вузлів у західних регіонах України, інфраструктури європейської колії та Дунайського транспортного коридору. Показано, що цифрові платформи, системи GPS і GIS, системи управління транспортом та інструменти штучного інтелекту створюють основу для прогнозування затримок і динамічної зміни маршруту відповідно до поточної ситуації. Практичне значення результатів полягає у можливості їх використання логістичними компаніями й органами державного управління для формування стійких транспортних мереж, планування альтернативних маршрутів і підвищення безперервності зовнішньої торгівлі України.*

Ключові слова: оптимізація маршрутів, транспортна логістика, воєнні ризики, транспортні коридори, мультимодальні перевезення, стійкість ланцюгів постачання, цифровізація логістики.

Introduction. Cooperation between Ukraine and the EU in the transport sector is governed by the Association Agreement between Ukraine and the European Union,

162-168
v.38 (2026)
https://smart-scm.org

the European Atomic Energy Community, and their member states. The aim is to promote the development of stable transport systems, ensure efficient and safe transportation, as well as intermodality and operational compatibility of transport systems. (Mission Ukraine to European Union (2026)).

In today's environment, logistics is one of the key factors supporting stable international trade and economic development. For Ukraine, the transport and logistics system is particularly important: the country remains an important link in European and international supply chains, while its geographical position creates opportunities for active transport connections with the European Union and other regions of the world (Ministry of Infrastructure of Ukraine (2025), European Commission (2025)). At the same time, the full-scale war has fundamentally changed the conditions in which the transport system operates, forcing both businesses and the state to seek new logistics solutions.

Before 2022, a significant share of Ukrainian exports and imports moved through Black Sea ports. Maritime transport made it possible to ship large volumes of grain, metallurgical products, raw materials, and other cargo at relatively low cost. As a result of hostilities, infrastructure damage, and restrictions on navigation, a substantial share of freight flows had to be redirected to land and river routes.

With maritime transport constrained, part of the load shifted to road and rail crossings with the EU and to the Danube corridor. As a result, Poland, Slovakia, Hungary, and Romania became even more important as transit countries. At the same time, the European Union launched the Solidarity Lanes, a network of alternative corridors that helped maintain the flow of Ukrainian exports and imports.

Under these conditions, the shortest route is far from always being the best one. Transport planning must simultaneously take into account cost, transit time, infrastructure capacity, border conditions, technical limitations, and wartime risks. Route optimization between Ukraine and the EU is therefore not merely an operational task for logistics companies, but an important component of the country's economic resilience.

The purpose of this study is to identify the main approaches to optimizing logistics routes between Ukraine and the European Union under wartime risks and to analyze the factors that influence the choice of an efficient, reliable, and resilient route.

1. Transformation of Ukraine's Logistics System during the War. The full-scale war has placed Ukraine's transport system under severe pressure. Changes in port operations, damage to rail and road infrastructure, risks to warehouse facilities, and general instability have forced established supply chains to be reorganized rapidly.

One of the most visible changes has been the reduced ability to use traditional maritime routes. As a result, Ukraine's land border with EU countries has gained strategic importance, with Poland, Slovakia, Hungary, and Romania becoming key directions for a significant share of Ukrainian exports and imports.

The EU Solidarity Lanes have played an important role in this restructuring. They provided additional road, rail, river, and maritime routes through which Ukraine can export agricultural products, metals, and industrial goods while importing fuel, equipment, humanitarian cargo, and other essential products.

At the same time, shifting a substantial share of freight traffic to land routes created new problems. One of the most important is the limited capacity of certain border crossings. Even when roads and railways within Ukraine operate without major restrictions, cargo may still lose considerable time at the border itself.

For this reason, the efficiency of an international route cannot be assessed solely by the distance between origin and

destination. Actual border-crossing time, road congestion, terminal availability, transshipment options, and the overall condition of infrastructure all have a direct impact on delivery performance.

Another persistent challenge is the difference between Ukrainian and European railway gauges. Ukraine predominantly uses the 1,520 mm gauge, while the standard across most EU countries is 1,435 mm. At the border, this often requires additional operations such as cargo transshipment, changing rolling stock, or applying specialized technical solutions.

Expanding European-standard gauge infrastructure within Ukraine could significantly simplify integration with the EU transport system. In the long term, it could reduce cargo handling time at the border and make rail transport faster and more predictable.

2. Main Ukraine–EU Logistics Corridors. Several key corridors currently shape international freight transport between Ukraine and the European Union.

The Polish corridor remains one of the most important because of Poland's developed transport infrastructure and convenient access to Germany, the Czech Republic, the Baltic states, and other EU markets. It is used extensively by both road and rail transport. Its main advantage is the large number of transport connections and a dense road and railway network. However, heavy pressure on individual border crossings can lead to queues and significantly longer delivery times.

The Slovak corridor through Zakarpattia provides access to Central European markets, including the Czech Republic, Austria, and Germany. It is particularly promising for rail logistics. The development of European-standard gauge sections is gradually reducing the impact of technical incompatibility between the railway systems.

Hungary can serve as an alternative corridor when routes through Poland or Slovakia are congested, temporarily restricted, or economically inefficient. The availability of several interchangeable directions is precisely what makes the logistics system more resilient.

The Romanian corridor is particularly important because it provides access to the Port of Constanța. A multimodal model can be effective here: cargo is transported to Romania by road or rail and then continues by sea.

The Danube transport corridor also occupies a distinct position. River transport can handle significant cargo volumes and connect Ukrainian logistics with European ports. This is especially important for grain and other bulk commodities.

For resilient logistics, Ukraine needs not one supposedly ideal route, but several fully functional corridors. If one direction becomes congested, blocked, or otherwise disrupted, part of the freight flow can then be redirected quickly to another.

3. Factors in Logistics Route Optimization. Under stable conditions, routes are usually compared primarily in terms of price and transit time. During wartime, that is not enough. Reliability must also be included in the calculation: a cheaper and shorter route may prove to be the worse option if the risk of blockage or prolonged delays is high.

Transportation cost remains a basic indicator. It includes not only fuel expenses, but also driver wages, the use of vehicles and infrastructure, loading and unloading operations, and related charges.

Delivery time is equally important. For a business, a delayed shipment may result in production downtime, additional storage costs, missed contractual deadlines, and direct financial losses.

Border waiting time should be calculated separately. On some routes, waiting at a border crossing may be comparable to the actual driving time or even exceed it. Distance alone therefore says little about real delivery speed; data on the actual or average

162-168
v.38 (2026)
https://smart-scm.org

processing time at a specific crossing are also required.

Wartime risk should also be treated as a separate variable. This includes possible infrastructure damage, temporary road closures, power disruptions, changes in the operating regime of individual facilities, and other events that are difficult to predict in advance.

Capacity is another constraint. An economically attractive corridor cannot become a full-scale solution for large shipments if its roads, railways, terminals, or border infrastructure are physically unable to handle the required freight volume.

Finally, the availability of a viable alternative matters. If a carrier can switch to another corridor without critical losses, disruption on one route is less likely to paralyze the entire supply chain.

Accordingly, an "optimal route" under wartime conditions represents a compromise among several parameters: cost, time, risk, reliability, and capacity.

In simplified form, the objective function can be expressed as follows:

$$F = w_1C + w_2T + w_3R + w_4D \quad (1)$$

where C is transportation cost, T is delivery time, R is the level of risk, D is the probability of delay, and w_1, w_2, w_3, w_4 are the weighting coefficients assigned to the respective criteria.

The weight of each criterion depends on the type of cargo. For humanitarian aid or urgently needed equipment, time may be decisive. For grain and other bulk commodities, transportation cost may carry more weight. For high-value equipment, safety and reliability become considerably more important.

4. The Role of Multimodal Transportation. One of the most promising directions for the development of Ukrainian logistics is multimodal transportation—the use of several modes of transport within a single supply chain.

For example, cargo may first be transported by truck to a rail terminal, then by rail to a logistics center in the EU, and finally by road for the last leg of the journey. Another option is rail delivery to a Romanian port followed by maritime transport.

The main advantage of this approach is flexibility. The most appropriate mode can be selected for each section of the route, dependence on a single corridor can be reduced, and rail and river transport can be used more efficiently for large cargo volumes.

However, a multimodal model requires appropriate infrastructure: logistics centers, warehouses, transshipment terminals, and digital systems for managing freight flows (Jeej W (2023)).

Coordination between different modes of transport is equally important. If a train arrives at a terminal but trucks for the next stage are not yet available, part of the benefit of a fast route is lost. Optimization should therefore cover the entire chain as a single system rather than treating each section in isolation.

5. Optimization through Digital Technologies. Modern logistics increasingly depends on data. GPS, geographic information systems, transport management systems, and artificial intelligence technologies make it possible to base decisions not only on a pre-defined plan, but also on current conditions Grabovskiy D.Y., Bugayko D.O. (2025)).

A digital platform can simultaneously take into account vehicle location, road conditions, congestion at border crossings, terminal availability, and changes in transportation costs. This creates the basis for dynamic routing.

With this approach, a route does not remain fixed from departure to arrival. If, for example, queues suddenly increase at the planned border crossing, the system can recommend another crossing. The same

principle applies when conditions change on road or rail sections.

Artificial intelligence can add a forecasting layer to this system. By analyzing accumulated data, algorithms can estimate the probability of delays, forecast arrival times, and suggest alternatives in advance (Grabovskiy D.Y., Bugayko D.O. (2025)).

In practice, digitalization changes the very principle of planning: instead of relying on a single route defined at the start, the carrier can adjust it while the shipment is already in transit. During wartime, when conditions on a particular section can change within hours, this flexibility is especially important.

6. Building a Resilient Logistics System. For Ukraine, the task is not simply to restore the pre-war transport system. More importantly, it is necessary to build a model capable of continuing to operate under serious disruption and adapting quickly to new constraints.

One of the basic principles of such a system is route redundancy. For a particular freight flow, for example, the route through Poland may serve as the primary option, Slovakia as the backup, and Hungary or Romania as additional alternatives.

Developing logistics hubs in western Ukraine is another important step. Such hubs can provide storage, sorting, transshipment, and redistribution of goods between different transport modes and routes (Lebedeva, L. , Shkuropadska, D. (2024)).

At the same time, border capacity needs to be increased by modernizing road and rail crossings, expanding terminals, and digitalizing customs procedures. The fewer manual and poorly synchronized operations there are, the more predictable the entire route becomes.

Further integration of Ukraine's railway system with the European network is also strategically important. Expanding 1,435 mm standard-gauge infrastructure could reduce the number of operations required at the border and accelerate freight movement.

It is equally important to continue developing river and port infrastructure in the Danube region. This gives Ukraine additional export options and reduces dependence on individual transport corridors.

Conclusions.

Optimizing Ukraine–EU logistics routes under wartime risks is a complex multi-criteria task. The full-scale war has changed the established structure of Ukraine's foreign trade and significantly increased the importance of land, rail, and river routes.

Today, choosing a route requires more than comparing its cost and duration. Reliability, the risk of delays, infrastructure capacity, security threats, and the ability to switch quickly to an alternative corridor must also be assessed.

Routes through Poland, Slovakia, Hungary, and Romania, together with the Danube corridor, play a key role in connecting Ukraine with the EU market. Developing these directions in parallel makes it possible to diversify freight flows and avoid critical dependence on a single route.

Multimodal transportation remains a promising area of development, combining road, rail, river, and maritime transport within a single supply chain. Digitalization is equally important: GPS, geographic information systems, artificial intelligence, and dynamic routing help operators respond more quickly to changing conditions and make better-informed decisions.

In the long term, the logistics system between Ukraine and the EU should be built around four principles: diversification, multimodality, digitalization, and redundancy. Combining several alternative corridors with modern infrastructure and responsive management enables businesses to adapt to wartime, economic, and infrastructure changes.

Optimization of Ukraine–EU routes therefore goes far beyond simply reducing transportation costs. The quality of these decisions affects the continuity of foreign trade, business operations, the resilience of

international supply chains, and Ukraine's further integration into the European Union's transport network.

References

1. Mission Ukraine to European Union (2026). https://ukraine-eu.mfa.gov.ua/en/2633-relations/galuzeve-spivrobitnictvo/transport.

2. Ministry of Infrastructure of Ukraine (2025). Eastern Partnership and TEN-T transport integration: History and current status. 2025. URL: https://mtu.gov.ua/content/shidne-partnerstvo.html..

3. European Union. Ukraine – Enlargement and Eastern Neighbourhood. European Commission (2025). URL: https://enlargement.ec.europa.eu/countries/ukraine_en.

4. Jeej W (2023). Organizational and methodological approaches to transport infrastructure restoration in Ukraine // Journal of Engineering and Economic Education. 2023. № 1716. URL: https://jeej.wunu.edu.ua/index.php/enjee/article/view/1716.

5. Grabovskiy D.Y., Bugayko D.O. (2025). Automation as the Future of Logistics. Intellectualization of Logistics and Supply Chain Management: Electronic scientific and practical journal, vol. 29, p. 50-54. DOI: https://doi.org/10.46783/smart-scm/2025-29-7 (In Ukrainian).

6. Grabovskiy D.Y., Bugayko D.O. (2025). The role of automation in ensuring sustainable development of the logistics industry. Polit. Modern problems of science. economics and business administration in aviation: abstracts of the reports of the XXV International Scientific and Practical Conference of Higher Education Applicants and Young Scientists, K., KAI. 2025. p. 71-73.

7. Lebedeva, L. Shkuropadska, D. (2024). Resilience of transport logistics in EU and Ukraine. Ius Modernum. 135, 4 (Sep. 2024), 108–127. DOI:https://doi.org/10.31617/3.2024(135)07.

Scientific publication

INTELLECTUALIZATION OF LOGISTICS AND SUPPLY CHAIN MANAGEMENT

The electronic scientifically and practical journal

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 June 11, 2026 No. 928 (Appendix 13 item 205).

Cluster: Economic Transformation, Business and Administration

Specialties: C1 – Economics and International Economic Relations (by specializations)
D3 – Management
D5 – Marketing

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2026-38

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

№ 38 (2026)
August 2026

ISSN 2708-3195
DOI: https://doi.org/10.46783/smart-scm/2026-38