Keywords: digitalization, international transportation, security, logistics, cybersecurity, digital technologies, digital infrastructure, human factor

Inna VISHTAK[1]*, Leonid MAIDANEVYCH[2], Volodymyr KUZHEL[3], Victoriia KHYMYCH[4]

AN INTEGRATED DIGITAL SECURITY FRAMEWORK FOR INTERNATIONAL TRANSPORTATION: A CONCEPTUAL STUDY BASED ON INTERNATIONAL EXPERIENCE

Summary. The article presents a conceptual study of digital security in international transportation under conditions of the ongoing digital transformation of global logistics. The research aims to substantiate an integrated digital security framework for international transportation based on the analysis of international practices, contemporary digital technologies, and existing approaches to transport security management. To achieve this objective, the study applies a combination of comparative analysis, statistical analysis of international logistics indicators, structural and logical analysis, content analysis of recent scientific publications and international reports, case-study analysis of leading digital logistics initiatives, and scenario-based risk assessment. The study identifies the major challenges affecting the security of international transportation, including the growing number of cyber threats, fragmented regulatory frameworks, insufficient interoperability among digital logistics platforms, and uneven development of digital infrastructure across countries. International experience in the implementation of blockchain technology, the Internet of Things (IoT), artificial intelligence, Big Data analytics, and digital freight information systems is analyzed to determine their contribution to improving transport security and logistics resilience. Based on the conducted analysis, the paper proposes an integrated digital security framework that combines a Digital Data Exchange Platform with four interconnected functional components: the Analytical Monitoring Module, the Security and Response Management Module, the Regulatory Coordination Module, and the Human Resource Support Module. The coordinated interaction of these components enables continuous risk monitoring, intelligent decision support, cybersecurity management, regulatory compliance, and the development of digital competencies required for secure international logistics operations. The scientific contribution of the study lies in the conceptualization of a holistic digital security architecture that integrates technological, organizational, regulatory, analytical, and human-centered dimensions within a unified decision-support environment. The proposed framework provides a systematic basis for strengthening the resilience, interoperability, and security of international transportation systems and may serve as a foundation for future quantitative validation, simulation modelling, and practical implementation in digital logistics management.

1. INTRODUCTION

[1] Vinnytsia National Technical University; Khmelnytsky highway, 95, Vinnytsia, 21021, Ukraine; e-mail: vishtakiv@vntu.edu.ua; orcid.org/0000-0001-5646-4996
[2] Vinnytsia National Technical University; Khmelnytsky highway, 95, Vinnytsia, 21021, Ukraine; e-mail: lmaidanevych@gmail.com; orcid.org/0000-0002-7364-8874
[3] Vinnytsia National Technical University; Khmelnytsky highway, 95, Vinnytsia, 21021, Ukraine; e-mail: kuzhel2017@gmail.com; orcid.org/ 0000-0001-5646-0274
[4] Vinnytsia National Technical University; Khmelnytsky highway, 95, Vinnytsia, 21021, Ukraine; e-mail: vikahimich10@gmail.com; orcid.org/0009-0007-7122-5038
* Corresponding author. E-mail: vishtakiv@vntu.edu.ua

The rapid growth of international trade has accelerated the digital transformation of transportation and logistics, making secure, transparent, and efficient information exchange a key requirement for global supply chains. Technologies such as blockchain, the Internet of Things (IoT), artificial intelligence (AI), and automated logistics platforms improve cargo visibility, operational efficiency, and decision-making. However, their implementation is constrained by cybersecurity risks, fragmented regulatory frameworks, interoperability challenges, and uneven digital maturity across countries [1–4].

Recent studies have extensively examined individual aspects of transport digitalization, including blockchain-based logistics, IoT-enabled monitoring, AI applications, and digital freight documentation [1–10]. Although these technologies improve logistics performance, existing research primarily focuses on isolated technological or organizational solutions, while limited attention has been devoted to integrating technological, analytical, regulatory, and human-centered components within a unified digital security architecture.

To complement the literature review, a statistical analysis of international logistics indicators was conducted using reports from the World Bank, UNCTAD, WTO, DCSA, DHL, McKinsey, IBM, and the World Customs Organization (Tab. 1). The results confirm the rapid adoption of digital technologies alongside the increasing frequency of cybersecurity incidents, emphasizing the need for integrated approaches to transport security.

Accordingly, the research gap lies in the absence of a holistic framework capable of combining analytical monitoring, cybersecurity management, regulatory coordination, risk assessment, and human resource support within a coherent digital security environment for international transportation.

The scientific contribution of this study is the development of an Integrated Digital Security Framework for International Transportation, which synthesizes international experience and contemporary digital technologies into a unified conceptual architecture supporting secure information exchange, continuous risk monitoring, and coordinated decision-making. The purpose of this conceptual study is to substantiate the proposed framework and define its principal structural components and interaction mechanisms.

Table 1

Comparative analysis of key indicators characterizing the digital transformation of international transport and Logistics

Indicator	2019	2021	2023/2024	Trend
Global logistics market size, USD trillion [11, 12]	8,6	9,8	11,2 (2024)	↑ +30%
World merchandise trade volume growth [13]	–0,1%	+10,7%	+2,7% (2024 forecast)	Recovery
Container throughput worldwide, million TEU [14]	811	866	944	↑ +16,4%
Share of digital documentation in international logistics [15]	18%	29%	47%	↑ +161%
Companies using IoT in logistics [16]	21%	38%	61%	↑ +190%
Logistics companies implementing AI [17]	12%	24%	42%	↑ +250%
Organizations reporting cyberattacks on logistics infrastructure [18]	28%	39%	56%	↑ +100%
Average logistics costs (% GDP, developing countries) [19]	16–18%	15–17%	13–16%	↓
Countries implementing electronic freight documents (e-CMR) [20]	22	29	36	↑
Average customs clearance time using digital platforms [21]	72 h	39 h	18 h	↓ –75%

A comparative analysis of international logistics reports demonstrates a steady trend toward the digital transformation of transport systems (Tab. 1). According to Grand View Research [11], the global

logistics market reached approximately USD 11,2 trillion in 2024, representing an increase of nearly 30% compared with 2019 [12]. During the same period, global container throughput increased from 811 million TEU to approximately 944 million TEU, highlighting the growing demand for automated cargo monitoring, real-time information exchange, and secure digital logistics solutions [14].

The analysis further indicates the rapid adoption of digital technologies across the transport sector. The share of electronic freight documentation increased from 18% to 47% between 2019 and 2024 according to the Digital Container Shipping Association (DCSA) [15], while 61% of logistics companies currently employ IoT-based monitoring systems and 42% have implemented AI-supported decision-making tools for route optimization, demand forecasting, predictive maintenance, and risk assessment [16, 17]. In parallel, fully digital customs procedures have reduced average customs clearance times from approximately 72 hours to less than 18 hours, and the number of countries implementing the e-CMR convention has increased from 22 to 36, demonstrating substantial progress toward transport digitalization and regulatory harmonization [19–21].

Despite these achievements, cybersecurity and interoperability remain major challenges. According to the IBM X-Force Threat Intelligence Report, more than 56% of logistics organizations experienced significant cyber incidents in 2024, reflecting the growing exposure of digital logistics systems to cyber threats [18]. These findings demonstrate that technological innovation alone cannot ensure secure international transportation and must be complemented by integrated cybersecurity governance, standardized digital regulations, and coordinated risk management.

Although previous studies have examined individual technologies such as blockchain, IoT, artificial intelligence, digital freight documentation, and cybersecurity, limited attention has been paid to their integration within a unified security architecture. Therefore, this study addresses the need for a holistic conceptual framework that combines analytical monitoring, risk assessment, cybersecurity management, regulatory coordination, and human resource support within a single decision-support environment. The scientific contribution of the paper is the development of an Integrated Digital Security Framework for International Transportation, which synthesizes international experience and contemporary digital technologies into a coherent conceptual architecture supporting secure, resilient, and interoperable international logistics. The purpose of this conceptual study is to substantiate this framework and define its principal structural components and interaction mechanisms.

2. RESEARCH MATERIALS AND METHODS OF ECONOMIC AND ECOLOGICAL ENGINE INDICATORS

The research materials used in this study include international and national regulatory documents, scientific publications, analytical reports, and practical case studies addressing the digitalization and security of international transportation. These materials provide the empirical and theoretical basis for identifying the technological, organizational, regulatory, and human-related factors that determine the security of modern logistics systems.

The methodological basis of the research combines systems analysis, comparative analysis, content analysis of scientific literature and regulatory documents, and conceptual modeling. These methods were used to identify the relationships among technological, regulatory, organizational, and human-oriented components of digital security and to develop the integrated framework proposed in this study.

The regulatory materials analyzed in this study include both national and international legal documents governing digital transformation and cybersecurity in transport systems. Their comparative analysis enabled the identification of common principles, regulatory differences, and best practices in the implementation of digital security measures across international transportation systems. In Ukraine, such documents include the Law of Ukraine “On the National Geospatial Data Infrastructure” [22], which establishes the legal foundations for the electronic management of transport infrastructure; the Law of Ukraine “On Electronic Identification and Electronic Trust Services” [23], which defines mechanisms for digital identification and electronic document flow in transportation; and the Concept for the Development of the Digital Economy and Society of Ukraine for 2018–2020, which promoted

the digital transformation of logistics processes, particularly through the implementation of Smart technologies [24].

Within the framework of European integration, Ukraine is also adapting the provisions of EU Regulation No. 910/2014 (eIDAS) on electronic identification, as well as the norms of the eFTI Regulation, which in the EU regulates the electronic exchange of freight transport information between businesses and public authorities [25].

International legislation actively promotes the unification of digital approaches to transport security. Among the key documents is the TIR Convention, which now includes provisions on the electronic eTIR system aimed at cargo protection and simplified control procedures [26]. Another example is the Agreement on the Facilitation of International Road Transport adopted under ESCAP (United Nations), which envisages the implementation of digital solutions to enhance transport security in the Asia-Pacific region. In 2021, the International Maritime Organization (IMO) also approved Cyber Risk Management Guidelines for maritime transport, establishing minimum digital security standards for shipping companies.

In the European Union, the eFTI (Electronic Freight Transport Information) platform has been introduced, which is mandatory for all freight carriers operating within the EU. This system contributes to the unification of security approaches, reduces paper-based documentation, and lowers cybersecurity risks [27].

In countries like Singapore and South Korea, there is an active development of national digital logistics strategies that emphasize the use of artificial intelligence and big data analytics to identify threats in real-time. These initiatives are backed by specific cybersecurity legislation, such as the Cybersecurity Act [28].

Despite significant progress in the implementation of digital technologies, the analysis revealed several common limitations. These include the absence of unified international digital security standards, insufficient interoperability between national digital platforms, uneven levels of technological maturity, and fragmented regulatory approaches. As a result, existing solutions are often unable to ensure continuous protection throughout the entire international transportation process. Thus, ensuring the digital security of international transportation should rely not only on the implementation of advanced technologies but also on systematic legislative coordination at both the national and international levels.

The analysis of the above-mentioned research materials demonstrates that existing digital security solutions are implemented in a fragmented manner and are often limited to individual technological or regulatory aspects. Based on the identified strengths and limitations of existing approaches, an integrated digital security framework for international transportation was developed. The framework consolidates the key technological, organizational, regulatory, and human-oriented components into a unified architecture that addresses the identified research gap (Fig. 1).

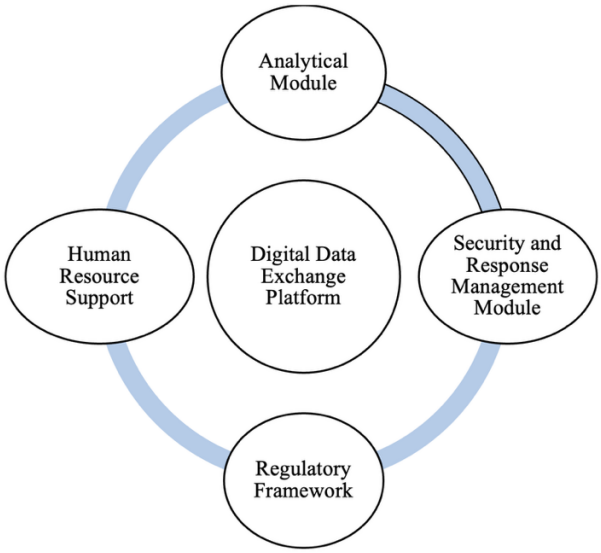


Fig. 1. Proposed integrated digital data exchange platform for secure international transportation

The proposed framework is designed as a multi-level digital architecture in which all functional components interact continuously to ensure secure and resilient international transportation. At the core of this model lies the Digital Data Exchange Platform, which ensures connectivity among all participants in the logistics chain: carriers, shippers, customs authorities, insurance companies, and control systems. Surrounding this platform are four critical components:

1. Analytical Module – designed for advanced data processing, predictive modeling, and real-time monitoring to enhance decision-making and optimize system performance.

2. Security and Response Management Module – providing rapid incident detection, emergency coordination, and system recovery measures to maintain resilience and reliability.

3. Regulatory Framework – encompassing the legal, institutional, and normative provisions that guarantee compliance, data protection, and cybersecurity.

4. Human Resource Support – reflecting the indispensable role of human expertise, training, and competence in ensuring the platform's sustainable functioning.

The proposed framework was developed using systems analysis and conceptual modeling. First, international regulations and digital logistics practices were analyzed to identify the key technological, organizational, regulatory, and human-centered factors influencing transport security. These components were subsequently integrated into a unified conceptual architecture supporting secure decision-making in international transportation.

The framework is built around a Digital Data Exchange Platform, which provides standardized and secure information exchange in accordance with international frameworks (e.g., eFTI, e-CMR, and ISO standards). The platform integrates blockchain technologies to ensure data integrity and authenticity, while IoT devices enable continuous real-time cargo monitoring.

The Analytical Monitoring Module collects and processes data from IoT sensors, cargo tracking systems, blockchain platforms, and external information sources to identify anomalies, assess transportation risks, and support predictive analysis. Using artificial intelligence and machine learning techniques, the module enables real-time situational awareness and provides decision support for risk prevention and route optimization [29–33].

The Security and Response Management Module receives analytical outputs and coordinates appropriate response actions, including cybersecurity protection, incident management, route adjustment, and security protocol activation. Its operation follows internationally recognized risk management principles defined in ISO 31000:2018, the NIST Cybersecurity Framework (CSF 2.0), and the ENISA Threat Landscape 2024, ensuring continuous risk assessment, regulatory compliance, and resilience of digital logistics systems [34–38].

The Regulatory Coordination Module ensures compliance with international transport regulations, digital documentation standards, and data protection requirements, whereas the Human Resource Support Module strengthens personnel competencies through training, certification, and cybersecurity awareness programs [39].

The coordinated interaction of these modules, illustrated in Fig. 2, establishes an integrated digital security environment capable of supporting continuous monitoring, secure information exchange, intelligent risk assessment, and coordinated decision-making throughout international transportation processes.

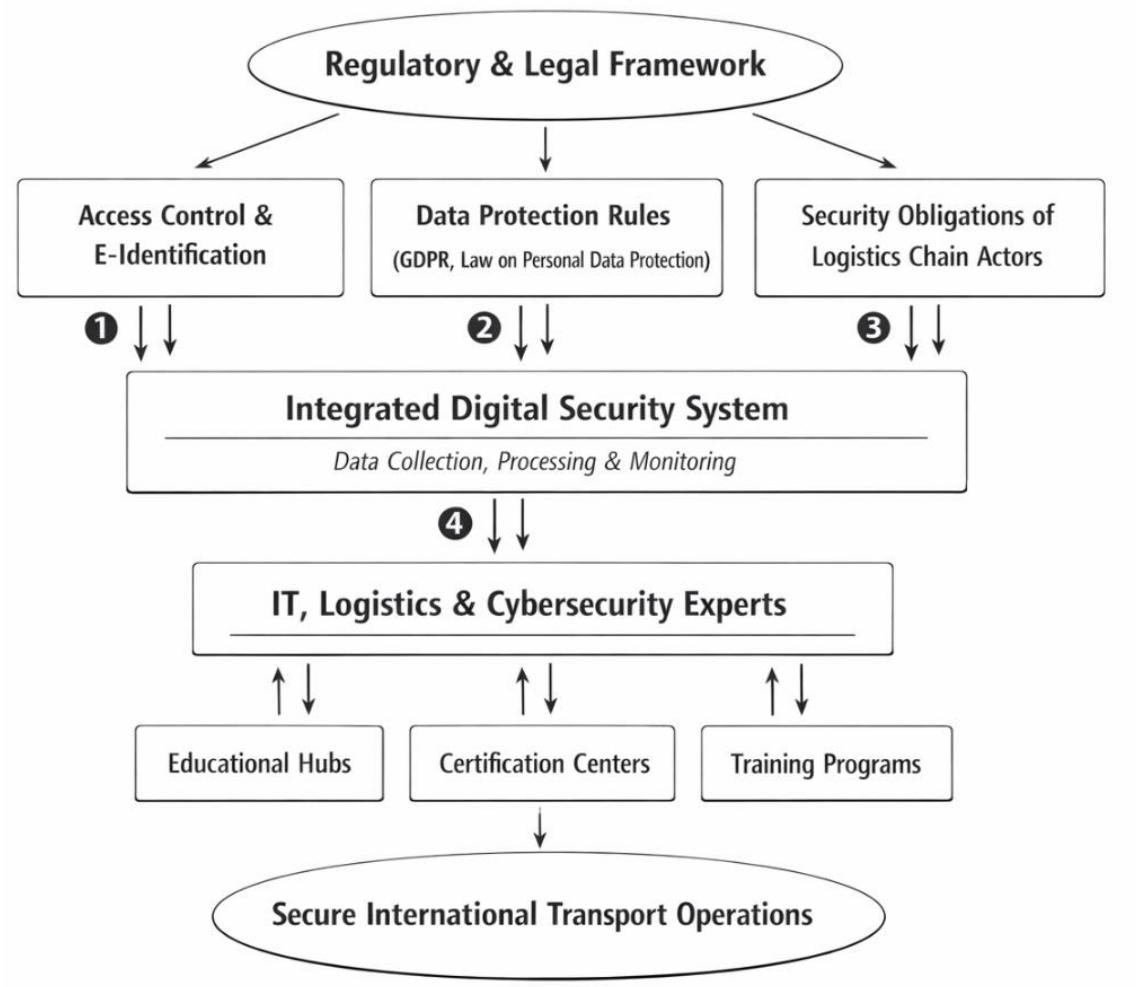


Fig. 2. Conceptual interaction of regulatory, technological, and human-oriented components within the integrated digital security framework

Fig. 2 presents a generalized scheme of the functioning of the digital security system for international transport, in which the regulatory and legal framework acts as a key integrating element. It defines the rules for access to digital platforms based on electronic identification, data protection requirements (in particular, in accordance with the GDPR and national legislation) and the obligations of participants in the logistics chain in the field of security. The central component is an integrated digital security system that ensures the collection, processing and monitoring of data. The effectiveness of its functioning largely depends on the human factor – specialists in the fields of IT, logistics and cybersecurity, whose training is carried out through educational hubs, certification centers and training programs. The combined interaction of these elements forms a holistic mechanism for ensuring the security of international transport operations in the digital environment.

3. RESEARCH METODOLOGY

Since this study is conceptual, the proposed Integrated Digital Security Framework was validated through complementary analytical, comparative, statistical, and scenario-based methods rather than software implementation or field experiments. The methodology was designed to evaluate the consistency, applicability, and practical relevance of the proposed framework using international regulations, scientific publications, logistics reports, and representative digital logistics initiatives.

The research comprised five stages. Comparative analysis was conducted to examine international approaches to transport digitalization, including eFTI, blockchain-based logistics platforms, DCSA initiatives, and national digital transport strategies. The findings, summarized in Tab. 2, revealed significant differences in digital maturity, interoperability, and cybersecurity governance, supporting the need for an integrated security framework.

Statistical and analytical analyses were performed using international logistics indicators reported by the World Bank, UNCTAD, WTO, DCSA, DHL, McKinsey, IBM, and the World Customs Organization [11–21]. The analyzed indicators included logistics market growth, container throughput, digital freight documentation, IoT and AI adoption, cybersecurity incidents, customs clearance time, and e-CMR implementation. The results (Tab. 1) confirm rapid digitalization accompanied by increasing cybersecurity risks, highlighting the need for integrated technological, organizational, and regulatory security measures.

Structural and logical analysis was applied to develop the conceptual architecture presented in Fig. 2, defining the interactions among analytical monitoring, cybersecurity management, regulatory coordination, and human resource support. In parallel, content and case-study analyses of more than 35 recent scientific publications, international reports, and representative digital logistics initiatives (TradeLens, eFTI, DCSA, and national digital freight platforms) provided the theoretical and practical basis for selecting the framework components.

Finally, scenario-based risk assessment was used to evaluate the framework under representative disruption scenarios, including cyberattacks, supply chain disruptions, unauthorized access to transport documentation, and regulatory inconsistencies. The probability–impact assessment (Tab. 3) demonstrated that effective transport security requires coordinated technological, organizational, regulatory, and human-centered measures rather than isolated digital solutions.

The combined application of these methods provides conceptual validation of the proposed framework and demonstrates its applicability as a unified decision-support architecture for secure international transportation under conditions of digital transformation.

4. ANALYSIS OF RESEARCH RESULTS TO DETERMINE THE MOST EFFECTIVE WORK PROCESS

The comprehensive analysis of scientific publications, international logistics reports, comparative case studies, and scenario-based risk assessment revealed that existing digital logistics initiatives predominantly address individual technological, organizational, or regulatory challenges. While blockchain platforms enhance data integrity, IoT technologies improve real-time cargo monitoring, and artificial intelligence supports predictive decision-making, these solutions are generally implemented independently and lack systematic integration within a unified digital security architecture.

The statistical analysis presented in Table 1 indicates a steady increase in the adoption of digital technologies across international transportation, including electronic freight documentation, IoT-enabled monitoring systems, and AI-based logistics management. At the same time, the growing number of cybersecurity incidents and the persistence of interoperability and regulatory challenges demonstrate that technological advancement alone is insufficient to ensure the security and resilience of international transportation systems.

Furthermore, the comparative analysis of international digital logistics initiatives (Tab. 2) and the scenario-based risk assessment (Tab. 3) highlight that effective transport security requires coordinated interaction among technological solutions, regulatory mechanisms, organizational processes, and human resource management. These findings confirm that a fragmented implementation of digital technologies cannot fully address the complexity of risks associated with modern international logistics.

Based on these findings, a conceptual integrated digital security framework was developed to consolidate the essential technological, analytical, organizational, regulatory, and human-centered components into a unified architecture. The framework is intended to support secure information exchange, continuous risk monitoring, intelligent decision-making, and coordinated response

mechanisms throughout international transportation processes. The proposed Integrated Digital Security Framework for International Transportation is presented in Fig. 3.

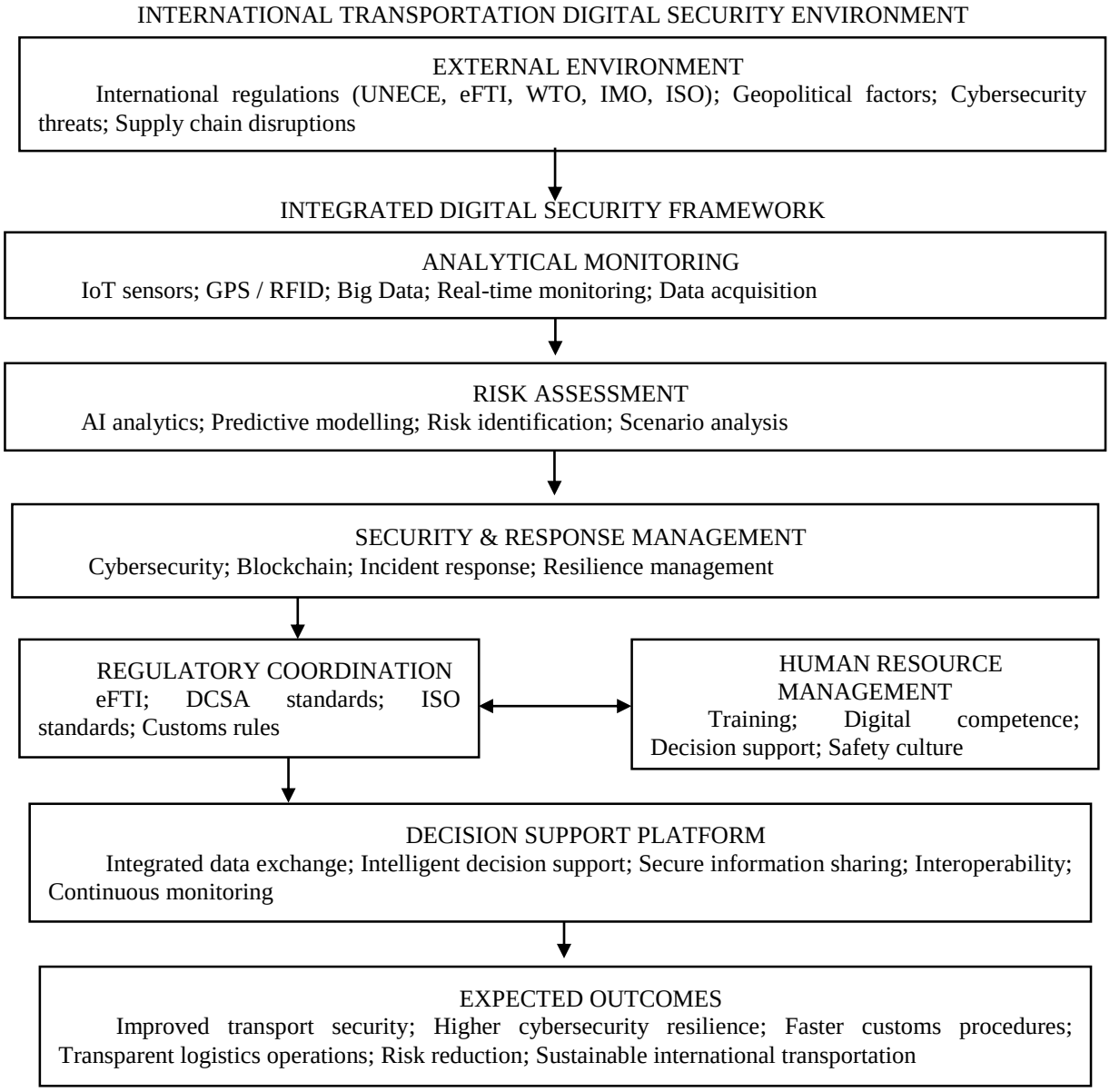


Fig. 3. Integrated Digital Security Framework for International Transportation

The proposed conceptual framework integrates technological, organizational, regulatory, and human-centered components into a unified digital security architecture for international transportation. The framework begins with continuous analytical monitoring based on IoT devices, GPS, RFID technologies, and Big Data collection. The acquired information is processed through artificial intelligence and predictive analytics to identify potential risks and evaluate transportation security.

Based on the analytical results, the security and response management module implements cybersecurity protection, blockchain-supported data integrity, incident response mechanisms, and resilience management. Regulatory coordination ensures compliance with international standards and digital logistics regulations, including eFTI, DCSA, ISO, and customs requirements, while the human resource management module supports personnel competency, cybersecurity awareness, and decision-making processes.

The interaction of all framework components is coordinated through an integrated decision-support platform that enables secure information exchange, interoperability among logistics stakeholders, and continuous monitoring of transportation processes. The expected outcomes include improved transport security, enhanced cybersecurity resilience, reduced operational risks, increased transparency of logistics operations, and sustainable development of international transportation systems

The proposed framework (Fig. 3) represents a holistic conceptual architecture that integrates the key technological, organizational, regulatory, analytical, and human-centered components required to ensure digital security throughout international transportation processes. Unlike existing approaches that primarily focus on isolated technological solutions, the proposed framework establishes functional relationships among continuous analytical monitoring, intelligent risk assessment, cybersecurity management, regulatory coordination, and human resource support within a unified decision-support environment.

The integration of these components enables continuous information exchange among logistics stakeholders, facilitates timely identification of potential threats, and supports coordinated decision-making under dynamic transportation conditions. Consequently, the framework provides a conceptual basis for improving the resilience, interoperability, and security of international logistics operations while supporting compliance with international digital transport standards.

To further evaluate the practical relevance of the proposed framework, it is necessary to compare its structural components with the capabilities of existing international digital logistics initiatives. Such a comparison makes it possible to identify the strengths and limitations of currently implemented solutions and to determine the extent to which they address the technological, organizational, regulatory, and security requirements of modern international transportation. The comparative analysis of the most widely adopted international digital logistics initiatives is presented in Tab. 2.

Table 2

Comparative analysis of international digital logistics initiatives and their contribution to transport security

Initiative	**Main objective**	**Core digital technologies**	**Security mechanisms**	**Advantages**	**Limitations**	**Relevance to the proposed framework**
TradeLens (IBM & Maersk) [1,14,18]	End-to-end visibility of maritime supply chains	Blockchain, cloud computing, smart contracts, APIs	Immutable transaction records, encrypted data exchange, decentralized validation	High transparency, reduced documentation time, improved cargo traceability	Platform discontinued in 2022; limited stakeholder adoption; interoperability issues	Demonstrates the importance of secure data sharing, blockchain integrity, and interoperability principles
eFTI (Electronic Freight Transport Information, EU) [13,20,25]	Standardized electronic freight information exchange across EU member states	Digital documents, interoperable data exchange, electronic signatures	Regulatory compliance, secure electronic document validation, access control	Harmonized regulatory framework, paperless logistics, faster customs procedures	Different implementation rates among EU countries; integration costs	Illustrates the role of regulatory coordination and standardized digital documentation
Digital Container Shipping Association (DCSA) [14,15]	Standardization of digital container shipping processes	Digital standards, APIs, electronic Bill of Lading	Standardized secure communication, authentication, digital	International interoperability, unified data standards, increased	Voluntary implementation by carriers; dependence	Supports interoperability and standardized cybersecurity requirements

		(eBL), interoperability protocols	documentation	digital adoption	on industry participation	
National Digital Logistics Platforms (Singapore, South Korea, Netherlands) [16,19]	National coordination of logistics information and customs services	IoT, AI, Big Data, cloud platforms, digital customs	Integrated cybersecurity, real-time monitoring, risk analytics	Efficient customs clearance, predictive logistics management, high operational efficiency	Different national regulations; limited cross-border compatibility	Demonstrates integration of analytical monitoring, AI decision support, and national cybersecurity policies
IoT-based Smart Logistics Platforms [2,16,17]	Real-time monitoring of cargo and transport infrastructure	IoT sensors, GPS, RFID, cloud computing	Continuous monitoring, anomaly detection, asset tracking	Increased cargo visibility, predictive maintenance, improved transport safety	Cybersecurity vulnerabilities of connected devices	Supports analytical monitoring and real-time risk detection
AI-driven Logistics Management Systems [3,17,18]	Intelligent transport planning and operational optimization	Artificial intelligence, machine learning, predictive analytics	Automated anomaly detection, predictive risk assessment	Route optimization, demand forecasting, proactive risk management	High implementation costs; dependence on data quality	Supports analytical risk assessment and decision-support module

The comparative analysis presented in Tab. 2 demonstrates that existing international digital logistics initiatives effectively address specific aspects of transport digitalization but do not provide a comprehensive digital security architecture. For example, TradeLens improved supply chain transparency through blockchain technology, while eFTI and the Digital Container Shipping Association (DCSA) have enhanced interoperability and standardized electronic freight information. Similarly, national digital logistics platforms successfully integrate customs authorities, logistics operators, and transport companies using IoT, artificial intelligence, cloud computing, and centralized digital services.

Despite these advances, common limitations remain. Most initiatives focus on individual technological or regulatory functions and provide only limited integration of cybersecurity management, analytical risk assessment, regulatory coordination, and human-centered decision support. In addition, differences in national legislation, uneven digital maturity, and the lack of universally accepted interoperability standards continue to create vulnerabilities in international transportation systems [15].

These findings justify the proposed Integrated Digital Security Framework, which combines technological, analytical, regulatory, organizational, and human resource components within a unified decision-support environment. Such integration is expected to improve situational awareness, strengthen transport resilience, support coordinated responses to emerging threats, and enhance the overall security of international logistics operations.

However, the practical applicability of any conceptual framework depends not only on its structural completeness but also on its ability to address realistic operational risks encountered during international transportation. Consequently, the proposed framework was further evaluated through a scenario-based risk assessment, which considers representative disruption scenarios and identifies appropriate response mechanisms for maintaining transport security and operational continuity. The results of the scenario-based risk assessment are presented in Tab. 3.

Table 3

Scenario-based risk assessment matrix for international transportation

Scenario	Probability	Potential impact	Risk level	Proposed response measures within the integrated digital security framework
Cyberattack on digital logistics infrastructure (ransomware, unauthorized access, data manipulation)	High	Disruption of transport operations, loss of cargo visibility, financial losses, leakage of confidential information	Critical	AI-based anomaly detection; multi-factor authentication; blockchain-secured transaction records; continuous cybersecurity monitoring; automated incident response; backup and disaster recovery procedures
Disruption of international supply chains caused by geopolitical conflicts or natural disasters	Medium–High	Cargo delays, increased transportation costs, route interruptions, reduced logistics resilience	High	Predictive analytics; dynamic route optimization; IoT-enabled cargo tracking; digital twin simulation; alternative supplier and transport route management
Failure or incompatibility of digital information exchange between international logistics partners	Medium	Delays in customs clearance, inconsistent documentation, reduced interoperability	Medium	Adoption of eFTI standards; DCSA interoperability protocols; standardized APIs; electronic freight documentation; automated data validation
Human errors during digital logistics operations (incorrect data entry, inadequate cybersecurity awareness, operational mistakes)	Medium	Documentation errors, delayed deliveries, increased security vulnerabilities	Medium	Personnel training; competency management; decision-support systems; automated verification procedures; continuous monitoring of operator activities; AI-assisted recommendations
Cyberattack on digital logistics infrastructure (ransomware, unauthorized access, data manipulation)	High	Disruption of transport operations, loss of cargo visibility, financial losses, leakage of confidential information	Critical	AI-based anomaly detection; multi-factor authentication; blockchain-secured transaction records; continuous cybersecurity monitoring; automated incident response; backup and disaster recovery procedures

5. CONCLUSIONS

The conducted conceptual study demonstrates that the digital transformation of international transportation creates new opportunities for improving logistics efficiency while simultaneously introducing significant cybersecurity, interoperability, and operational resilience challenges. The analysis of scientific literature, international regulations, logistics reports, and global digital practices confirms that existing approaches primarily address isolated technological or organizational aspects of transport digitalization and lack an integrated security architecture.

The study combined comparative, statistical, structural and logical, content, case-study, and scenario-based analyses to substantiate an Integrated Digital Security Framework for International

Transportation. The obtained results indicate that, despite the rapid adoption of IoT, blockchain, artificial intelligence, electronic freight documentation, and interoperable digital platforms, effective transport security requires coordinated interaction among technological, analytical, regulatory, organizational, and human-centered components. Comparative analysis of leading international digital logistics initiatives and scenario-based risk assessment further revealed that cyberattacks, supply chain disruptions, interoperability failures, and human-related factors remain the principal threats affecting international transportation.

The principal scientific contribution of this study is the development of a holistic conceptual framework that integrates analytical monitoring, cybersecurity management, blockchain-supported data exchange, regulatory coordination, and human resource support within a unified decision-support environment. The proposed framework provides a systematic basis for improving the resilience, interoperability, and security of international transportation systems and may support the development of digital logistics strategies and transport security management practices.

Future research should focus on validating the proposed framework using real-world logistics datasets, simulation modelling, Digital Twin technologies, and artificial intelligence methods to evaluate its effectiveness under different operational scenarios and regulatory environments.

References

1. Ahmed, W. & Rios, A. Digitalization of the international shipping and maritime logistics industry: a case study of TradeLens. *The Digital Supply Chain*. 2022. Pp. 309–323. DOI: 10.1016/B978-0-323-91614-1.00018-6.
2. Rybchuk, A.V. & Lapchuk, Ya.S. & Palasevych, M.B. Global digitalization of the world transport services market. *Business Inform*. 2022. No. 12. P. 173–178. DOI: 10.32983/2222-4459-2022-12-173-178.
3. Mahraz, M.-I. & Berrado, A. & Benabbou, L. Digital transformation and logistics optimization. In: *Proceedings of the International Conference on Industrial Engineering and Operations Management*. 2019. P. 917–931.
4. Cichosz, M. & Wallenburg, C.M. & Knemeyer, A.M. Digital transformation at logistics service providers: barriers, success factors and leading practices. *International Journal of Logistics Management*. 2020. Vol. 31. P. 209–238. DOI: 10.1108/IJLM-08-2019-0229.
5. Nitsche, B. & Straube, F. Current state and future of international logistics networks—The role of digitalization and sustainability in a globalized world. *Logistics*. 2023. Vol. 7. No. 83. DOI: 10.3390/logistics7040083.
6. Ahir, D. & Agrawal, A. & Sumetha, M. A research paper on study of digitalization in international logistics. *International Journal of Creative Research Thoughts*. 2023. Vol. 11. No. 2.
7. Ivanov, D. The Industry 5.0 framework: viability-based integration of the resilience, sustainability, and human-centricity perspectives. *International Journal of Production Research*. 2023. №61(5). P. 1683–1695. DOI: 10.1080/00207543.2022.2118892
8. Ivanov, D., Dolgui, A., Blackhurst, J. V., & Choi, T. M. Toward supply chain viability theory: from lessons learned through COVID-19 pandemic to viable ecosystems. *International Journal of Production Research*. 2023. №61(8). P. 2402–2415. DOI: 10.1080/00207543.2023.2177049
9. Jović, M., Tijan, E., Brčić, D., Pucihar, A. Digitalization in Maritime Transport and Seaports: Bibliometric, Content and Thematic Analysis. *Journal of Marine Science and Engineering*. 2022. Vol. 10(4). 486. DOI: 10.3390/jmse10040486
10. Tijan, E., Jović, M., Brčić, D., Pucihar, A. Factors of Digital Transformation in the Maritime Transport Sector. *Sustainability*. 2022. Vol. 14(15). 9776. DOI: 10.3390/su14159776
11. Grand View Research. *Logistics Market Size, Share & Trends Analysis Report. 2024*. URL: https://www.grandviewresearch.com/industry-analysis/logistics-market
12. Statista. *Global Logistics Industry Market Size from 2019 to 2024*. 2024. URL: https://www.statista.com

13. World Trade Organization. *Global Trade Outlook and Statistics 2024*. Geneva : World Trade Organization, 2024. URL: https://www.wto.org
14. United Nations Conference on Trade and Development. Review of Maritime Transport 2024. New York; Geneva: United Nations, 2024. URL: https://unctad.org/publication/review-maritime-transport-2024
15. Digital Container Shipping Association. *DCSA Annual Report 2024*. 2024. URL: https://dcsa.org/
16. DHL. DHL Logistics Trend Radar 7.0. *DHL Customer Solutions & Innovation*. 2024. URL: https://www.dhl.com/global-en/home/insights-and-innovation/insights/logistics-trend-radar.html
17. McKinsey & Company. *The State of AI in Supply Chain and Logistics*. 2024. URL: https://www.mckinsey.com
18. IBM Security. *X-Force Threat Intelligence Index 2024*. 2024. URL: https://www.ibm.com/reports/threat-intelligence
19. World Bank. Connecting to Compete 2023: Trade Logistics in the Global Economy – The Logistics Performance Index and Its Indicators. *Washington, DC* : World Bank, 2023. URL: https://lpi.worldbank.org
20. International Road Transport Union (IRU). *IRU Annual Report 2024*. 2024. URL: https://www.iru.org
21. World Customs Organization. Time Release Study (TRS) Guide. Version 4. Brussels : *World Customs Organization, 2024*. URL: https://www.wcoomd.org
22. Verkhovna Rada of Ukraine. *Law of Ukraine "On the National Infrastructure of Geospatial Data"*. Available at: https://zakon.rada.gov.ua/laws/show/554-20.
23. Verkhovna Rada of Ukraine. *Law of Ukraine "On Electronic Identification and Electronic Trust Services"*. Available at: https://zakon.rada.gov.ua/laws/show/2155-19.
24. Verkhovna Rada of Ukraine. *Resolution "On approval of the Concept for the development of the digital economy and society of Ukraine for 2018–2020 and approval of the action plan for its implementation"*. Available at: https://zakon.rada.gov.ua/laws/show/67-2018-p.
25. European Union. *Regulation (EU) 2019/1239 of the European Parliament and of the Council of 20 June 2019 establishing a European Maritime Single Window environment and repealing Directive 2010/65/EU*. Available at: https://eur-lex.europa.eu/eli/reg/2019/1239/oj.
26. UNECE. *TIR Handbook – Eleventh Revised Edition*. United Nations Economic Commission for Europe. Available at: https://unece.org/transport/publications/tir-handbook-eleventh-revised-edition.
27. European Union. *Electronic freight transport information*. Available at: https://eur-lex.europa.eu/EN/legal-content/summary/electronic-freight-transport-information.html.
28. Cyber Security Agency of Singapore. *Cybersecurity Act*. Available at: https://www.csa.gov.sg/legislation/cybersecurity-act.
29. Volkov, V. & Volkova, T. & Kuzhel, V. & Kyrytsya, I. & Vishtak, I. Intelligent manufacturing systems for controlling the technical condition of vehicles in the life cycle. In: *Advances in Design, Simulation and Manufacturing VIII*. Cham: Springer. 2025. P. 241–254. DOI: 10.1007/978-3-031-95211-1_21.
30. Volkov, V. et al. Information systems for vehicles technical condition monitoring. In: *Data Centric Business and Applications*. Lecture Notes on Data Engineering and Communications Technologies. Vol. 195. Cham: Springer. 2024. P. 61–96. DOI: 10.1007/978-3-031-54012-7_4.
31. Kechagias, E.P., Chatzistelios, G., Papadopoulos, G.A., Apostolou, P. Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*. 2022. Vol. 37. DOI: 10.1016/j.ijcip.2022.100526
32. Podrecca, M., Culot, G., Nassimbeni, G., Sartor, M. Information security and value creation: The performance implications of ISO/IEC 27001. *Computers in Industry*. 2022. Vol. 142. 103744. DOI: 10.1016/j.compind.2022.103744
33. Alevizos, L., Bhakuni, L., Jäschke, S. A value driven framework for cybersecurity innovation in transportation and infrastructure. *International Journal of Information Technology*. 2025. DOI: 10.1007/s41870-024-02288-w

34. Fan, S. & Yang, Z. Safety and security co-analysis in transport systems: Current state and regulatory development. *Transportation Research Part A: Policy and Practice*. 2022. Vol. 166. P. 369–388. DOI: 10.1016/j.tra.2022.11.005
35. Zhou, Y. et al. Digitalization in the Maritime Logistics Industry: A Systematic Literature Review of Enablers and Barriers. *Journal of Marine Science and Engineering*. 2025. Vol. 13(4). 797. DOI: 10.3390/jmse13040797
36. International Organization for Standardization. *ISO 31000:2018 Risk management — Guidelines*. Geneva : ISO, 2018. URL: https://www.iso.org/standard/65694.html.
37. National Institute of Standards and Technology. *The NIST Cybersecurity Framework (CSF) 2.0*. Gaithersburg, MD: U.S. Department of Commerce, National Institute of Standards and Technology, 2024. URL: https://www.nist.gov/cyberframework .
38. European Union Agency for Cybersecurity. *ENISA Threat Landscape 2024*. Heraklion : ENISA, 2024. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 (дата звернення: 30.07.2026).
39. Kumar, S., Mallipeddi, R. Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*. 2022. Vol. 31(12). DOI: 10.1111/poms.13859

Received XX.XX.20XX; accepted in revised form XX.XX.20XX