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

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

Contents

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.

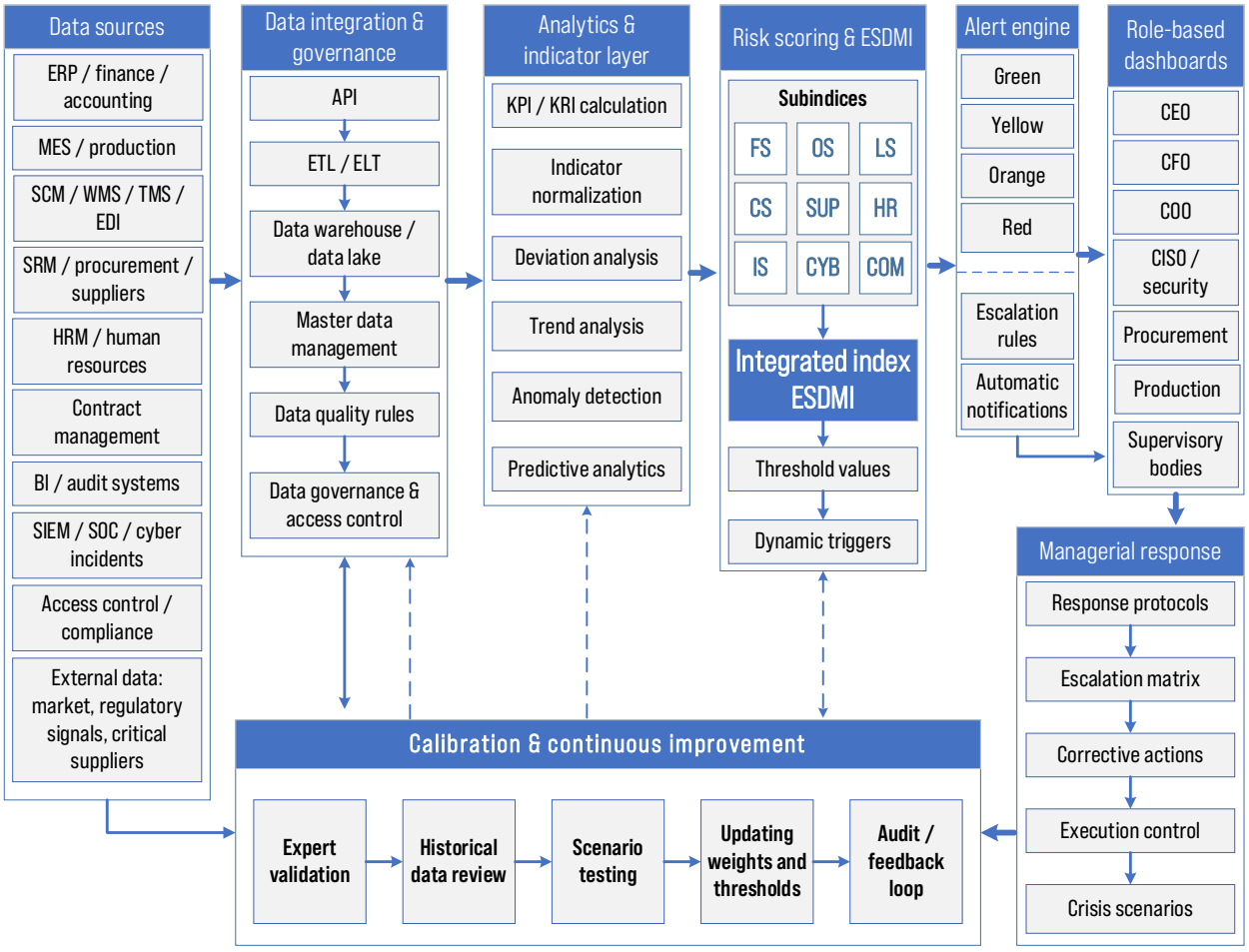
Component weights may be determined in several ways. At the first stage, expert assessment with specialists in finance, production, logistics, procurement, corporate governance, cybersecurity and defence management is appropriate. To improve methodological reliability, the Delphi procedure, AHP or the 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