INFORMATION SYSTEMS AND DECISION SUPPORT IN NATIONAL SECURITY: DIGITAL TRANSFORMATION OF ROMANIA'S DEFENCE CAPABILITIES

Assoc. Prof. Florentina-Loredana DRAGOMIR-CONSTANTIN, PhD

"Carol I" National Defence University, Bucharest

DOI: 10.55535/RMT.2026.1-2.06

The article analyses the role of information systems in configuring and optimizing Romania's defence architecture, highlighting their contribution to supporting strategic governance and decision-making processes. The study starts from the premise that the efficiency of the defence system depends essentially on the capacity to integrate, process and capitalize on data from multiple sources, in order to build a coherent and updated operational picture.

In this context, the paper highlights the role of integrated information infrastructures in increasing institutional interoperability and facilitating coordination between defence actors. Advanced information systems allow the correlation of operational requirements with available resources, supporting strategic planning, efficient allocation of capabilities and substantiating decisions through risk assessment and investment prioritization.

At the same time, integrated digital platforms contribute to the aggregation and correlation of heterogeneous data flows, supporting the development of situational awareness and the anticipation of strategic developments through the use of big data and artificial intelligence technologies. In addition, the article highlights the role of information systems in supporting the national defence industry, through the development of collaborative platforms dedicated to research and development management, monitoring industrial capabilities and aligning production with operational requirements. Overall, the study highlights the contribution of information systems to increasing the coherence, efficiency and adaptability of the defence architecture, in the context of a dynamic security environment.

Keywords: information systems; national security; decision support; digital sovereignty; interoperability;

INTRODUCTION

The contemporary security environment, marked by complexity, uncertainty and increasing interdependencies, requires a profound rethinking of the way in which defence systems are configured and managed. Information is becoming a fundamental strategic resource, and the capacity to collect, integrate, analyse and capitalize on data is emerging as a determining factor in decision-making efficiency and organizational performance. Thus, information systems no longer represent just a technological support, but a central element in the functional architecture of modern defence systems.

Information is becoming a fundamental strategic resource, and the capacity to collect, integrate, analyse and capitalize on data is emerging as a determining factor in decision-making efficiency and organizational performance.

In the case of Romania, the need to consolidate an adaptive and coherent defence architecture is closely linked to the development of information infrastructures capable of supporting rapid, substantiated and integrated decision-making processes. From this perspective, institutional interoperability, coordination between relevant actors and efficient use of resources directly depend on the level of maturity of information systems and their degree of integration. Moreover, technological developments in the field of big data and artificial intelligence create significant opportunities for improving situational awareness and anticipating strategic dynamics.

The article aims to analyse the role of information systems in configuring and optimizing Romania's defence architecture, with a focus on their contribution to supporting strategic governance and decision-making processes. The approach is based on the premise that the efficiency of the defence system depends essentially on the capacity to integrate and capitalize on data from multiple sources, in order to build a coherent and updated operational picture. In this framework, the paper examines the contribution of integrated information infrastructures to increasing institutional interoperability and facilitating coordination between defence actors, highlighting the role of advanced information systems in correlating operational requirements with available resources. It also analyses the implications

of using integrated digital platforms and emerging technologies in supporting strategic planning, risk assessment and forecasting processes.

Finally, the article addresses the role of information systems in supporting the national defence industry, emphasizing the importance of developing collaborative platforms for research and development management and aligning production with operational requirements. Through this approach, the study contributes to the outline of a conceptual and application framework for the integration of information systems into the defence architecture, in order to increase its coherence, efficiency and adaptability.

The analysis of Romania's current defence architecture reveals the existence of systemic vulnerabilities that go beyond the strictly operational dimension and reflect profound dysfunctions at the level of strategic governance.

STRUCTURAL DEFICIENCIES AND VULNERABILITIES OF THE DEFENCE ARCHITECTURE

The analysis of Romania's current defence architecture reveals the existence of systemic vulnerabilities that go beyond the strictly operational dimension and reflect profound dysfunctions at the level of strategic governance. These vulnerabilities are not generated exclusively by budgetary limitations, but especially by the absence of a coherent information structure that integrates decision-making processes.

One of the main dysfunctions is institutional fragmentation. Relevant actors in the defence field – the Ministry of National Defence, intelligence structures, institutions responsible for the defence industry and regulatory bodies – often operate in the absence of a common digital framework, which limits information exchange and strategic coordination. In the absence of information interoperability, decisions are made on the basis of incomplete data sets, which reduces efficiency and increases the risk of strategic errors.

Another critical element is the decision-making vacuum generated by the absence of integrated planning mechanisms. The lack of IT tools capable of correlating operational needs with available resources and strategic priorities leads to incoherence in the procurement process and inefficient use of resources. In this framework, planning becomes reactive, dependent on external pressures or immediate constraints, instead of being the result of data-driven strategic analysis.

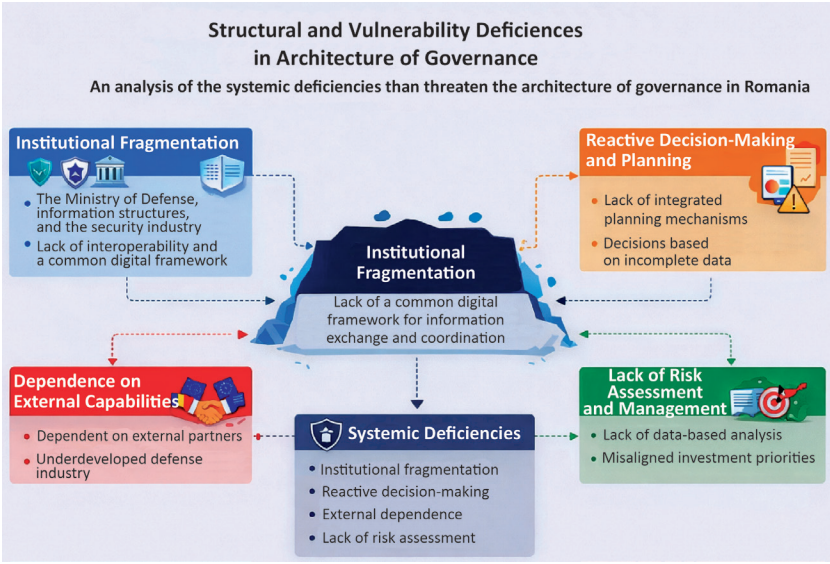

Figure 1: Structural deficiencies and vulnerabilities of the defence architecture

Dependence on external capabilities is another major vulnerability. In the absence of a functional defence industry and an information infrastructure to support its development, Romania is forced to rely on external partners to ensure security. This dependence limits decision-making autonomy and reduces the state's ability to act independently in crisis situations.

Also, the lack of a systematic risk assessment and clear prioritization of investments highlights the absence of a data-based decision-making culture. In a security environment characterized by uncertainty and complexity, the ability to anticipate developments and allocate resources optimally becomes essential. Without adequate information tools, this capacity remains limited. These deficits indicate the existence of a structural problem: the absence of an integrated information architecture to support strategic governance. Its absence determines that institutional reforms and material investments cannot produce sustainable effects, because there is no coherent coordination and evaluation mechanism.

In a security environment characterized by uncertainty and complexity, the ability to anticipate developments and allocate resources optimally becomes essential. Without adequate information tools, this capacity remains limited.

INFORMATION SYSTEMS AS A SUPPORT FOR STRATEGIC DECISION

The military decision-making process requires information infrastructures capable of managing large volumes of data and providing analytical support in real time, becoming essential components of the command-and-control architecture and directly influencing the efficiency of military leadership. In this context, the transition from a model based predominantly on intuition to one based on data represents a paradigmatic change, in which decisions are supported by complex analyses generated by advanced information systems, contributing to reducing uncertainty and increasing accuracy.

A defining function of modern information systems is the integration of data from operational, logistical, economic and intelligence sources into a unitary analytical framework. Their strategic value derives from the ability to transform large volumes of data into contextualized and decision-relevant knowledge, through interoperability, semantic standardization, and real-time analysis.

A defining function of modern information systems is the integration of data from operational, logistical, economic and intelligence sources into a unitary analytical framework. Their strategic value derives from the ability to transform large volumes of data into contextualized and decision-relevant knowledge, through interoperability, semantic standardization, and real-time analysis (Onwujekwe, Weistroffer, 2025; Rane, Chika, Rane, 2026). Multi-source integration allows the construction of a unified operational picture, in which performance indicators, risks, and external environmental dynamics are correlated coherently and predictively (Li, Zhang, 2025; Jafari, Akhavan, Akbari, 2026).

This information convergence supports the development of an extended situational awareness and improves the ability to anticipate developments. Studies show that the integration of data from multiple sources contributes to increasing the quality of situational diagnosis and the formulation of adaptive responses in contexts characterized by complexity and volatility (Onwujekwe, Weistroffer; Adha et al., 2026). At the same time, integrated digital infrastructures allow for early identification of vulnerabilities and opportunities, by simultaneously analysing the dynamics associated with resources, logistics, and the operational environment (Sarkar, Gunasekaran, Patil, 2025; Sentia et al., 2026). Centralizing real-time data is associated with optimizing resource allocation, reducing decision latency, and increasing institutional agility (Kazak et al., 2025; Su, 2026), facilitating the shift to a proactive approach based on anticipation (Shoaib et al., 2026; Li, Zhang). The integration of artificial intelligence and machine learning technologies extends these capabilities, allowing for the identification

of patterns and the estimation of developments based on historical correlations and current dynamics. These technologies facilitate the transition from descriptive to predictive analytics, providing support for scenario simulation and decision support in real time (Hurochkina, Bondarenko, 2025; Jimoh, Adejobi, 2026). Simulation models allow for the probabilistic assessment of different courses of action and the development of robust planning mechanisms capable of integrating uncertainty and optimizing responses in dynamic environments (Lee et al., 2023; Ruther, Strohal, Stütz, 2023). The use of digital twin technologies also facilitates the testing of strategic hypotheses without exposure to real risks (Saha, Gupta, Rao, 2026).

In this context, predictive analytics supports the development of a proactive approach, in which decisions are adapted anticipatory of expected developments. Artificial intelligence-based models allow the assessment of adversary behaviour and the impact of strategic options, contributing to improving the quality of decisions and situational awareness (Kase et al., 2022; Lemieux, Abouzeid, 2026). The integration of these capabilities into information systems leads to the development of intelligent decision-making support systems, capable of recommending optimal actions based on advanced analytical models, such as deep learning or Bayesian models (Kumar et al., 2026; Pfaff, Hickey, 2025).

Simulation models allow for the probabilistic assessment of different courses of action and the development of robust planning mechanisms capable of integrating uncertainty and optimizing responses in dynamic environments.

In this context, the role of the human factor is redefined, with the decision-maker having the function of validating and interpreting the results generated by intelligent systems, in a framework of human-machine collaboration (Kase et al. ib.). Thus, information systems evolve from monitoring tools to anticipatory strategic support platforms, contributing to reducing uncertainty and optimizing the decision-making process in environments characterized by complexity and dynamism.

DIGITAL RECONFIGURATION OF THE NATIONAL DEFENCE INDUSTRY

The national defence industry in the case of Romania is facing a series of persistent structural dysfunctions. They derive not only from underfunding or lack of investment, but especially from the absence of an integrated information framework that allows for the efficient

coordination of the actors involved and the alignment of strategic objectives with existing capabilities.

The institutional fragmentation between the Ministry of National Defence, the Ministry of Economy, the industrial and academic environments generate systemic blockages, in the absence of a common digital planning and communication mechanism. Each actor operates on the basis of distinct data sets, without interoperability, which leads to decision-making incoherence and the inability to develop integrated procurement and innovation programs.

The digital reconfiguration of the defence industry involves the adoption of an integrated information platform model, designed as a central hub for the aggregation, analysis and distribution of strategic data. This type of digital architecture allows the synchronization of actors in the defence ecosystem (public institutions, industry, research centres), reducing information fragmentation and increasing the ability to respond to dynamic operational requirements (Galdino, Pellanda, 2026).

The digital reconfiguration of the defence industry involves the adoption of an integrated information platform model, designed as a central hub for the aggregation, analysis and distribution of strategic data.

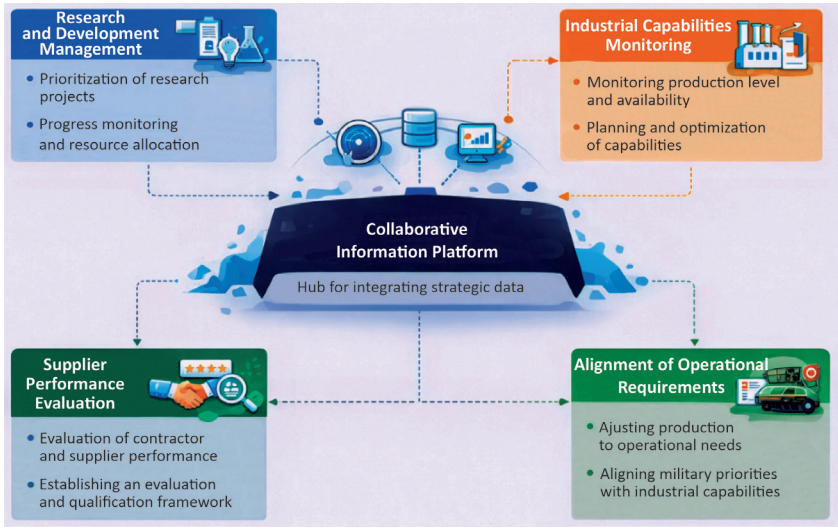

Figure 2: Digital reconfiguration of the national defence industry

Recent literature highlights that the digitalization of the defence industry is not limited to process automation, but involves a systemic reconfiguration of data flows and decision-making mechanisms, in which digital platforms become critical infrastructures for innovation

and production management (Öztürk, Sîr, 2024; Kim, 2025). In this sense, a collaborative platform must integrate several interdependent functional modules.

A module dedicated to the management of research and development (R&D) activities must be designed in such a way as to ensure integrated monitoring of the entire innovation cycle, coherently covering the stages from the early phase of conception (front-end of innovation) to the final phases of implementation and production, under conditions of complete traceability of decisions and intermediate results. The specialized literature highlights that the efficiency of innovative processes in the defence sector is deeply conditioned by the early integration of relevant actors and the use of advanced digital decision support systems, capable of correlating heterogeneous data and supporting complex evaluation and selection processes (Girardi et al., 2024; Galdino, Pellanda, 2026). The information platform should facilitate, in a systemic and data-driven manner, the prioritization of research and development projects according to strategic relevance, risk level and estimated operational impact, thus contributing to the optimization of the investment portfolio. At the same time, it would allow the dynamic allocation of resources in real time, by integrating information on the availability of technological, financial and human capabilities, which would lead to increased efficiency in their use and reduced operational bottlenecks. The platform would also support inter-institutional collaboration within the triple helix model (state – industry – academia), fostering knowledge exchange, co-creation of innovative solutions and synchronization of strategic objectives between the actors involved. Therefore, the implementation of such integrated digital mechanisms becomes essential for accelerating innovation cycles and for reducing the gap between technological development and its application in the operational environment, contributing to increasing the adaptive capacity and consolidating the strategic advantage (Turnip, Kristian, 2026).

The information platform should facilitate, in a systemic and data-driven manner, the prioritization of research and development projects according to strategic relevance, risk level and estimated operational impact, thus contributing to the optimization of the investment portfolio.

Another essential module of the information platform is the one aimed at ensuring the visibility and integrated assessment of existing industrial capacities, since, in the current context marked by geopolitical instability, disruptions of supply chains and intensified strategic competition, industrial resilience becomes a critical component

of national security and strategic autonomy (Gunnarsson, 2025). In this sense, recent literature highlights the role of digitalization in creating systems capable of providing a coherent and up-to-date picture of industrial infrastructure and its performance, thus facilitating strategic planning and adaptation processes (Hu et al., 2026; Li et al., 2026).

Operationally, the platform would allow for detailed mapping of production capacities, by integrating data on industrial infrastructure, resource utilization and technological capabilities, contributing to a systemic understanding of the available industrial potential. At the same time, it would facilitate the identification of bottlenecks and vulnerabilities in supply chains, by analysing the interdependencies between suppliers, processes and critical resources, an essential aspect in the context of increasing risks associated with logistical discontinuities and external disruptions (Samuels, 2025; Plevnik, Rupnik, 2026). In addition, the use of advanced modelling tools would allow the simulation of production scenarios, including through digital twin technologies, offering the possibility of assessing the impact of different strategic decisions on industrial performance and system resilience (Albanna, 2023; Li et al., 2026).

Operationally, the platform would allow for detailed mapping of production capacities, by integrating data on industrial infrastructure, resource utilization and technological capabilities, contributing to a systemic understanding of the available industrial potential.

In line with these directions, recent strategic documents emphasize that the digitalization of industrial processes and supply chains is an essential condition for the development of a *"resilient and adaptive"* defence ecosystem, capable of responding rapidly to changes in the operational environment and supporting military modernization efforts (Hicks, 2023). Thus, the integration of these functionalities into a unified digital platform contributes not only to increasing operational efficiency, but also to strengthening the anticipation and reaction capacity of the entire defence industrial system.

One of the major structural advantages of an integrated information platform lies in its ability to dynamically correlate operational requirements of the armed forces with the available industrial capacities, thus contributing to significantly reducing the latency between identifying needs and delivering the appropriate technological solutions. In the absence of effective alignment mechanisms, the literature highlights the emergence of systemic failures, manifested by production delays, inefficient use of resources and the inability

of industry to promptly respond to emerging requirements of the operational environment (Wasser, Sheers, 2025; Mariscal, Cornish, 2025).

Within this framework, the digital platform should ensure, first of all, the full traceability of operational requirements by integrating them into standardised digital flows, allowing them to be tracked throughout the decision-making and production chain. Secondly, the system would facilitate the rapid adaptation of production by using real-time data and flexible production mechanisms specific to the Industry 4.0 paradigm, allowing industrial capacities to be adjusted according to evolving requirements and strategic context (Kaur, 2025). Thirdly, the platform would contribute to the optimisation of the product portfolio by continuously linking operational demand with industrial supply, reducing redundancies and targeting investments towards solutions with high strategic relevance. This integration logic is supported by the emerging transition trend from traditional *"project-driven"* models, characterized by rigidity and long development cycles, to *"product-driven"* models, which privilege product modularity, reuse and adaptability in relation to dynamic end-user requirements (Sundell, 2025). In this context, the continuous alignment between requirements and production becomes a determinant of industrial performance and operational efficiency.

Advanced information systems can facilitate the identification of these opportunities through integrated analysis of data from the economic, academic and technological environment, thus contributing to accelerating innovation and expanding the industrial defence base.

A central element of this transformation is the integration of the concept of dual-use technologies, which allows the exploitation of synergies between the civil and military sectors, through the two-way transfer of innovation, knowledge and technological capabilities. Advanced information systems can facilitate the identification of these opportunities through integrated analysis of data from the economic, academic and technological environment, thus contributing to accelerating innovation and expanding the industrial defence base (Parikh, 2025; Smiljanic et al., 2025). Overall, the collaborative information platform is shaping up as the core of the digital transformation of the defence industry, as it enables the integration of data flows, the coordination of institutional and industrial actors and the optimization of decision-making processes at strategic level. By modularising functionalities – from R&D management and industrial capacity monitoring to supplier evaluation and correlation

of operational requirements –, it becomes an essential tool to increase the efficiency, resilience and competitiveness of the defence ecosystem in the context of contemporary challenges.

In addition, the use of big data and artificial intelligence technologies can radically transform the way defence investments are planned. By analysing large volumes of data, it is possible to identify technological trends, assess risks and optimise the allocation of resources. Thus, the defence industry can move from a reactive model to a proactive one, oriented towards anticipation and innovation.

The use of big data and artificial intelligence technologies can radically transform the way defence investments are planned. By analysing large volumes of data, it is possible to identify technological trends, assess risks and optimise the allocation of resources.

The digitalization of the defence industry is not only a technological process, but also a strategic one, which involves redefining the relationship between the state and its industrial infrastructure. By creating an integrated information ecosystem, Romania can develop autonomous capabilities and reduce dependence on external suppliers.

BIBLIOGRAPHICAL REFERENCES:

1. Adha, R.I., Mardamsyah, A. et al. (2026). *Big data analytics framework for defense strategic intelligence and decision support systems,* in *Journal of Defense Technology and Engineering*.
2. Dragomir, F. (2017). *Aspects of the information security model*. National, European and Euro-Atlantic Security scientific communication session, no. 3, pp. 184-190.
3. Dragomir, F.-L. (2024). *The potential for intensifying Austria's opposition to Schengen enlargement*, in *European Journal of Accounting, Finance & Business,* 12(2), pp. 120-128. ISSN 2344-102X Issue 2/June 2024 ISSN-L 2344-102X DOI: 10.4316/EJAFB.2024.
4. Dragomir, F.-L. (2025a). *Algorithmic Transparency in Information Systems: A Legal Necessity for the Protection of Fundamental Rights*. *Acta Universitatis Danubius. Juridica,* 21(1), pp. 126-136.
5. Dragomir, F-L. (2025b). *How information systems are reshaping national security strategies*, in *Romanian Military Thinking*, 1(1), pp. 202-213. Defence Staff.
6. Dragomir, F.-L. (2025c). *Integrating artificial intelligence into operational research – New horizons for national security,* in *Romanian Military Thinking,* 1(1), pp. 174-187. Defence Staff.
7. Dragomir-Constantin, F.-L. (2025d). *Modeling Fiscal Pressure for Economic Resilience: An Intelligent Information System Approach Based an J48 Tree*. *Acta Universitatis Danubius. Œconomica*, 21(3). University Danubius Press.

8. Dragomir, F-L. (2025e). *Multilevel architecture of information systems for monitoring radicalization trends in digital environments*, in *Romanian Military Thinking*, 1(2). Defence Staff.
9. Dragomir, F.-L. (2025f). *Confidentiality, Loyalty, and Responsibility: The Ethical Triad in Information Systems Management in the Field of National Security*. *Bulletin of "Carol I",* National Defence University, 14(2), pp. 296-310. El Ghamari, M. (2025). *Strategic Thinking: Geopolitical Rivalry in the Middle East*. Wojsko Polskie.
10. Dragomir, F.-L., Alexandrescu, G., Postolache, F. (2018). *Tools for Hierarchical Security Modeling*, The 14th International Scientific Conference eLearning & Software for Education Bucharest: "Carol I" National Defence University, 4(10.12753/2066-026X-18-219), pp. 34-38.
11. Dragomir, F.-L., Enache, R. (2025). *Information Systems in the Analysis of Ideological Terrorism Modeling: the Interaction between Attacks, Arrests and Convictions in Europe (2017-2022)*, in *Romanian Military Thinking*, 1(2). Defence Staff.
12. Dragomir-Constantin, F.-L., Beldiman, C.M., Zlati, M.L. (2025). *Informational Approaches in Modelling Social and Economic Relations: Study on Migration and Access to Services in the European Union*. *Systems*, 13(6), 469. MDPI.
13. Galdino, J.F., Pellanda, P.C. (2026). *Decision support systems in defense innovation management. Public Administration Journal*.
14. Girardi, R., Galdino, J.F., Pellanda, P. C. (2024). *The front end of innovation in defense: A comprehensive literature review*. In *IntechOpen*.
15. Hicks, K.H. (2023). *National defense industrial strategy*. U.S. Department of Defense.
16. Hurochkina, V., Bondarenko, S. (2025). *The implementation of artificial intelligence technologies in the military domain: Opportunities and risks*. In *Proceedings of the International Conference* (IEEE).
17. Jafari, M., Akhavan, P., Akbari, A.H. (2026). *Enhancing supply chain agility and performance through big data analytics: The role of digitalization and top management support*. *International Journal of Productivity and Performance Management*.
18. Jimoh, O.I., Adejobi, A.O. (2026). *Artificial intelligence and the future of knowledge preservation: Implications for national security and strategic decision-making*, in *Journal of Artificial Intelligence*.
19. Kase, S.E., Hung, C.P., Krayzman, T., Hare, J.Z. (2022). *The future of collaborative human-artificial intelligence decision-making for mission planning*, in *Frontiers in Psychology, 13,* 850628.

20. Kazak, O., Ptashchenko, O., Zyma, O. et al. (2025). *Digital transformation in logistics: Driving sustainable growth in international commerce*, in *European Journal of Sustainable Development*.
21. Kim, J.E. (2025). *Digital transformation of Poland's defense industry*, in *SSRN Electronic Journal*.
22. Korkmaz, G. (2024). *Supply chain risks and management strategies in the defense industry*, in *Journal of Defense Resources Management*.
23. Koval, V. (2026). *Strategic priorities of the defense-industrial complex*, in *Public Administration and Economics Review*.
24. Kumar, S., Pandey, A.K., Singh, A.K., Kaiwartya, O. (2026). *Artificial intelligence and machine learning integration with IoT for enhanced defence applications*, in *Emerald Publishing*.
25. Lee, C.E., Baek, J., Son, J., Ha, Y.G. (2023). *Deep AI military staff: Cooperative battlefield situation awareness for commander's decision making*, in *The Journal of Supercomputing, 79,* pp. 1-23.
26. Lemieux, F., Abouzeid, S. (2026). *Artificial intelligence and intelligence analysis*.
27. Li, P., Zhang, L. (2025). *Application of big data technology in enterprise information security management*. *Scientific Reports, 15*, Article 85403.
28. Onwujekwe, G., Weistroffer, H.R. (2025). *Intelligent decision support systems: An analysis of the literature and a framework for development*. *Information Systems Frontiers*.
29. Pfaff, C.A., Hickey, C.J. (2025). *Integrating artificial intelligence and machine learning technologies into common operating picture and course of action development*. U.S. Army War College Press.
30. Rane, N.L., Chika, O.E., Rane, J. (2026). *Business intelligence systems integrating artificial intelligence, big data analytics, machine learning, internet of things, and blockchain*, in *International Journal of Applied Research in Science*.
31. Ruther, P., Strohal, M., Stütz, P. (2023). *A situation analysis process in computer-generated forces team behavior within air combat simulations under risk and uncertainty*, in *Springer Proceedings*.
32. Saha, B., Gupta, G., Rao, D.V. (2026). *A big data analytics architecture for tactical control station of full mission combat simulators*, in *Defence Science Journal*.
33. Sarkar, P., Gunasekaran, A., Patil, H.K. (2025). *Survivability of supply chains in the era of Industry 4.0*, in *Global Journal of Flexible Systems Management*.
34. Muhammad S., Shengzhong Z., Hassan, A., Muhammad, S.A. Leveraging blockchain for sustainable supply chains: a qualitative approach for achieving the United Nations Sustainable Development

Goals, in *International Journal of Logistics Research and Applications* 0:0, pp. 1-35.
35. Su, Z. (2026). *Digital transformation in port logistics*. *Encyclopedia, 6(1)*, 28.
36. Sundell, M. (2025). *Product development in the defence industry. Transitioning from project-driven to product-driven development*, *Aalto University Repository*.