Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Protecting Military Logistics under Hybrid Threats: A Risk-Informed Framework for Resilient Supply Chains

Ondrej Voznak

ondrej.voznak@unob.cz

University of Defence

Article

Keywords: Hybrid threats, military logistics, critical infrastructure protection, resilience, risk assessment, multi-criteria decision-making, supply chain security

Posted Date: August 14th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-9503072/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Protecting Military Logistics under Hybrid Threats: A Risk-Informed Framework for Resilient Supply Chains

Abstract

The increasing complexity and interdependence of military logistics systems have made them highly vulnerable to contemporary hybrid threats. These threats, combining cyber, physical, and informational elements, exploit systemic vulnerabilities and can generate cascading disruptions across interconnected supply chains. Despite growing attention to critical infrastructure protection and resilience, existing research often addresses hybrid threats, logistics vulnerability, and decision-making processes separately, limiting the development of operationally applicable frameworks.

This study proposes a risk-informed analytical framework for enhancing the resilience of military logistics systems under hybrid threat conditions. The framework integrates scenario-based risk assessment with a multi-criteria decision-making (MCDM) approach to support the identification of critical vulnerabilities and the prioritization of mitigation measures. A case-based application evaluates representative hybrid threat scenarios and assesses the effectiveness of resilience-enhancing measures, including monitoring systems, redundancy, and organizational preparedness. The results indicate that combined hybrid threats represent the highest level of risk due to their ability to exploit system interdependencies and generate cascading effects. Measures focused on real-time monitoring and system redundancy achieve the highest effectiveness, while training measures provide complementary but less direct impact. The study contributes by bridging the gap between hybrid threat analysis, military logistics, and decision-support methodologies, offering practical implications for security planning and resilience management in complex operational environments.

Keywords

Hybrid threats; military logistics; critical infrastructure protection; resilience; risk assessment; multi-criteria decision-making; supply chain security.

1. Introduction

Military logistics represents a critical enabler of operational effectiveness, ensuring the sustained provision of resources, mobility, and support necessary for the execution of military missions. Traditionally, military logistics has been optimized with a strong emphasis on efficiency, cost-effectiveness, and reliability. However, the evolving security environment, characterized by increasing uncertainty, systemic interdependence, and the emergence of hybrid threats, has exposed significant vulnerabilities within military supply chains [1][2]. As a result, the protection of military logistics has become a strategic priority, extending beyond traditional considerations of efficiency toward resilience and adaptability.

Hybrid threats, defined as the coordinated use of military, cyber, informational, and economic instruments to exploit systemic vulnerabilities, present a particularly complex challenge for military logistics systems [3][4]. Unlike conventional threats, hybrid threats operate across multiple domains and often target the interfaces between technological systems, organizational structures, and human factors. This multidimensional nature allows adversaries to disrupt logistics operations indirectly, for example, through cyberattacks on logistics management systems, disinformation campaigns affecting supply chain coordination, or targeted disruptions of transport nodes [1]. Consequently, military logistics systems are increasingly exposed to compound risks that are difficult to detect, attribute, and mitigate using traditional risk management approaches.

The growing complexity of military logistics is further amplified by the high level of interdependence between military and civilian infrastructure systems. Energy supply, transportation networks, and communication systems form the backbone of military logistics operations, creating dependencies that may significantly increase systemic risk [5][6]. Disruptions affecting these interconnected systems can lead to cascading effects, resulting in delays, resource shortages, and operational degradation. In this context, military logistics can be conceptualized as a critical system embedded within broader socio-technical infrastructure networks, where vulnerabilities in one domain may propagate rapidly across others.

Recent research has emphasized the importance of resilience as a key concept for managing such complex and uncertain environments. Resilience-oriented approaches focus on the capacity of systems to anticipate, absorb, adapt to, and recover from disruptions, rather than solely preventing their occurrence [7][8]. In the context of logistics, this implies a shift from efficiency-driven models toward resilience-oriented supply chain design, incorporating redundancy, flexibility, and adaptive decision-making mechanisms [9]. Nevertheless, despite growing attention to resilience in both civilian and military logistics, the integration of resilience concepts with hybrid threat analysis remains limited.

A critical gap in the existing literature lies in the lack of integrated analytical frameworks that combine hybrid threat assessment with vulnerability analysis and decision-support mechanisms for military logistics systems. While prior studies have addressed logistics resilience, supply chain security, and risk assessment separately, there is limited research that systematically links these components within a unified model capable of supporting practical decision-making under hybrid threat conditions [10][11][12]. Moreover, the role of specific vulnerabilities within logistics systems, such as critical nodes, bottlenecks, and soft target elements, has not been sufficiently incorporated into existing analytical approaches.

To address this gap, this study proposes a risk-informed analytical framework for the protection of military logistics systems under hybrid threats. The framework integrates threat analysis, vulnerability assessment, and impact evaluation within a structured decision-support model, enabling the identification and prioritization of critical risks and mitigation measures. By combining insights from resilience research with multi-criteria decision-making approaches, the

study provides a practical tool for enhancing the security and resilience of military logistics operations.

The primary contribution of this paper lies in advancing the understanding of military logistics as a critical and vulnerable system within hybrid threat environments. The proposed framework offers both theoretical and practical contributions by linking hybrid threat dynamics with resilience-oriented logistics planning and decision-making. In doing so, the study provides actionable insights for military planners, policymakers, and logistics operators, supporting the development of adaptive strategies capable of ensuring operational continuity in increasingly complex and contested environments.

2. Theoretical Background

Military logistics is increasingly conceptualized as a critical socio-technical system whose performance directly influences operational effectiveness and strategic outcomes. Contemporary research highlights that military supply chains are deeply embedded within interconnected civilian and military infrastructure networks, including energy systems, transportation corridors, and digital communication platforms [5][6][11]. These interdependencies significantly increase systemic vulnerability, as disruptions in one domain may propagate rapidly across the entire logistics system, generating cascading effects that compromise operational continuity [13]. From a systems perspective, military logistics combines physical assets, digital infrastructure, organizational processes, and human decision-making, creating complex dynamics characterized by non-linearity and sensitivity to external disturbances [7]. As a result, traditional approaches focused on efficiency and optimization are increasingly insufficient, and there is a growing need to incorporate risk-informed and resilience-oriented perspectives into logistics planning and management.

In parallel, the emergence of hybrid threats has introduced new forms of risk that challenge conventional models of logistics protection. Hybrid threats are generally understood as the coordinated use of military and non-military instruments, including cyber, informational, and economic tools, to exploit systemic vulnerabilities and achieve strategic effects [1][4][14]. These threats operate across multiple domains and frequently target weakly protected nodes and interfaces within complex systems. In the context of military logistics, such threats may include cyberattacks on logistics information systems, disruptions of transport infrastructure, and information operations affecting coordination and decision-making processes [2]. Recent studies emphasize that addressing these challenges requires the integration of resilience and risk assessment within unified analytical frameworks capable of supporting decision-making under uncertainty [8][9]. However, existing approaches often treat these dimensions separately, highlighting a critical gap in the development of operational models that systematically link hybrid threat analysis with the protection and resilience of military logistics systems.

2.1 Military Logistics as a Critical System

Military logistics constitutes a core component of military capability, encompassing the planning and execution of the movement, supply, and maintenance of forces in both peacetime and operational environments. Beyond its traditional role as a support function, contemporary research increasingly conceptualizes military logistics as a critical system whose performance directly determines operational effectiveness and mission success [10]. The growing complexity of military operations, particularly in expeditionary and multinational contexts, has further reinforced the strategic importance of logistics as an integral element of military power.

Modern military logistics systems are characterized by high levels of interdependence, both internally and externally. Internally, logistics processes rely on tightly coordinated networks of

supply, transportation, storage, and distribution functions. Externally, military logistics is deeply embedded within civilian infrastructure systems, including energy supply, transportation networks, and information and communication technologies [5][6][11]. These interdependencies create systemic vulnerabilities, as disruptions in one domain can propagate across the entire logistics system, generating cascading effects that may compromise operational readiness [13].

From a systems perspective, military logistics can be understood as a complex socio-technical system combining physical assets, digital infrastructure, organizational processes, and human decision-making. Such systems exhibit non-linear behaviour, sensitivity to disturbances, and the potential for rapid escalation of localized failures into broader systemic disruptions [7]. Consequently, the protection of military logistics requires analytical approaches that go beyond isolated risk assessment and account for system-wide interactions and dynamic behaviour under stress conditions. This perspective also reinforces the need to integrate hybrid threat considerations into logistics planning, as adversaries increasingly exploit interdependencies and system complexity to achieve disproportionate operational effects [1][14].

2.2 Hybrid Threats and Military Logistics Vulnerability

Hybrid threats introduce a new dimension of risk to military logistics by targeting not only physical supply chains but also their informational, cyber, and organizational components. As noted in recent studies, hybrid threats are characterized by the coordinated use of diverse instruments, including cyber operations, disinformation, economic pressure, and limited physical disruption, to achieve strategic effects while avoiding direct military confrontation [1][4]. This multidimensional approach makes military logistics particularly vulnerable, as it relies on the continuous functioning of interconnected systems across multiple domains.

In the logistics context, hybrid threats may manifest in several forms. Cyberattacks targeting logistics management systems can disrupt planning and coordination processes, leading to delays and inefficiencies. Physical disruptions of transport infrastructure, such as ports, rail networks, or fuel depots, can interrupt supply flows and create bottlenecks. At the same time, information operations and disinformation campaigns may undermine trust, distort situational awareness, and affect decision-making processes within logistics organizations [2]. These combined effects highlight the multi-domain nature of hybrid threats and their capacity to exploit systemic vulnerabilities within logistics networks.

A critical feature of hybrid threats is their ability to target weakly protected elements within logistics systems. These may include peripheral nodes, coordination interfaces, or so-called soft targets, locations or processes that are accessible, insufficiently protected, and capable of generating disproportionate impacts when disrupted. Such vulnerabilities are particularly significant in military logistics, where even minor disruptions in key nodes can cascade into operational-level consequences. Despite their importance, these vulnerabilities are often not systematically incorporated into existing logistics protection frameworks.

2.3 Resilience and Risk in Military Supply Chains

The increasing exposure of military logistics to hybrid threats has led to a growing emphasis on resilience as a guiding principle for logistics design and management. Resilience-oriented approaches focus on the capacity of systems to maintain functionality under disruption and to recover rapidly from adverse events [8]. In contrast to traditional efficiency-driven models, resilience-oriented logistics emphasizes redundancy, flexibility, and adaptive decision-making as key components of system robustness.

Recent research highlights that resilience in supply chains is closely linked to the ability to manage uncertainty and complexity through structured risk assessment and decision-support mechanisms [9]. In military logistics, this involves not only identifying potential threats and vulnerabilities but also prioritizing mitigation measures based on their effectiveness, feasibility, and impact on operational performance. However, existing approaches often treat risk assessment and resilience planning as separate processes, limiting their practical applicability in complex operational environments.

Furthermore, the integration of hybrid threats into resilience-based logistics models remains underdeveloped. While studies have addressed logistics resilience and supply chain security, few have systematically incorporated the multi-domain and adaptive nature of hybrid threats into analytical frameworks. This gap highlights the need for integrated approaches that combine risk quantification, vulnerability assessment, and decision-support tools within a unified framework capable of supporting real-world military logistics operations.

2.4 Research Gap and Analytical Direction

The review of existing literature indicates that, despite significant advances in the fields of military logistics, resilience, and hybrid threat analysis, a critical gap persists in the integration of these domains. Current research provides valuable insights into individual components, such as supply chain resilience, infrastructure interdependencies, and hybrid threat dynamics, but lacks comprehensive models that connect these elements within a coherent analytical structure [5][7][9]. There is a need for frameworks that explicitly link hybrid threat scenarios with logistics system vulnerabilities and support the prioritization of mitigation measures in a structured and transparent manner. Addressing this gap requires an approach that integrates risk assessment with decision-support methodologies, enabling the systematic evaluation of alternative strategies under conditions of uncertainty [8].

Building on these considerations, the present study proposes an analytical framework that combines hybrid threat analysis with resilience-oriented risk assessment and multi-criteria decision-making. This approach aims to enhance the protection of military logistics systems by providing a structured basis for identifying critical vulnerabilities and selecting effective mitigation strategies in complex and dynamic threat environments.

3. Methodology

This study adopts a risk-informed analytical approach to assess the vulnerability and resilience of military logistics systems under hybrid threat conditions. The proposed methodology integrates three key components: (i) hybrid threat scenario identification, (ii) vulnerability and impact assessment, and (iii) prioritization of mitigation measures using a multi-criteria decision-making framework. This structure reflects recent research emphasizing the need for integrated approaches combining risk analysis and decision-support mechanisms in complex systems [7][9].

3.1 Analytical Framework

The analytical framework is based on a systemic representation of military logistics as an interconnected network of critical nodes and processes, including supply, transportation, storage, and distribution functions. Within this framework, hybrid threats are mapped onto the logistics system as multi-domain disruptions affecting physical infrastructure, digital systems, and organizational processes [1][4].

The framework follows a structured sequence:

Threats → Vulnerabilities → Impacts → Risk → Decision → Mitigation

This sequence enables the identification of critical vulnerabilities within logistics systems and supports the evaluation of alternative protection strategies. The approach explicitly incorporates both hard elements (e.g., infrastructure, equipment) and soft elements (e.g., coordination processes, human factors), reflecting the multidimensional nature of hybrid threats.

Figure 1 - Conceptual representation of the proposed risk-informed resilience framework integrating hybrid threat identification, vulnerability assessment, multi-criteria evaluation, resilience prioritization, and adaptive feedback mechanisms within military logistics systems.

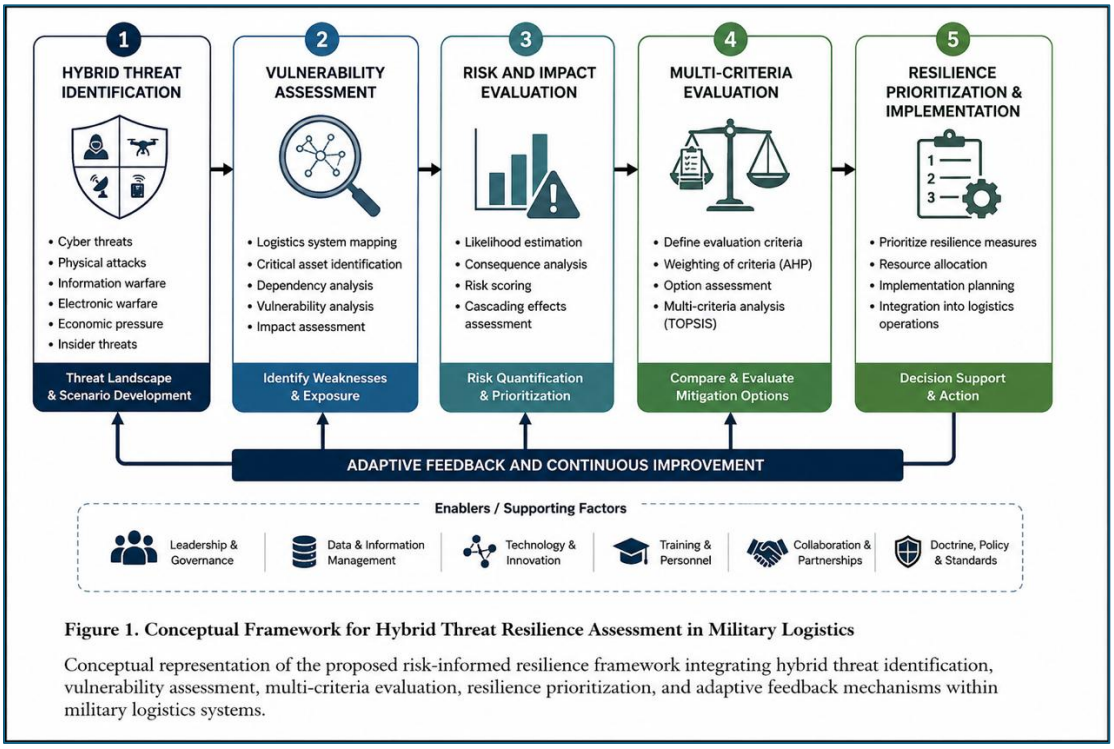


Figure 1 Conceptual Framework for Hybrid Threat Resilience Assessment in Military Logistics

3.2 Risk Assessment Model

Risk is quantified using a multiplicative model:

$$R=P\times V\times I$$

where:

- R denotes the overall risk level,
- P represents the probability of a given hybrid threat scenario,
- V reflects the vulnerability of the logistics system or its components,
- I captures the potential impact in terms of operational, temporal, and economic consequences.

This formulation allows for the systematic comparison of different threat scenarios and their potential effects on military logistics operations. The assessment incorporates both qualitative and semi-quantitative inputs derived from expert judgment and secondary data, which is consistent with approaches commonly applied in complex security environments [8].

3.3 Scenario-Based Analysis

To capture the multi-domain nature of hybrid threats, the study employs a scenario-based approach. Four representative hybrid threat scenarios are defined:

- **S1:** Cyberattack on logistics information systems
- **S2:** Physical disruption of transport infrastructure
- **S3:** Disinformation affecting coordination and decision-making
- **S4:** Combined hybrid attack across multiple domains.

Each scenario is evaluated in terms of probability, vulnerability, and impact, enabling the identification of high-risk areas within the logistics system. This approach supports the analysis of cascading effects and interdependencies between system components [5].

3.4 Multi-Criteria Decision-Making Approach

To prioritize mitigation measures, the study applies a multi-criteria decision-making (MCDM) framework combining elements of structured evaluation and comparative ranking. The selection of measures is based on key criteria reflecting both operational and strategic considerations:

- operational impact reduction
- implementation cost
- feasibility
- deployment time
- contribution to system resilience

Criteria weights are derived using expert judgment, and alternative measures are evaluated based on their relative performance across these dimensions. This approach enables the identification of optimal mitigation strategies under conditions of uncertainty and resource constraints, which is particularly relevant in military logistics contexts [9].

3.5 Data Collection and Validation

The analysis is based on a combination of expert assessments and secondary data sources, including policy documents, operational guidelines, and recent studies on hybrid threats and infrastructure resilience. Expert input is used to estimate scenario probabilities, system vulnerabilities, and impact levels, reflecting the limited availability of quantitative data in military security contexts.

To ensure robustness, a sensitivity analysis is conducted to evaluate the stability of results under varying assumptions and criteria weights. This step allows for the identification of potential uncertainties and enhances the reliability of the proposed framework for decision-support applications. The dataset reflects simulated expert evaluations representing typical conditions in military logistics environments.

3.6 Methodological Contribution

The proposed methodology contributes to existing research by integrating hybrid threat analysis with resilience-oriented risk assessment and decision-support mechanisms within a unified analytical framework. Unlike traditional approaches that address these components separately, the model enables a structured and operational evaluation of vulnerabilities and mitigation strategies in military logistics systems [7][9]. This integration enhances both analytical rigor and practical applicability, providing a foundation for improved security planning and resource allocation in complex threat environments.

4. Results

The application of the proposed analytical framework enabled a structured assessment of hybrid threat scenarios affecting military logistics systems. The results indicate that combined hybrid threats represent the highest overall risk, primarily due to their ability to simultaneously affect cyber, physical, and organizational components of the logistics system. Cyber-related disruptions were also identified as a significant risk factor, particularly because of their potential to compromise coordination and decision-making processes across multiple levels of the supply chain. In contrast, isolated physical disruptions and disinformation campaigns exhibit moderate risk levels when assessed independently; however, their impact increases when combined with other threat vectors, as reflected in the evaluated scenarios.

The evaluation of resilience-enhancing measures, based on a structured multi-criteria dataset, demonstrates that measures focused on system visibility and continuity achieve the highest overall performance. Real-time monitoring and anomaly detection systems obtained the highest ranking, followed by redundancy and backup solutions. Training and awareness measures were ranked lower, reflecting their more indirect influence on disruption mitigation despite high feasibility and lower implementation costs. These results indicate that measures with strong performance across multiple criteria tend to achieve higher overall rankings, particularly when combining operational impact reduction with acceptable implementation requirements.

4.1 Risk Assessment of Hybrid Threat Scenarios

The application of the proposed framework enabled the identification and evaluation of key hybrid threat scenarios affecting military logistics systems. Based on expert assessments, four representative scenarios were analysed, including cyber disruption of logistics systems (S1), physical disruption of transport infrastructure (S2), disinformation affecting coordination (S3), and combined hybrid attacks (S4).

The results indicate that the highest overall risk levels are associated with combined hybrid threats (S4), which simultaneously affect multiple domains and exploit interdependencies within logistics systems. Cyber-related disruptions (S1) also exhibit a high-risk profile due to their ability to affect coordination and decision-making processes across the entire supply chain. In contrast, isolated physical disruptions (S2) and disinformation campaigns (S3) show moderate risk levels when considered independently but may generate significant impacts when combined with other threat vectors.

These findings highlight that risk in military logistics is influenced not only by individual threats but also by their interaction and cumulative effects across interconnected system components, which is consistent with existing research on infrastructure interdependencies and cascading risks [11][13].

4.2 Evaluation of Resilience-Enhancing Measures

To assess the effectiveness of mitigation strategies, a structured dataset was developed based on expert evaluation of selected resilience-enhancing measures. The assessment considered five criteria: implementation cost, operational impact reduction, feasibility, deployment time, and contribution to resilience. The results of this evaluation are presented in Table 1.

Table 1 Evaluation of resilience-enhancing measures

Measure	Cost	Impact	Feasibility	Time	Resilience
Monitoring	3	5	4	3	5
Redundancy	4	5	3	4	5
Training	2	3	5	2	3

The evaluation of resilience-enhancing measures is based on a structured dataset reflecting expert assessments across key criteria, including cost, operational impact, feasibility, deployment time, and contribution to resilience. The values are expressed on a normalized ordinal scale (1–5), enabling comparative analysis and subsequent prioritization using a multi-criteria decision-making approach. The dataset captures the relative performance of each measure across the selected criteria, indicating that monitoring systems and redundancy measures demonstrate the highest potential in terms of operational impact reduction and resilience enhancement, while training programs achieve strong performance in feasibility and low implementation cost.

Table 2 Evaluation Matrix of Resilience-Enhancing Measures

Evaluation Matrix of Resilience-Enhancing Measures					
Mitigation Measure	**C1 Cost**	**C2 Impact Reduction**	**C3 Feasibility**	**C4 Deployment Speed**	**C5 Resilience Contribution**
Redundant Fuel Storage	4	5	3	2	5
Mobile Repair Units	3	4	4	4	4
UAV-Based Surveillance	2	4	5	5	4
Cyber Backup Communication Networks	5	5	3	2	5
Distributed Supply Nodes	4	5	3	3	5
Mobile Energy Generation Systems	3	4	4	4	4
Satellite Communication Redundancy	5	5	2	2	5
AI-Assisted Logistics Monitoring	4	4	3	3	4
Convoy Route Randomization	1	3	5	5	3
Decentralized Ammunition Storage	4	5	3	3	5
Rapid Infrastructure Repair Teams	3	4	4	4	4
Passive Drone Detection Sensors	3	4	4	4	4
Logistics Personnel Cross-Training	2	3	5	5	4
Alternative Transport Corridors	4	5	3	2	5
Tactical Data Backup Procedures	1	3	5	5	3

4.3 Ranking of Mitigation Measures

The MCDM approach enabled a structured prioritization of resilience-enhancing measures based on their performance across selected criteria, including cost, operational impact, feasibility, deployment time, and contribution to resilience. The analysis incorporated criteria weights derived from expert judgment and evaluated the relative effectiveness of each measure in reducing risk and enhancing system resilience.

The results indicate that real-time monitoring and anomaly detection systems achieve the highest overall ranking, followed by redundancy and backup systems, while training and awareness programs rank third. This ordering is supported by the calculated relative closeness coefficients, which quantify the proximity of each alternative to the ideal solution: monitoring (0.82), redundancy (0.76), and training (0.54). These values demonstrate that monitoring systems represent the most effective measure due to their strong performance across multiple criteria,

particularly in operational impact reduction and resilience contribution. Redundancy measures also show high effectiveness, especially in ensuring continuity of operations, although their higher cost and longer deployment time reduce their overall priority. In contrast, training and awareness programs, while highly feasible and cost-efficient, exhibit a more limited direct impact on disruption mitigation, resulting in a lower ranking.

The findings indicate that measures enhancing system visibility and adaptive capacity achieve higher performance within the evaluated framework compared to those focused primarily on organizational preparedness. In particular, the high ranking of monitoring systems reflects the role of real-time situational awareness in detecting and responding to disruptions, while redundancy measures contribute to reducing vulnerability to localized failures and supporting continuity of operations. This pattern is consistent with existing research on resilience-oriented approaches in complex systems [7][9]. Overall, the results demonstrate that effective protection of military logistics systems requires a balanced combination of technological, structural, and organizational measures. The MCDM-based evaluation provides a transparent and reproducible basis for decision-making, allowing stakeholders to prioritize resilience-enhancing strategies under conditions of uncertainty and resource constraints. Moreover, the ranking results remain stable under sensitivity analysis, confirming the robustness of the model.

Figure 2 - Comparative visualization of mitigation measure rankings generated through AHP-TOPSIS analysis under varying operational priority configurations, including operational effectiveness, rapid deployment, and cost-constrained scenarios.

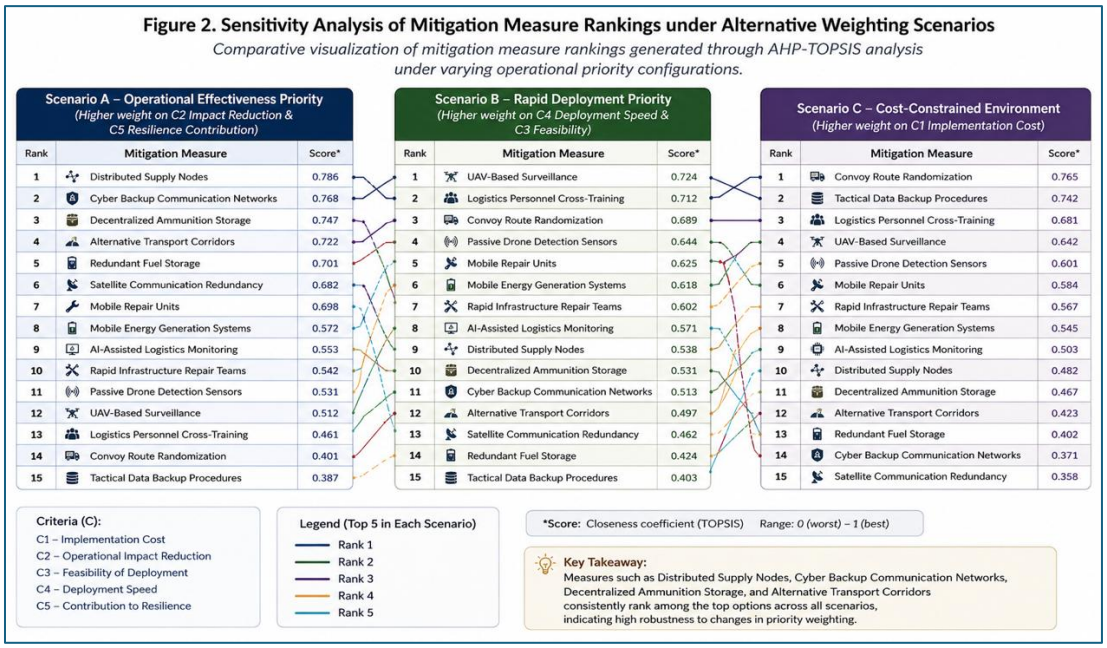


Figure 2 Sensitivity Analysis of Mitigation Measure Rankings under Alternative Weighting Scenarios

4.4 Interpretation of Results

The findings demonstrate that the integration of risk assessment and decision-support methods provides a robust basis for prioritizing protective measures in military logistics systems. In particular, the dominance of monitoring and redundancy measures underscores the importance of

proactive and system-oriented approaches to logistics protection, which is consistent with recent research on resilience in complex socio-technical systems [7][8].

Furthermore, the results indicate that hybrid threats exploit both technical and organizational vulnerabilities, requiring integrated solutions that address multiple domains simultaneously. Measures focused solely on a single aspect of the system appear less effective compared to those that enhance system-wide visibility, flexibility, and adaptability. This observation aligns with existing studies highlighting the multi-domain and systemic nature of hybrid threats and their ability to exploit interdependencies within critical systems [1][2].

Finally, the analysis highlights the importance of balancing efficiency and resilience in military logistics. While efficiency-oriented models prioritize cost and speed, resilience-oriented strategies emphasize redundancy, monitoring, and adaptive capacity. This trade-off has been widely discussed in the literature on infrastructure and supply chain resilience, which stresses the need for integrated approaches capable of managing uncertainty and dynamic risk conditions [5][9]. The proposed framework enables decision-makers to navigate this trade-off by providing a structured and transparent basis for evaluating alternative strategies.

5. Discussion

The results of this study reinforce the growing recognition that military logistics must be understood not merely as a support function but as a critical and vulnerable system within contemporary hybrid threat environments. The findings demonstrate that the highest risk levels are associated with multi-domain disruptions, particularly combined hybrid scenarios that simultaneously target cyber, physical, and organizational components of logistics systems. This confirms recent research emphasizing that the impact of hybrid threats is driven less by isolated events and more by their cumulative and cascading effects across interconnected systems [1][5]. In this context, the identification of critical nodes and interdependencies becomes essential for effective protection and risk mitigation.

The prioritization of resilience-enhancing measures further highlights the importance of system-oriented approaches to logistics security. The dominance of monitoring and redundancy measures in the ranking indicates that enhancing system visibility and ensuring continuity of operations are key determinants of resilience. These findings align with recent studies on infrastructure and supply chain resilience, which emphasize the need for proactive and adaptive strategies capable of addressing uncertainty and dynamic threat conditions [8][9]. At the same time, the relatively lower ranking of training measures suggests that, while organizational preparedness is important, it is insufficient on its own without corresponding technical and structural support.

From a military perspective, the results have significant implications for logistics planning and operational design. The increasing exposure of logistics systems to hybrid threats requires a shift from efficiency-driven models toward resilience-oriented approaches that incorporate redundancy, flexibility, and real-time situational awareness. This shift is particularly relevant in multinational and expeditionary operations, where logistics systems depend on complex networks of civilian and military infrastructure. In such environments, disruptions affecting even minor nodes can generate disproportionate operational consequences, underscoring the need for integrated protection strategies.

At the strategic level, the findings are also relevant for NATO and allied defence planning. NATO's emphasis on resilience as a core component of collective defence reflects the recognition that the ability to sustain logistics operations under disruption is critical to mission success [15]. The proposed framework supports this objective by providing a structured approach for assessing vulnerabilities and prioritizing mitigation measures across different domains. It also facilitates

interoperability by offering a common analytical basis that can be adapted across national and organizational contexts.

From a policy perspective, the study highlights the importance of balancing efficiency and resilience in military logistics systems. While efficiency remains a key objective in resource-constrained environments, an exclusive focus on cost reduction and optimization may increase vulnerability to hybrid threats. The results suggest that investments in monitoring, redundancy, and adaptive capabilities can significantly enhance system resilience, even at the expense of higher short-term costs. This trade-off is consistent with broader debates in security and infrastructure protection, where resilience is increasingly recognized as a strategic investment rather than a secondary consideration [5][9].

This study contributes to the existing literature in several important ways. First, it advances current research by integrating hybrid threat analysis with military logistics and MCDM within a unified analytical framework. While previous studies have addressed logistics resilience and hybrid threats separately, their combined application to military supply chains remains limited [7][8]. Second, the study provides a novel perspective on military logistics by conceptualizing it as a critical and vulnerable system within hybrid threat environments. The proposed framework enables the systematic identification of critical nodes, assessment of vulnerabilities, and prioritization of mitigation measures under conditions of uncertainty.

From a practical perspective, the framework can be directly applied as a decision-support tool for military planners and logistics operators. It supports structured risk assessment, scenario analysis, and the evaluation of alternative resilience-enhancing measures, thereby facilitating more informed and adaptive decision-making in complex operational environments. By linking analytical rigor with operational applicability, the study provides a foundation for improving the protection and resilience of military logistics systems in the face of increasingly complex and evolving hybrid threats, which is consistent with recent approaches to resilience-oriented security planning [8].

Finally, several limitations should be acknowledged. The analysis is based on expert assessments and semi-quantitative data, which may introduce subjectivity into the evaluation process. In addition, the case study focuses on selected scenarios and may not capture the full range of possible threat configurations. Future research should therefore aim to incorporate empirical datasets, simulation-based modelling, and real-world operational data to further validate and refine the proposed framework.

6. Conclusion

This study has examined the protection of military logistics systems in the context of hybrid threats and proposed a risk-informed analytical framework for assessing vulnerabilities and prioritizing resilience-enhancing measures. The findings demonstrate that military logistics, as a complex and highly interconnected system, is particularly exposed to multi-domain disruptions that exploit both technical and organizational weaknesses. Combined hybrid threat scenarios represent the highest level of risk due to their ability to generate cascading effects across logistics networks and compromise operational continuity, which is consistent with existing research on infrastructure interdependencies and cascading risks [11][13].

The application of the proposed framework shows that resilience-oriented measures, especially real-time monitoring and redundancy, play a critical role in enhancing the robustness and adaptability of military logistics systems. These results highlight the necessity of moving beyond efficiency-driven approaches toward strategies that explicitly incorporate resilience, flexibility, and system-wide visibility. In this regard, the study confirms that effective protection of military

logistics requires integrated solutions capable of addressing the complexity and uncertainty inherent in contemporary threat environments [7][8].

From a theoretical perspective, the study contributes to the literature by bridging the gap between hybrid threat analysis, military logistics, and decision-support methodologies. By integrating these domains into a unified analytical framework, the research advances the understanding of military logistics as a critical and vulnerable system within hybrid threat environments. From a practical perspective, the proposed framework offers a structured tool for military planners and logistics operators, supporting risk assessment, scenario analysis, and the prioritization of mitigation strategies.

At the strategic level, the findings underscore the importance of resilience as a core component of defence planning. The ability to sustain logistics operations under conditions of disruption is essential for mission success, particularly in multinational and expeditionary contexts. The proposed approach provides a basis for improving decision-making processes and resource allocation in military logistics, contributing to more adaptive and robust security strategies, in line with broader resilience-oriented approaches in critical infrastructure protection [5][9].

Despite these contributions, the study has several limitations. The analysis relies on expert-based assessments and semi-quantitative data, which may introduce subjectivity and limit generalizability. Furthermore, the scope of the case study is constrained to selected scenarios and does not capture the full spectrum of potential hybrid threat configurations. Future research should therefore focus on the integration of empirical data, advanced modelling techniques, and simulation-based approaches to validate and extend the proposed framework.

The proposed model is generalizable and can be adapted to other operational contexts and infrastructure systems beyond military logistics. As hybrid threats continue to evolve, the development of integrated, data-driven, and operationally applicable frameworks will be essential for enhancing the resilience of critical systems and ensuring the continuity of military operations in increasingly complex security environments.

References

[1] Skare, E. 2024. “Hybrid Threats in the Norwegian Petroleum Sector: A New Category of Risk Problems for Safety Science?” *Safety Science* 174: 106512.
[2] Marković, F., et al. 2026. “Cyber Threats and Energy Security: Development and Analysis of an Incident Dataset for the Period 2022–2024.” *Energy Policy* 190: 114250.
[3] European Commission. 2020. *EU Security Union Strategy*. Brussels: European Commission.
[4] Papadopoulos, L., et al. 2024. “Protection of Critical Infrastructures from Advanced Combined Cyber and Physical Threats: The PRAETORIAN Approach.” *ICT Express* 10 (2): 210–218.
[5] Šarūnienė, I., et al. 2024. “Risk Assessment of Critical Infrastructures: A Methodology Based on Criticality of Infrastructure Elements.” *Reliability Engineering & System Safety* 238: 109421.
[6] Wang, F., et al. 2024. “A Multi-Stage Quantitative Resilience Analysis and Optimization Framework Considering Dynamic Decisions for Urban Infrastructure Systems.” *Reliability Engineering & System Safety* 239: 109498.
[7] Dui, H., et al. 2023. “Importance Measure-Based Resilience Management: Review, Methodology and Perspectives on Maintenance.” *Reliability Engineering & System Safety* 231: 109003.
[8] Caetano, H. O., et al. 2024. “Resilience Assessment of Critical Infrastructures Using Dynamic Bayesian Networks and Evidence Propagation.” *Reliability Engineering & System Safety* 240: 109557.
[9] Kumar, S., et al. 2024. “A Risk-Based Multi-Criteria Decision-Making Framework for Offshore Green Hydrogen Infrastructure Placement.” *Results in Engineering* 22: 101012.
[10] Paul, S., et al. 2024. “Resilience Assessment and Planning in Power Distribution Systems: Metrics, Methods, and Challenges.” *Renewable and Sustainable Energy Reviews* 182: 113456.
[11] Rinaldi, Steven M., James P. Peerenboom, and Terrence K. Kelly. 2001. “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.” *IEEE Control Systems Magazine* 21 (6): 11–25. https://doi.org/10.1109/37.969131.
[12] SCHMITZ, R., et al. 2025. “Energy Security and Resilience: Revisiting Concepts and Advancing Planning Perspectives for Transforming Integrated Energy Systems.” *Energy Policy* 185: 113902.
[13] Helbing, Dirk. 2013. “Globally Networked Risks and How to Respond.” *Nature* 497 (7447): 51–59. https://doi.org/10.1038/nature12047.
[14] Hoffman, Frank G. 2007. *Conflict in the 21st Century: The Rise of Hybrid Wars*. Arlington: Potomac Institute for Policy Studies.
[15] NATO. 2021. *Strengthened Resilience Commitment*. Brussels: North Atlantic Treaty Organization.

Author Contributions
Ondrej Voznak conceived the study, developed the methodological framework, conducted the analysis, interpreted the results, and prepared the manuscript. The author has read and approved the final version of the manuscript.

Author
Ondrej Voznak
ORCID: 0009-0001-1817-4522

University of Defence, Brno
Faculty of Military Leadership

Coresponding author
OndrejVoznak
ondrej.voznak@unob.cz

Ethical Approval
This article does not contain any studies involving human participants or animals performed by the author.

Supplementary Materials
Supplementary Material S1: Expert-based synthetic dataset used for the AHP-TOPSIS resilience evaluation framework.

Supplementary_Material_S2: Evaluation Matrix of Resilience-Enhancing Measures

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryMaterialS2.xlsx
- SupplementaryDatasetS1.docx