

Enhancing the Resilience of Critical Military Supply Chains through External Threat Management

Aidas VASILIS VASILIAUSKAS^{1*}

General Jonas Žemaitis Military Academy of Lithuania, Šilo g. 5A, LT-10322 Vilnius

*Correspondence: *aidas.vasilisvasiliauskas@lka.lt*

Abstract

In recent decades, the importance of supply chain management has increased due to the frequency and severity of disruptions. The issue of supply chain resilience is widely discussed in the scientific literature. It should be noted that most studies focus on the functioning of commercial supply chains. Given the lack of a systematic approach to the specific threats and measures to ensure the resilience of military supply chains within the context of the Lithuanian Armed Forces (LAF), the objective of this article is to present the main findings of the research conducted to identify threats that are crucial for the supply chains important to the LAF and to outline measures that are taken to cope with the identified external threats.

KEY WORDS: *Supply chain, Armed forces, Supply chain resilience, Supply chain threats.*

Citation: Vasilis Vasiliauskas, A. Enhancing the Resilience of Critical Military Supply Chains through External Threat Management. In Proceedings of the Challenges to National Defence in Contemporary Geopolitical Situation, Brno, Czech Republic, 7-10 September 2026. ISSN 2538-8959, <https://doi.org/10.47459/cndcgs.2026.155>

Introduction

In recent decades, the importance of supply chain management has increased due to the frequency and severity of disruptions in global markets. Global shocks such as the COVID-19 pandemic and the military conflict in Ukraine have exposed the vulnerabilities of global supply chains and prompted a re-evaluation of risk management strategies and the strengthening of supply chain resilience. The war in Ukraine has demonstrated that supply chain resilience is critically essential for the continuity of a nation's armed forces and national security.

The issue of supply chain resilience is widely discussed in foreign scientific literature. Since 2000, hundreds of articles have been published exploring operational risks within supply chains and measures to enhance resilience while mitigating the negative impacts of both internal and external threats. A substantial body of knowledge has developed, encompassing definitions and typologies of threats, assessment methods for resilience, and strategies for supply chain recovery after disruptions. However, it is noted that most studies focus on the functioning of commercial supply chains, while the effects of armed conflicts and geopolitical threats on supply chain resilience remain under-researched. In Lithuania, the topic of risk management and resilience assurance in supply chains is still in its nascent stages. Some authors analyze the impact of the COVID-19 pandemic on global supply chains, while others examine opportunities for enhancing the resilience of small businesses' supply chains. Systematic research encompassing the concept of supply chain resilience, potential threat classification, and management measures is still lacking in Lithuania. Additionally, targeted studies related to the impact of armed conflicts and geopolitical shocks on the resilience of supply chains relevant to the national armed forces are absent. Given the lack of a systematic approach to identifying potential specific threats and exact measures to ensure the stability of military supply chains under disruption conditions, the objective of this article is to identify risks that may arise in supply chains crucial to the Lithuanian Armed Forces and to outline measures that can ensure the resilience and operational stability of these chains. To achieve this objective, the article presents a summary of scientific literature review on supply chain threat and the results of an empirical study that reveals threats pertinent to the Lithuanian Armed Forces' supply chains and their management measures.

1. Supply Chain Threats

In the context of the supply chain, a threat is understood as any potential factor or event capable of disrupting the flow of material resources, services, or information between interrelated participants in the chain. The scholarly

literature emphasizes that a threat is not identical to risk — risk arises only when a threat is able to exploit an existing vulnerability within the supply chain [13]. This distinction is particularly important when examining the enhancement of resilience in military supply chains, as it allows the precise identification of which threats may affect supply processes and, accordingly, the design of appropriate mitigation measures. In a military context, a threat can have a direct impact on operational capability and combat readiness; the identification and systematic assessment of threats is therefore an essential precondition for enhancing the resilience of military supply chains.

The identification of threats makes it possible to reveal critical dependencies among suppliers, technological components, and service providers, and to identify weak points within the system [6, 12]. Threats also reveal the networked nature of the supply chain — a breach at a single node can have a cascading effect on other participants in the chain [12]. Even a threat that has not materialized can influence strategic supply decisions, encouraging supplier diversification or the strengthening of control mechanisms, particularly under conditions of geopolitical tension [14]. Finally, the realization of a threat makes it possible to assess the actual level of supply chain resilience and its capacity to absorb and manage adverse effects [4, 9].

From a structural perspective, supply chain threats display several important characteristics. They are frequently directed not at the ultimate target but at weaker links in the supply chain, through which the core system can be reached [12]. Threats can also manifest at different stages of the chain — their source may lie at an early stage of supply, while the consequences become apparent only at the final stage of use [6]. They operate at different levels — within software, hardware, or organizational processes [21]. Some threats are latent, meaning that they may be embedded in a system as early as the development or manufacturing stage and manifest only after a certain period of time [6]. The complexity of the supply chain and the large number of participants further increase the potential for such threats to spread, since each additional link can become a potential point of compromise [7].

In the military environment, the concept of threat acquires strategic significance. Military supply chains are directly linked to operational capability, so disruptions to them can result not only in logistical or economic losses but also in reduced combat readiness or a weakening of national security [9]. Geopolitical shocks, sanctions, or the compromise of technological components can act as systemic threats that limit the availability and reliability of critical resources [14]. For this reason, in a military context a threat must be assessed not merely as a logistical disturbance but as a strategic factor capable of affecting the entire defense system.

External threats to the resilience of military supply chains arise from an environment that the organization does not directly control: geopolitical shocks, market and supplier instability, transport and infrastructure disruptions, cyberattacks carried out through suppliers, and regulatory change [7]. Such threats are particularly important in the defence sector, since even short-term supply delays can have a direct impact on operational readiness, and alternatives are not always quickly available [8]. The manifestation of external threats and their possible impact on supply chains are summarized in Table 1.

Table 1.

Manifestation and impact of external threats on the supply chain

Threat	Manifestation	Impact
Geopolitical	Restrictions, price spikes, loss of access	High uncertainty, cascading disruptions
Supplier and market instability	Unfulfilled contracts, capacity shortages	Long recovery times, shortages of critical goods
Transport and infrastructure disruptions	Route restrictions, border-crossing problems	Delays, reduced reliability
Cyber	Supplier compromise	Systemic IT disruptions, risk of data loss
Regulatory and political	Sanctions, export controls, standards	Restricted supply, higher costs

Source: compiled by the author.

2. Threats Specific to Military Supply Chains

In order to enhance the resilience of supply chains that are important to the armed forces, it is not sufficient to assess only threats that arise beyond the boundaries of the system and are related to environmental conditions. Resilience is also significantly shaped by the specific military context in which the supply chain operates, giving rise to a separate group of threats. These threats typically arise from conditions of crisis or conflict, in which supply must be maintained under greater uncertainty, limited infrastructure throughput, and rapidly changing needs [9]. Such threats encompass not only conventional actions but also irregular, informational, and cyber means that may be directed at communications, information systems, and infrastructure. From the standpoint of enhancing resilience, this means that

the supply chain must be able to maintain its supply function when disruptions occur simultaneously across several links [2].

In summary, threats arising from the military environment affect the resilience of the armed forces' supply chain most strongly when supply must be maintained under conditions of high uncertainty, limited infrastructure throughput, and rapidly changing needs. The greatest impact is caused by mobility and throughput disruptions and by dependence on a limited pool of suppliers, since these factors directly determine the continuity of supply and the speed of recovery. A significant share of threats is related to technological disruptions, which can affect planning and coordination.

Table 2.

Manifestation and impact of military-environment threats on the supply chain

Threat	Manifestation	Impact on the chain
Mobility and throughput disruptions	Delays, route changes, node congestion	Reduced continuity of supply
Dependence on a limited pool of suppliers	Limited alternatives, long replacement time	Slow recovery, greater shortages
Software supply incidents	Disrupted software updates	Disruption of critical processes
Coordination complexity during crises	Conflicting priorities, delayed decisions	Slower response and distribution disruptions
Cybersecurity gaps	Weak incident management, limited supplier oversight	Greater spread of disruptions

Source: compiled by the author.

3. Research Methodology

Analysis of the scholarly literature revealed that the functioning of military supply chains is undermined by a variety of internal, external, and military-environment threats. As a result, resilience becomes an essential property of military supply chains, ensuring that the supply of forces is maintained even under conditions of disruption [3, 5, 14].

Resilience is described as a process aimed at rapidly restoring supply chain operations after disruptions, combining prior preparedness, response, and recovery [10]. The resilience of military supply chains is understood as the ongoing capacity to reduce vulnerabilities in advance, detect disruptions in a timely manner, adapt to changing conditions, and restore supply in such a way that the provisioning of critical armed-forces capabilities is maintained within an acceptable time frame and at an acceptable cost. Resilience is most commonly analyzed through four interrelated types: structural, operational, technological, and strategic resilience. Such a typology makes it possible to link different resilience-enhancing measures more clearly to the strengthening of the supply chain [1, 4, 16, 19, 20, 22].

Various scholarly sources likewise identify a large number of threat-management measures - risk assessment, inventory reserves, diversification of suppliers and supply routes, digitalization, and disruption-management plans [11, 13, 15, 17, 18].

Taking into account the supply chain threats and resilience-enhancing measures identified in the scholarly literature, the aim of the empirical study presented in this article is to identify the categories of external supply chain threats relevant to the Lithuanian Armed Forces (LAF) and to assess the application of measures that enhance the resilience of these chains.

A qualitative research method was chosen to achieve this aim. The method was selected in light of the scope of the study: given a small number of highly qualified respondents, a qualitative approach makes it possible to extract the maximum amount of information from each participant. A purposive sampling method was applied to select the experts. It was chosen because the aim of the study is to examine which threats affect LAF supply chains in practice and which practical resilience-enhancing measures are applied. Obtaining such answers requires individuals with experience of threats to LAF supply chains and of ensuring the resilience of these chains. Experts were selected according to the following criteria:

1. Currently work, or have worked for at least three years, in LAF supply or logistics.
2. Have been directly involved in supply planning, inventory, or risk-management (decision-making) processes.
3. Know, and have themselves applied, measures aimed at enhancing the resilience of LAF-critical supply chains.

A semi-structured questionnaire was used to collect the empirical data. The content of the questions was developed on the basis of the findings of the scholarly-literature analysis. The empirical data collected were analysed using qualitative content analysis, which allows open-ended respondent answers to be processed systematically by

distinguishing key themes, salient ideas, and recurring patterns. This method of analysis was chosen because the study involves a small number of experts, and the survey seeks not to measure phenomena quantitatively but to gain a deeper understanding of their causes. Fundamental principles of research ethics were observed throughout the study (the interview instrument was designed so that no personal data were requested, and the questions were formulated in general terms in order to ensure anonymity and reduce the possibility of identifying specific individuals).

4. Main Research Findings

In pursuit of the study's aim, expert interviews were conducted and the resulting answers processed; the principal threats to LAF-critical supply chains were identified first.

Table 3.

Main external supply chain threats

Category	Subcategory	Supporting statements
External threats	Supplier and market threats	Suppliers are unable to deliver the required goods / suppliers capable of meeting needs are not always available, causing delays in supply
External threats	Geopolitical and political threats	The geopolitical situation (particularly the war in Ukraine) increases demand, shifts priorities, and causes major supply disruptions
External threats	Economic and financial threats	Price changes and changes in funding affect procurement volumes and plan execution
External threats	Legal and regulatory threats	Public-procurement appeals / litigation halt processes and delay deliveries
External threats	Natural and environmental threats	Supply was disrupted during the COVID period, and orders were subsequently delayed, catching up only after the pandemic

Source: compiled by the author, based on the empirical research data.

The summarized responses show that, in the experts' experience, the main external threats are related primarily to supplier and market capacity and to the geopolitical environment. The experts note that suppliers capable of meeting needs on time are not always available, causing supply delays, and that the situation is further complicated by geopolitical events — particularly the war in Ukraine — which increase demand and shift priorities. Economic changes, such as price fluctuations and funding constraints, are also identified as external factors, since they can reduce procurement volumes or force plans to be adjusted. Legal factors are likewise emphasized, as public-procurement appeals and litigation halt processes and delay deliveries. The impact of the pandemic also stands out, since disruptions during the COVID period caused some orders to be delayed and fulfilled only later.

The experts' assessments also indicate that external threats to LAF supply chains do not occur continuously but rather episodically, making it difficult to predict when they will arise. The experts' answers also made it possible to identify the main causes of external threats (Table 4).

Table 4.

Causes of external supply chain threats

Category	Subcategory	Supporting statements
External threats	Legal causes	Legal proceedings and disputes can halt procurement and delay delivery
External threats	Financial causes	Changes in funding volumes alter the planned scope of procurement and its timelines
External threats	Supplier-related causes	Supplier capacity and priorities: large orders for other countries, redirection to conflict zones, inability to meet delivery deadlines
External threats	Environmental causes	Political decisions and the security environment (e.g., war), economic imbalances (demand, prices), and the effects of the pandemic

Source: compiled by the author, based on the empirical research data.

It can be seen that external threats to the LAF supply chain arise from several distinct causes. The experts distinguish four groups: legal processes, changes in funding, supplier capacity and priorities, and the broader security and economic environment. Disruptions most often arise when several of these factors act simultaneously. The experts link legal disruptions to complaints and disputes that halt procurement or prolong the process. Changes in funding affect planning stability, since a change in volumes requires procurement plans and timelines to be revised. On the supplier side, the most important factors are limited capacity and the reallocation of priorities (large orders for other countries mean that supply is delayed or that some needs remain unmet). Environmental factors are linked to war, political decisions, changes in demand and prices, and the effects of the pandemic, all of which shift priorities and extend timelines.

Further analysis of the expert interview results made it possible to identify the specific methods and measures applied to detect and mitigate threats to LAF supply chains (Table 5).

Table 5.

Measures for detecting and mitigating threats to LAF-critical supply chains

Category	Subcategory	Supporting statements
Risk assessment	Monitoring	Monitoring of consumption; procurement status tracked through reporting
Risk assessment	Planning	Annual procurement planning; planning based on realistic delivery deadlines and advance notification when deadlines slip
Risk assessment	Inventory buffers	Use of reserves and accumulation of additional stock, taking storage capacity into account
Risk assessment	Escalation and alternatives	Where a problem is anticipated, decisions are “escalated,” resources are reallocated, plans are adapted, and, if necessary, expedited procurement and alternative channels are used

Source: compiled by the author, based on the empirical research data.

The table shows that the detection of threats and the mitigation of their impact rest on four practical groups of measures. These encompass monitoring, planning, inventory reserves, and the escalation of decisions together with the search for alternatives. Risk is first identified through consumption signals and the tracking of procurement status, and is subsequently mitigated through the maintenance of reserves, the adjustment of plans, and faster decision-making. In summary, threat management within LAF supply chains proceeds as a consistent process from an early signal to concrete actions that provide time to maintain supply when the normal channel is disrupted.

Finally, the summary of the interview results identified the measures that, in the experts’ opinion, contribute most to enhancing the resilience of LAF-critical supply chains.

Table 6.

Measures that most strengthen supply chain resilience

Category	Subcategory	Supporting statements
Assessment of resilience outcomes	Inventory	The accumulation of stock and the holding of reserves contributed the most
Assessment of resilience outcomes	Alternatives	When supply cannot be obtained through the regular supplier, alternative solutions are applied — an agency or other procurement channels are used, thereby ensuring supply
Assessment of resilience outcomes	Digitalization	Digitalization provides the information base; without it, inventory and risk management become very difficult

Source: compiled by the author, based on the empirical research data.

The measures that most enhance resilience are regarded by the experts as interrelated. The greatest effect comes from a combination of measures, since inventory provides time, alternative channels provide options for a solution, and digitalization provides the data needed to respond in a timely and accurate manner. The results showed that the resilience of Lithuanian Armed Forces supply chains does not depend on a single solution but on several interconnected elements — the quality of coordination, risk management, inventory reserves, alternative procurement channels, and the maturity of digitalization. In practice, the maintenance of resilience rests on reserves, monitoring and

plan adjustment, decision escalation, and alternative channels, while technologies and information systems help to detect warning signals and make decisions more quickly; their benefit, however, depends directly on the quality of the data and on whether digitalization extends down to the warehouse level.

5. Conclusions

Analysis of the literature showed that threats relevant to the supply chain can be clearly grouped into several categories. The external threats examined in this article arise from the geopolitical environment, supplier and market instability, transport or infrastructure disruptions, cyber risks originating through suppliers, and regulatory change. The resilience-enhancing measures identified in the literature, meanwhile, are most commonly associated with systematic risk assessment, inventory and reserve management, the diversification of suppliers and channels, alternative procurement routes, and digitalization, which increases the visibility and transparency of ongoing processes.

The empirical study showed that external-environment threats to supply chains important to the Lithuanian Armed Forces more often occur as isolated cases, but their impact can be substantial and can significantly lengthen supply timelines. The most frequently recorded external threats are shortfalls in supplier capacity, price fluctuations, and the influence of the geopolitical environment. In practice, the impact of these threats is mitigated through the accumulation of material reserves, the diversification of supply channels, and legal and financial risk-management solutions.

The empirical results largely confirm the principal supply chain threats identified in the theoretical section and the resilience-enhancing measures proposed in the literature, while at the same time highlighting a practical problem: formally described procedures alone do not guarantee resilience. Resilience is weakened most by delayed information and occasional coordination failures, as a result of which measures are applied too late or not as intended. The greatest supply chain resilience is achieved when inventory, supplier diversification, digitalization, risk monitoring, and crisis preparedness operate together as a coordinated set of measures rather than as isolated initiatives.

Acknowledgements. This work was conducted in accordance with the Research Supporting Studies, order No. V-292 and V-295 of 2 April 2026, General Jonas Žemaitis Military Academy of Lithuania.

References

1. **Alquraish, M.** (2025). Digital transformation, supply chain resilience, and sustainability: A comprehensive review with implications for Saudi Arabian manufacturing. *Sustainability*, 17(10), Article 4495. <https://doi.org/10.3390/su17104495>
2. **Ekström, T.** (2023). Towards defence supply chain resilience: A prestudy of the Swedish defence sector. *The NATO Science and Technology Organization (STO) Journal*, 3, 8-1–8-20.
3. **Ekström, T.** (2025). Supply chain resilience: An empirical exploration of barriers and enablers in military settings. *Scandinavian Journal of Military Studies*, 8(1), 119–136. <https://doi.org/10.31374/sjms.350>
4. **Elvemo, L.** (2025). Supply chain resilience in military operations: A case study exploring command and control. *Scandinavian Journal of Military Studies*, 8(1), 178–199. <https://doi.org/10.31374/sjms.356>
5. **Emrouznejad, A., Abbasi, S., & Sıcakyüz, Ç.** (2023). Supply chain risk management: A content analysis-based review of existing and emerging topics. *Supply Chain Analytics*, 3, Article 100031. <https://doi.org/10.1016/j.sca.2023.100031>
6. **Gokkaya, B., Aniello, L., & Halak, B.** (2026). Software supply chain: A taxonomy of attacks, mitigations and risk assessment strategies. *Journal of Information Security and Applications*, 97, Article 104324. <https://doi.org/10.1016/j.jisa.2025.104324>
7. **Gokkaya, B., Karafili, E., Aniello, L., & Halak, B.** (2025). Global supply chains security: A comparative analysis of emerging threats and traceability solutions. *Benchmarking: An International Journal*, 32(3), 917–942. <https://doi.org/10.1108/BIJ-08-2023-0535>
8. **Grala, D.** (2024). Resilience of military supply chains. In *Digital Synergy* (pp. 257–263). CRC Press. <https://doi.org/10.1201/9781003440406-29>
9. **Hellberg, R., & Lundmark, M.** (2025). Transformation in European defence supply chains as Ukraine conflict fuels demand. *Scandinavian Journal of Military Studies*, 8(1), 17–39. <https://doi.org/10.31374/sjms.303>
10. **Hosseini Shekarabi, S. A., Kiani Mavi, R., & Romero Macau, F.** (2025). Supply chain resilience: A critical review of risk mitigation, robust optimisation, and technological solutions and future research directions. *Global Journal of Flexible Systems Management*, 1–55. <https://doi.org/10.1007/s40171-025-00441-4>

11. **Kancs, D. A.** (2024). Uncertainty of supply chains: Risk and ambiguity. *The World Economy*, 47(5), 2009–2033. <https://doi.org/10.1111/twec.13534>
12. **Konecka, S., & Bentyn, Z.** (2024). Cyberattacks as threats in supply chains. *European Research Studies Journal*, 27(3), 778–796. <https://doi.org/10.35808/ersj/3467>
13. **Latsiou, A., & Lambrinoudakis, C.** (2026). Cyber supply chain risk management: From threats to treatment. *International Journal of Information Security*, 25, Article 40. <https://doi.org/10.1007/s10207-025-01207-9>
14. **López, C., Morales-Contreras, M. F., Langella, I. M., & Alonso-Monge, J.** (2025). Modeling supply chain disruptions due to geopolitical reasons: A systematic literature review. *Transportation Research Part E: Logistics and Transportation Review*, 202, Article 104290. <https://doi.org/10.1016/j.tre.2025.104290>
15. **Papaphilippou, M., Moulinos, K., & Theodoridou, M.** (2023). *Good practices for supply chain cybersecurity*. European Union Agency for Cybersecurity (ENISA).
16. **Paulus, A.** (2025). *An Achilles heel of today's armed forces: Managing software supply chain risk in the military sector* (SWP Research Paper 2025/RP 06). Stiftung Wissenschaft und Politik (SWP).
17. **Pedersen, O., Jahre, M., & Norrman, A.** (2025). A balancing act: Towards a conceptual framework for the governance of buyer–supplier relationships in defence supply chains. *Scandinavian Journal of Military Studies*, 8(1), 152–177. <https://doi.org/10.31374/sjms.354>
18. **Rozhkov, M., Ivanov, D., Blackhurst, J., & Nair, A.** (2022). Adapting supply chain operations in anticipation of and during the COVID-19 pandemic. *Omega*, 110, Article 102635. <https://doi.org/10.1016/j.omega.2022.102635>
19. **Sani Mohammed, S., Schaefer, D., & Milisavljevic-Syed, J.** (2023). Towards pre-emptive resilience in military supply chains: A compromise decision support model based approach. *Production & Manufacturing Research*, 11(1), Article 2220768. <https://doi.org/10.1080/21693277.2023.2220768>
20. **Singh, G., Rajesh, R., Misra, S. C., & Singh, S.** (2024). Analyzing the role of digital twins in developing a resilient sustainable manufacturing supply chain: A grey influence analysis approach. *Technological Forecasting and Social Change*, 209, Article 123763. <https://doi.org/10.1016/j.techfore.2024.123763>
21. **Wen, S. F., & Sharma, A.** (2025). A unified, threat-validated taxonomy for hardware security assurance. *Journal of Cybersecurity and Privacy*, 5(4), Article 86. <https://doi.org/10.3390/jcp5040086>
22. **Zhao, N., Hong, J., & Lau, K. H.** (2023). Impact of supply chain digitalization on supply chain resilience and performance: A multi-mediation model. *International Journal of Production Economics*, 259, Article 108817. <https://doi.org/10.1016/j.ijpe.2023.108817>

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of CNDCGS 2026 and/or the editor(s). CNDCGS 2026 and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.