Journal of Defense Analytics and Logistics

Supply-chain risks and resilience mechanisms relevant to military aviation: a systematic review of defense and aerospace literature

Rui Fernando Correia Ferreira
Master's Program in Administration, Unihorizontes University Centre, Belo Horizonte, Brazil and
Minas Gerais State University, Cláudio Campus, Cláudio, Brazil
Wesley Canedo Souza Junior
Digital Metropolis Institute, Federal University of Rio Grande do Norte, Natal, Brazil, and
Bruno Vilela
Department of Administration, Federal University of Espírito Santo, Vitória, Brazil

Received 16 June 2025
Revised 25 July 2026
19 August 2026
27 August 2026
Accepted 31 August 2026

Abstract

Purpose – This study synthesizes defense and aerospace supply-chain literature to identify and organize risks and resilience mechanisms relevant to the industrial, maintenance, and sustainment systems supporting military aviation, with particular attention to aircraft availability and operational continuity.

Design/methodology/approach – A systematic review of Scopus and Web of Science identified 20 studies addressing defense, military and aerospace supply chains. Following a PRISMA-based selection process, risk and resilience statements were extracted, thematically coded, supported by lexical matching and manually reviewed.

Findings – Four risk clusters were identified, Physical/Cybersecurity, Strategic Dependency, Hostile External Environment and Inefficient Management, and five resilience clusters, Structural Preparedness, Adaptive Response, Operational Intelligence, Strategic Cooperation, and Critical Sustainment. Together, they show how readiness depends on industrial capacity, maintenance continuity, information, adaptation and cooperation.

Research limitations/implications – The corpus is limited to two overlapping databases, title-based queries, retrievable full texts and 20 studies. Grey literature and specialized defense repositories are not systematically covered. The clusters should therefore be interpreted as a preliminary taxonomy requiring validation across countries and aviation programs.

Practical implications – The study links strategic stocks, supplier diversification, predictive monitoring, rapid reconfiguration, allied cooperation and lifecycle sustainment to operational continuity.

Social implications – Stronger military aviation supply chains support national security and the continuity of strategic public capabilities during conflict or systemic disruption.

Originality/value – The study offers a disaggregated taxonomy of risks and resilience mechanisms relevant to military aviation supply chains, connecting technical, industrial, organizational, geopolitical and sustainment dimensions while distinguishing aviation-specific evidence from transferable evidence drawn from adjacent contexts.

Keywords Military aviation, Supply chain resilience, Strategic risks, Defense industry, Sustainment, Systematic review

Paper type Literature review

Journal of Defense Analytics and Logistics
Emerald Publishing Limited
e-ISSN: 2399-6447
p-ISSN: 2399-6439
DOI 10.1108/JDAL-06-2025-0016

1. Introduction

Military aviation supply chains have received increasing attention as geopolitical tensions and industrial-capacity constraints have intensified. In Europe, the European Investment Bank (EIB) tripled its support for small and medium-sized enterprises (SMEs) in the air-defense supply chain—from €1 billion to €3 billion as of June 2025—thereby bolstering regional industrial resilience and reducing reliance on external suppliers (Reuters, 2025a). In the United States, Joe DePietro, Vice President of Lockheed Martin, emphasized that supply-chain integrity must be regarded as a “frontline” strategic priority, noting the urgent need to address a “speed mismatch” to ensure logistical agility and national security during periods of heightened geopolitical tension (Axios, 2025).

Moreover, tariff disputes and geopolitical pressures are compelling firms such as Lockheed Martin and Raytheon to reassess their production strategies. These developments underscore the critical importance of strengthening domestic manufacturing, advancing logistical innovation, and diversifying supplier bases—measures deemed essential for rapid response capability during emerging crises and for maintaining operational superiority (Reuters, 2025b). Together, these developments suggest that airpower readiness and military operational capability will increasingly depend upon the robustness, adaptability, and autonomy of air-defense supply chains.

These policy responses show that defense supply-chain resilience is not only an operational logistics concern but also an industrial-policy issue shaped by trade exposure, strategic autonomy, procurement rules, and the capacity to mobilize civilian and defense suppliers. Lucas *et al.* (2024) argue that defense disruption management must account for the multisectoral nature of defense supply chains and must evaluate carefully which commercial practices can be transferred to defense. This perspective is particularly relevant to military aviation, where production, maintenance, software, electronics, energy, transport, and public procurement are institutionally interdependent.

This sector is highly strategic, complex, and interdependent, characterized by protracted product life cycles, high technological intensity, and sophisticated contractual and logistical structures. Ng *et al*. (2009) argue that the adoption of outcome-based contracts necessitates systemic coordination between clients and suppliers, transforming the supply chain into a value co-creation ecosystem. Similarly, Turkina *et al*. (2016) highlight that this industry is knowledge- and innovation-intensive, operating within geographically specialized global industrial clusters, as exemplified by the production network of the Boeing 787.

Oksuz Gurdal and Testik (2025) emphasize the role of digitalization, highlighting technologies such as Digital Twin and Product Lifecycle Management (PLM), which enable real-time tracking and integration. Mejino-Lopez and Wolff (2025) warn of recent geopolitical challenges, such as the war in Ukraine, which underscore the need for a coordinated expansion of European production capacity. Finally, according to Achmadi and Sutawidjaya (2024), the sector’s effectiveness depends on coordination among government, the armed forces, and private firms, and is heavily influenced by public policies and national defense strategies.

Risks relevant to military aviation arise from both non-deliberate disruptions and deliberate hostile action. Industrial and commercial disruptions include supplier failure, trade restrictions, infrastructure outages, material shortages, and abrupt demand changes; adversarial disruptions refer specifically to cyberattacks, sabotage, counterfeit or malicious components, and attacks on logistics nodes. This distinction is important because the industrial and maintenance focus of this article does not make every operational threat directly comparable to an ordinary market disruption. Both types can nevertheless converge and compromise aircraft availability and operational continuity (Elvemo, 2025; Ivanov and Dolgui, 2020; Ahn *et al.*, 2025). Resilience is therefore understood as the capacity to prepare for, absorb, adapt to, recover from, and sustain operations during disruptions, supported by connectivity, control, flexibility, and redundancy (Ponomarov and Holcomb, 2009).

Therefore, the interplay between risk and resilience reveals the strategic importance of robust and adaptive supply chains in military aviation, particularly during prolonged crises.

The study asks: What supply-chain risks and resilience mechanisms identified in the defense and aerospace literature are relevant to the industrial, maintenance, and sustainment systems supporting military aviation? To answer this question, the study maps and classifies recurring risks and resilience mechanisms and examines how the resulting clusters contribute to aircraft availability, logistical autonomy, and operational continuity.

The scope is therefore narrower than military logistics as a whole. It centers on the industrial, maintenance, and sustainment arrangements that provide aircraft, systems, spare parts, repair, technical information, and supporting infrastructure. Literature from broader defense, civilian, humanitarian, medical, or historical contexts is included only when it explains a transferable mechanism—such as supplier concentration, redundancy, disruption propagation, mobilization, or coordination. Such sources provide contextual or analogical evidence and are not treated as direct proof of aviation-specific effects.

A structured literature review was conducted using Scopus and Web of Science (WoS), followed by a PRISMA-based selection process and qualitative content analysis (Moher *et al.*, 2009; Tranfield *et al.*, 2003; Krippendorff, 2019, pp. 102–156). The review combines thematic coding with lexical matching as an organizational aid and manual verification of the final assignments.

The structure of the article is organized into five main sections. The introduction presents the research context and defines the central question. The literature and context section discusses key concepts related to risks and resilience relevant to military aviation. Next, the methodology section outlines the systematic review strategy based on the PRISMA protocol. The analysis and discussion section consolidates the findings into thematic groupings. Finally, the conclusion synthesizes the results, highlights the study's contributions, acknowledges its limitations, and proposes directions for future research.

2. Literature and context

The literature review is organized to support the research question and the subsequent coding. Section 2.1 defines the military aviation context and the sectoral characteristics that shape supply-chain vulnerability. Sections 2.2 and 2.3 establish the risk and resilience concepts used to interpret the extracted statements. This structure also clarifies why some adjacent sources are relevant and how their evidential weight differs from studies directly addressing military aviation or defense-industrial supply chains.

2.1 Military aviation context

The military aviation industry is distinguished by its structural and contractual complexity, operating under highly sophisticated business models. According to Ng *et al*. (2009), the logic of performance-based contracts—by replacing compensation for completed tasks with outcome-oriented remuneration—redefines the relationship between governments and suppliers, positioning the client as a co-producer of value. This model requires firms to integrate both tangible and intangible resources into systems that not only deliver products but also ensure long-term support services over decades. Such an approach demands coordination among actors, technologies, and processes, increasing the complexity of contract management and supply-chain coordination.

The aerospace sector's production structure is organized into highly specialized, multilayered collaborative networks. As noted by Turkina *et al*. (2016), this industry operates within industrial clusters that connect global prime contractors to specialized suppliers. These networks extend well below Tier 1 and Tier 2: major military aviation programs may include several additional sub-tiers comprising hundreds or thousands of firms that provide systems, electronics, components, materials, and maintenance inputs. The Eurofighter Typhoon, for example, involves more than 400 European firms and multiple vertical levels of design and supply responsibility, illustrating how political work-sharing, cross-border interdependence, and lower-tier visibility create organizational complexity (Matthews and Al-Saadi, 2023). Such structures enable specialization and innovation but also increase coordination costs, exposure to bottlenecks, and difficulty in tracing vulnerabilities.

Military aviation also combines several characteristics that intensify supply-chain risk: long and costly platform lifecycles, strict airworthiness and security requirements, low-volume production, dependence on defense electronics and software, component obsolescence, and growing fleets of unmanned systems that require interoperable architectures and long-term support. International co-development and co-production can distribute development costs and preserve national industrial participation, but politically negotiated work shares may increase bureaucracy, duplication, and cost (Matthews and Al-Saadi, 2023). The increasing importance of open architectures in unmanned aircraft further illustrates the tension between interoperability, proprietary control, upgradeability, and sustainment (US Government Accountability Office, 2013).

The adoption of digital technologies has profoundly transformed how the sector manages its products and processes. According to Oksuz Gurdal and Testik (2025), the integration of Digital Twins into Product Lifecycle Management enables the digital tracking of assets throughout their entire life cycle, facilitating more accurate decision-making and reducing costs associated with physical prototypes. Furthermore, the connection with IoT sensors and machine learning algorithms enhances predictive capabilities and logistical efficiency across the organizations involved. Digital integration can improve production resilience and make supply-chain information increasingly important to technological and operational performance.

Geopolitical dynamics and public policy play a central role in shaping the defense aerospace industry. As noted by Mejino-Lopez and Wolff (2025), the conflict in Eastern Europe has renewed the urgency of expanding defense production capacity, reducing procurement fragmentation, and improving standardization. Achmadi and Sutawidjaya (2024) similarly show that supply-chain effectiveness depends on coordination among the state, armed forces, and private firms. The relevant institutional arrangements differ across countries: the United States, European collaborative programs, Brazil, Indonesia, and other settings combine industrial policy, sovereignty, competition, and international dependence in distinct ways. Accordingly, this study adopts a cross-national, mechanism-oriented lens. Its clusters identify recurrent mechanisms across contexts rather than estimating the prevalence or severity of risks in any single country or alliance.

2.2 Supply-chain risk

Supply chain risk, as described by various authors, refers to the potential occurrence of unexpected events that negatively affect coordination, performance, and the continuity of logistics operations (Kleindorfer and Saad, 2005; Ponomarov and Holcomb, 2009; Tang, 2006). Kleindorfer and Saad (2005) distinguish between coordination risks and disruption risks, with the latter being more critical as they involve natural disasters, operational failures, or human actions such as terrorism. Tang (2006) complements this view by categorizing risks as either operational or disruptive, emphasizing that both can severely impact firms' financial performance, as exemplified by the cases of Ericsson and Apple. Ponomarov and Holcomb (2009) further emphasize the risks created by globally interconnected supply chains, whose structural complexity increases exposure to risks that may propagate throughout the network, raising costs and compromising service continuity.

In military aviation, supply-chain risks take on strategic significance because aircraft availability, continuing airworthiness, mission readiness, and national sovereignty are affected simultaneously. Deliberate threats may include cyber interference, sabotage, counterfeit components, and attacks on logistics or critical infrastructure, whereas non-deliberate risks include supplier failure, obsolescence, sanctions, and sudden demand shifts (Ahn *et al.*, 2025; Elvemo, 2025). The war in Ukraine also demonstrates that an adversary may target industrial capacity, transport infrastructure, and civilian facilities on which defense supply chains depend. Risk anticipation is therefore not limited to delivery performance; it also protects the ability to generate and sustain air power.

The complexity of supply chains is heightened by global interdependence, sensitive technologies, long platform lifecycles, and limited sources for certified components. Civilian cases such as Toyota and pandemic-related disruptions remain useful for explaining generic mechanisms such as disruption propagation, single points of failure, and the vulnerability of lean networks (Pettit *et al*., 2010; Ivanov and Dolgui, 2020). However, these cases are treated as mechanism-level analogies rather than direct evidence of military aviation outcomes. Aviation-specific interpretation requires attention to airworthiness, security restrictions, low production volumes, maintenance documentation, technological obsolescence, and the operational consequences of unavailable parts.

Risk management, in this sense, should be integrated into the entire lifecycle of the supply chain, from product design to final delivery, as advocated by Ahn *et al.* (2025). In addition to physical and natural threats, cybersecurity and safety failures are emerging concerns, particularly in safety- and mission-critical sectors such as military aviation. Malicious insertions in technological components, for instance, may compromise the functioning of entire defense systems. Therefore, supply chain governance must incorporate robust monitoring, traceability, and practices for responding rapidly to disruptive events, ensuring that operations remain uninterrupted even in crisis scenarios.

These distinctions guide the results section. Sources directly addressing military aviation or defense-industrial systems carry the greatest weight for sector-specific claims. Broader military evidence is used to explain defense governance or operational mechanisms, while civilian and historical examples are used only to illuminate generic supply-chain processes. The resulting clusters therefore integrate evidence at different levels without assuming that all examples are equally representative of contemporary military aviation.

2.3 Supply-chain resilience

Supply chain resilience, according to Kleindorfer and Saad (2005), is grounded in the ability to withstand and recover from disruptions through preventive and structural actions such as source diversification, redundancy, and process modularity. This approach shifts the traditional focus on efficiency to also encompass flexibility and readiness in the face of unforeseen events. Tang (2006) further emphasizes the role of coordinated and collaborative strategies in mitigating risks, highlighting the importance of integrated supply chain management as a means to ensure continuity and profitability. Thus, resilience emerges as a critical attribute for addressing the complexity and volatility of the organizational environment.

In the military aviation industry, resilience plays a strategic role due to the sector's operation in high-risk and uncertain contexts. As Elvemo (2025) notes, a resilient military supply chain must demonstrate readiness, rapid response capability, and efficient recovery—essential elements for ensuring the continuity of critical missions. Ponomarov and Holcomb (2009) complement this perspective by incorporating organizational, ecological, and psychological dimensions into the concept, arguing that adaptive capacity and organizational learning are crucial to overcoming disruptions. This combination of factors underscores the central role of resilience in maintaining operational superiority and national security.

The complexity of the supply chain in military aviation demands sophisticated technical and organizational solutions. Ahn *et al.* (2025) point out that, in the face of cyber risks and technical failures, resilience relies on architectures such as the Zero Trust model, the use of artificial intelligence for anomaly detection, and multiple layers of redundancy. Ivanov and Dolgui (2020) emphasize that resilience should not be conflated with stability or robustness, as it requires active adaptation processes to restore performance. During the COVID-19 pandemic, traditional solutions proved insufficient, underscoring the need to complement resilience with concepts such as viability under prolonged crisis conditions.

Ultimately, resilience also emerges as a lever for competitive advantage—even in the defense sector. Pettit *et al*. (2010) argue that resilience must integrate attributes such as diversity, cohesion, and adaptability, enabling organizations not only to withstand turbulent events but to grow from them. Dell's experience, in which the company capitalized on a crisis to expand its sales, illustrates how strategic adaptation can yield substantial gains. In this sense, resilience extends beyond traditional risk management and can become an important source of sustained organizational performance in highly technological and interdependent military supply chains.

For this study, resilience is treated as a sequence of related capabilities spanning preparedness, response, recovery, and prolonged sustainment. The broader literature identifies readiness, response, and recovery as recurring dimensions (Han *et al*., 2020), while military research emphasizes that preparedness and sustainability requirements can differ from commercial priorities centered on cost efficiency (Ekström *et al*., 2020; Ekström, 2025). This distinction provides the conceptual link between the literature review and the five higher-order clusters of resilience mechanisms reported below.

3. Material and methods

The study adopted a structured literature review that combines the transparent selection logic of PRISMA with the evidence-informed management principles proposed by Tranfield *et al*. (2003). PRISMA was selected because its identification, screening, eligibility, and inclusion stages provide an auditable account of how records entered the review, while the management-review perspective emphasizes the need to connect the protocol to the research question and to assess contextual transferability. Scopus and Web of Science (WoS) were selected because of their broad multidisciplinary coverage and established journal indexing (Mongeon and Paul-Hus, 2016). Their considerable overlap and limited coverage of grey literature, technical reports, defense white papers, NATO publications, and specialized repositories such as the Defense Technical Information Center mean that the study synthesizes indexed academic literature rather than the full body of defense practitioner knowledge.

The search was conducted on June 11, 2025, using the title-field queries presented in Figure 1. The queries were designed to identify literature concerning risk and resilience in defense, military, and aerospace supply chains. Because they did not include aviation-specific terms, the search should not be interpreted as providing exhaustive coverage of the military-aviation literature. Instead, the review evaluates the relevance and transferability of this broader evidence base to military aviation. The searches identified 28 Scopus and 14 WoS records. After title and abstract screening, full-text eligibility assessment, database merging, and duplicate removal, 20 unique studies remained: 15 journal articles, three conference papers, and two book chapters. The original protocol required retrievable full text because factor-level coding depended on complete documents. This criterion may introduce availability bias and is therefore treated as a limitation rather than a neutral administrative condition. A targeted supplementary search conducted in July 2026 examined additional relevant sources and backward references. These materials were used as contextual support to assess coverage and the stability of the higher-order clusters, but they were not retrospectively recoded as members of the original corpus.

After study selection, each document was read in full and an extraction matrix was used to record its context and every explicit statement describing either a supply-chain risk or a resilience mechanism. The unit of analysis was a distinct textual statement that identified a source of disruption or a capability, practice, or resource associated with preparation, response, recovery, or sustainment. This procedure generated 116 risk statements and 107 resilience-mechanism statements. Content analysis was used to interpret these statements in context, while unitizing and recording followed the logic described by Krippendorff (2019,

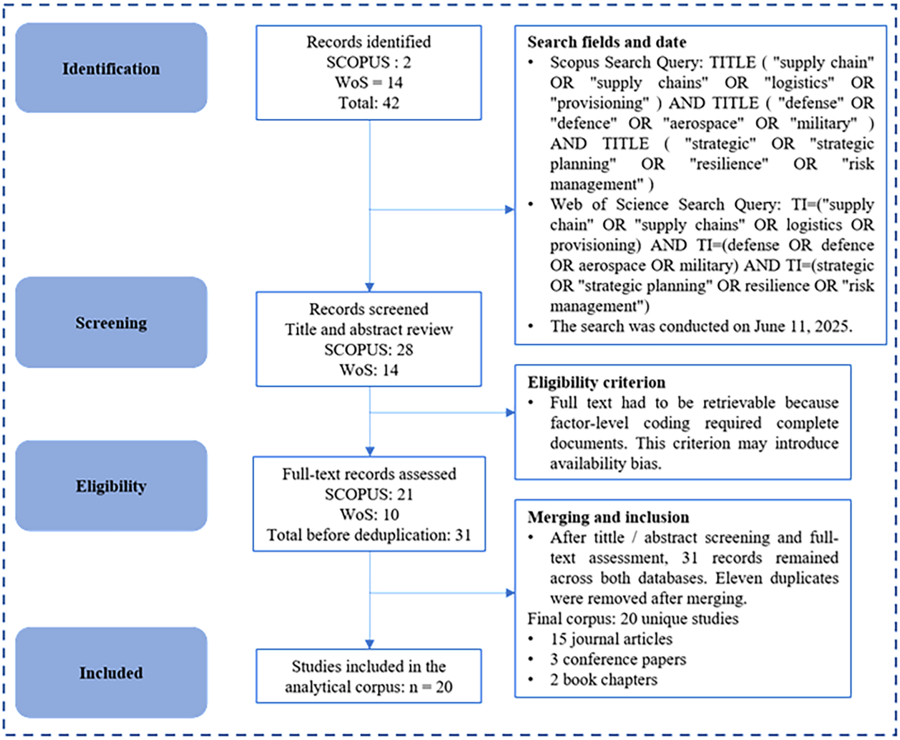

Figure 1. PRISMA-based study selection process. **Source**: Prepared by the authors

pp. 102–156). Elvemo (2025) was used as a related military benchmark for comparison, not as a taxonomy adopted in advance.

The clustering proceeded in five stages. First, semantically equivalent statements were grouped, while contextual differences were retained in the extraction matrix. Second, open thematic coding generated provisional labels. Third, representative words and expressions were used in a lexical matching procedure to suggest provisional groupings, drawing on text-mining and natural-language-processing principles (Feldman and Sanger, 2006; Grimmer and Stewart, 2013). Fourth, each assignment was manually checked against the source passage so that semantic meaning prevailed over lexical similarity. Fifth, the provisional groupings were iteratively compared to define higher-order clusters with internal coherence and clear distinction from the other clusters (Braun and Clarke, 2006; Guest *et al.*, 2012). The lexical procedure supported organization; it did not independently determine the final categories.

Manual validation consisted of rereading each statement in its original article context, examining boundary cases, and revising assignments that were semantically inconsistent with the provisional cluster. Final cluster assignments therefore reflect researcher judgment informed, but not determined, by the lexical matching procedure. Because the classification was not independently replicated by additional coders, no intercoder reliability coefficient could be calculated. This limits replicability and should be addressed in future validation studies using an explicit codebook and independent coders. Accordingly, the nine clusters should be interpreted as researcher-validated analytical categories rather than mechanically generated results.

Once categorization was finalized, cross-cluster relationships were interpreted qualitatively by comparing how risks and resilience mechanisms were connected across the reviewed studies. No formal network model or inferential causal test was performed. Accordingly, the results are presented as an analytical taxonomy that organizes recurring evidence and supports theory development, not as a quantified model of causal effects or prevalence.

4. Results

4.1 Risks relevant to military aviation

Across the 20 studies in the analytical corpus, 116 risk statements relevant to defense and aerospace supply chains were identified. The coding process organized them into four higher-order clusters—Physical/Cybersecurity, Strategic Dependency, Hostile External Environment, and Inefficient Management. These clusters synthesize recurrent mechanisms rather than measuring their frequency or impact in a particular country. Table 1 presents the categories that guide the subsequent interpretation, with aviation-specific conclusions distinguished from evidence transferred from broader military, civilian, or historical contexts.

Physical and cybersecurity risks within military aviation supply chains arise from intentional attacks, sabotage, counterfeit or unverified components, malicious hardware or software, falsified certificates, and vulnerabilities in digital and physical infrastructure. These mechanisms are directly relevant to military aviation because compromised electronics, maintenance data, or component provenance can affect airworthiness and mission systems. Evidence addressing military cyber-risk management, malicious insertions, component authentication, and attacks on critical nodes provides the strongest basis for this cluster (Ahn *et al.*, 2025; Panko, 2011; Anuat *et al.*, 2022).

Table 1. Supply-chain risk clusters relevant to military aviation

Risk cluster	Description	Authors
Physical/ cybersecurity	Refers to risks arising from intentional attacks, sabotage, counterfeiting, and digital or physical vulnerabilities that compromise the integrity of the military supply chain, including systems, equipment, and critical infrastructure	Ahn *et al.* (2025), Anuat *et al.* (2022), Brick (2016), Elvemo (2025), Gürtlich and Lampl (2022), Hui *et al.* (2022), Panko (2011), Sani Mohammed *et al.* (2023), Sani *et al.* (2022), Ti (2022), Urmston *et al.* (2024)
Strategic dependency	Involves risks associated with dependence on single suppliers, concentrated infrastructure, external funding, or foreign sources, which limits the autonomy, resilience, and responsiveness of the military aviation logistics chain	Ahn *et al.* (2025), Anuat *et al.* (2022), Armstrong (2002), Brick (2016), Cabrera *et al.* (2023), Chappell and Peck (2006), Dimitrova and Terziev (2015), Elvemo (2025), Gürtlich and Lampl (2022), Hui *et al.* (2022), Kleczka *et al.* (2024), Sani Mohammed *et al.* (2023), Ti (2022), Urmston *et al.* (2024)
Hostile external environment	Encompasses risks stemming from external and uncontrollable factors such as geopolitical conflicts, natural disasters, pandemics, sanctions, and economic crises that directly affect the stability and continuity of military logistics operations	Ahn *et al.* (2025), Anuat *et al.* (2022), Brick (2016), Cabrera *et al.* (2023), Dimitrova and Terziev (2015), Elvemo (2025), Funo *et al.* (2011), Gürtlich and Lampl (2022), Nagurney (2023), Sani Mohammed *et al.* (2023)
Inefficient management	Pertains to internal failures in administrative, operational, and logistical processes, including delays, disorganization, bureaucracy, lack of system integration, and absence of effective planning, all of which undermine the continuity and reliability of military supply operations	Ahn *et al.* (2025), Armstrong (2002), Brick (2016), Cabrera *et al.* (2023), Chappell and Peck (2006), Funo *et al.* (2011), Hui *et al.* (2022), Laudares *et al.* (2019), Panko (2011), Sani *et al.* (2022), Ti (2022), Urmston *et al.* (2024)

Source(s): Prepared by the authors

Evidence from broader military logistics is used only where the underlying mechanism is transferable. Attacks on supply lines and the vulnerability of fixed logistics facilities illustrate physical exposure, but they do not by themselves establish aviation-specific cyber risk (Sani *et al.*, 2022; Chappell and Peck, 2006). Accordingly, claims about military aviation cybersecurity are anchored primarily in studies addressing cyber risk, component integrity, traceability, and high-criticality defense systems, while broader operational examples are explicitly treated as contextual evidence.

Strategic dependency is characterized by excessive reliance on single suppliers, foreign sources, civilian infrastructure, or politically allocated work packages. In military aviation, specialized certification, low production volumes, and proprietary technology restrict substitution. Multinational programs may also distribute work according to sovereignty objectives and juste retour rather than solely according to cost or efficiency. The Eurofighter case illustrates a multi-tier collaborative network of more than 400 firms, while related evidence points to substantial non-domestic supplier dependence in European defense programs (Matthews and Al-Saadi, 2023; Kleczka *et al.*, 2024).

The absence of stockpiles, scarcity of reliable suppliers, dependence on external funding, technological obsolescence, and foreign acquisition of critical capabilities may reduce logistical autonomy (Ahn *et al.*, 2025; Dimitrova and Terziev, 2015; Hui *et al.*, 2022; Armstrong, 2002). Evidence concerning military blood supplies (Ti, 2022) is retained only as an analogy illustrating how limited reserve capacity and legal mobilization mechanisms can create strategic dependence; it is not treated as direct evidence about aircraft components. Reducing strategic dependency therefore requires selective diversification, lifecycle and obsolescence planning, secure allied arrangements, and, where operationally justified, domestic or regional capacity for mission-critical inputs.

The Hostile External Environment cluster includes geopolitical conflict, sanctions, natural disasters, pandemics, labor disruptions, economic volatility, and restrictions on transport routes or critical materials. Evidence from military food or medical supply chains illustrates how system-wide disruptions propagate through defense support networks, but it is not direct evidence of aviation-specific effects (Sani Mohammed *et al.*, 2023). For military aviation, the relevant implications arise when such events restrict certified components, semiconductors, maintenance inputs, energy, transport access, or industrial capacity (Nagurney, 2023; Ahn *et al.*, 2025).

Earthquakes, wildfires, labor strikes, semiconductor shortages, and financial instability exceed the direct control of military aviation organizations and may interact with geopolitical restrictions (Anuat *et al.*, 2022; Gürtlich and Lampl, 2022; Nagurney, 2023). Because aviation supply chains are global and platforms require long-term support, mitigation depends on geostrategic mapping, stress testing, alternative routes, supplier visibility, and multi-level contingency planning. The cluster therefore captures the external source of disruption, while the resilience clusters explain the organizational capabilities used to respond.

Inefficient management refers to internal fragilities such as a lack of planning, failures in information systems, bureaucratic delays, and logistical disorganization. Military aviation, which deals with complex systems and strict timelines, is particularly impacted by such bottlenecks. Issues such as delays in procurement processes (Laudares *et al.*, 2019), lack of integration between warehouse systems (Chappell and Peck, 2006), and insufficient risk management tools (Laudares *et al.*, 2019) directly affect aircraft availability and mission efficiency.

Other risks include the absence of quality and inventory monitoring (Funo *et al.*, 2011), outdated practices (Chappell and Peck, 2006), interoperability inefficiencies (Brick, 2016), and the difficulty in estimating the costs of war (Dimitrova and Terziev, 2015). This combination of internal failures leads to cascading effects across the supply chain. For instance, a shortage caused by a delayed procurement process may reduce the readiness or availability of entire units. Therefore, improving governance, digitizing processes, and investing in personnel training are essential measures to overcome the limitations posed by inefficient management.

4.2 Resilience mechanisms relevant to military aviation

The review identified 107 resilience-mechanism statements related to risk mitigation and operational continuity in defense and aerospace supply chains. These individual mechanisms were organized into five higher-order clusters: Structural Preparedness, Adaptive Response, Operational Intelligence, Strategic Cooperation, and Critical Sustainment. Robustness and flexibility are treated as complementary but distinct resilience capabilities: robustness emphasizes resistance through redundancy and protected capacity, whereas flexibility emphasizes reconfiguration and alternative courses of action. Table 2 presents the five clusters, which are interpreted as mutually reinforcing capabilities rather than isolated solutions (Ekström, 2025).

Structural Preparedness refers to the deliberate development of physical, technical, and organizational capabilities before a crisis. In military aviation, it includes strategic stocks of mission-critical items, supplier diversification, redundant capacity, energy resilience for air bases, standardization where airworthiness permits, and selective vertical integration

Table 2. Supply-chain resilience mechanisms relevant to military aviation

Resilience cluster	Description	Authors
Structural preparedness	A set of pre-established physical, technical, and organizational capabilities designed to ensure operational continuity during crises (e.g. stockpiling, redundancy, standardization, vertical integration)	Ahn *et al.* (2025), Anuat *et al.* (2022), Armstrong (2002), Brick (2016), Dimitrova and Terziev (2015), Elvemo (2025), Funo *et al.* (2011), Gürtlich and Lampl (2022), Hui *et al.* (2022), Kleczka *et al.* (2024), Nagurney (2023), Panko (2011), Sani Mohammed *et al.* (2023), Sani *et al.* (2022), Ti (2022), Urmston *et al.* (2024)
Adaptive response	The ability to respond swiftly and flexibly to disruptive events, including process reconfiguration, emergency mobilization, and responses to unforeseen threats	Ahn *et al.* (2025), Brick (2016), Cabrera *et al.* (2023), Elvemo (2025), Funo *et al.* (2011), Gürtlich and Lampl (2022), Hui *et al.* (2022), Kleczka *et al.* (2024), Nagurney (2023), Sani Mohammed *et al.* (2023), Sani *et al.* (2022), Ti (2022), Urmston *et al.* (2024)
Operational intelligence	The capacity to anticipate risks, simulate scenarios, monitor the supply chain, and make data-driven decisions using predictive tools and technologies	Ahn *et al.* (2025), Anuat *et al.* (2022), Armstrong (2002), Cabrera *et al.* (2023), Chappell and Peck (2006), Dimitrova and Terziev (2015), Elvemo (2025), Gürtlich and Lampl (2022), Hui *et al.* (2022), Kleczka *et al.* (2024), Panko (2011), Sani Mohammed *et al.* (2023), Ti (2022), Urmston *et al.* (2024)
Strategic cooperation	Coordination among internal and external actors (suppliers, allies, civil and military partners) to strengthen the supply chain based on trust, integration, and structured alliances	Armstrong (2002), Brick (2016), Cabrera *et al.* (2023), Elvemo (2025), Funo *et al.* (2011), Hui *et al.* (2022), Kleczka *et al.* (2024), Sani *et al.* (2022), Urmston *et al.* (2024)
Critical sustainment	Capabilities that preserve long-term aircraft availability and mission support when normal supply channels remain degraded, including maintenance and repair capacity, lifecycle and obsolescence management, protected stocks, technical data, and access to critical resources	Armstrong (2002), Brick (2016), Chappell and Peck (2006), Dimitrova and Terziev (2015), Nagurney (2023), Panko (2011), Ti (2022)

Source(s): Prepared by the authors

(Ahn *et al.*, 2025; Anuat *et al.*, 2022; Kleczka *et al.*, 2024). These measures increase robustness by reducing the likelihood that the failure of one supplier, facility, energy source, or component will immediately interrupt maintenance or flight operations.

Examples involving pre-stored medical supplies or historical campaign infrastructure illustrate the general value of reserves and protected logistics capacity, but they are treated as analogies rather than direct evidence about current aircraft sustainment (Sani Mohammed *et al.*, 2023; Armstrong, 2002). Aviation-specific application requires aligning inventories and backup capacity with component criticality, shelf life, certification, obsolescence, maintenance demand, and expected disruption duration. Structural preparedness therefore provides the protected baseline from which the other resilience mechanisms can operate.

Adaptive Response represents the ability to reconfigure operations rapidly when disruption occurs. In military aviation, this includes rerouting supplies, changing maintenance priorities, reallocating scarce components, mobilizing alternative suppliers, and responding to cyber or sabotage indicators. Artificial intelligence for anomaly detection, early-warning information, and command-and-control capabilities can shorten recognition and decision time (Ahn *et al.*, 2025; Elvemo, 2025). Defense examples from other sectors, such as the strategic reorganization of industrial assets, are used as transferable evidence of institutional adaptability rather than as aviation-specific proof (Kleczka *et al.*, 2024).

The operational value of adaptability lies not in decision speed alone but in the ability to implement feasible alternative courses of action without compromising safety and mission priorities. Flexible delivery, emergency mobilization rules, pre-authorized procedures, trained personnel, and access to civilian reserves may support reconfiguration under pressure (Sani *et al.*, 2022; Ti, 2022). Because these examples originate in different national and functional contexts, their transfer to military aviation depends on governance, airworthiness, security, and interoperability requirements.

Operational Intelligence concerns anticipation, continuous monitoring, scenario simulation, and real-time decision support. In military aviation, it includes digital twins, integrated enterprise systems, predictive models, supplier and inventory visibility, condition-monitoring data, and performance indicators that can reveal emerging shortages or maintenance constraints (Ahn *et al.*, 2025; Funo *et al.*, 2011; Anuat *et al.*, 2022; Urmston *et al.*, 2024). These tools strengthen decision quality when their data cover lower-tier suppliers and when technical, procurement, and operational organizations share a common picture.

Traceability and demand forecasting can affect both mission success and continuing airworthiness. Systems such as ICATS, which combine tracking with digital authentication, illustrate how component provenance and information integrity can reduce counterfeit risk (Panko, 2011). Operational intelligence therefore supports efficiency, but its defense-specific value lies in anticipating component unavailability, identifying cyber or quality anomalies, and prioritizing limited resources according to operational criticality.

Strategic Cooperation refers to coordination with national and international partners, including armed forces, procurement agencies, prime contractors, lower-tier suppliers, allies, and civilian infrastructure providers. Military aviation examples include NATO cooperation, outsourced logistics, co-development and co-production programs, and work-sharing arrangements such as juste retour (Brick, 2016; Kleczka *et al.*, 2024; Matthews and Al-Saadi, 2023). Cooperation can distribute risk and expand access to technology, maintenance capacity, transport, and stocks, but it may also generate bureaucracy, information silos, and politically constrained supplier choices.

Information sharing, trust-based supplier relationships, and coordinated governance can maintain logistical flows during scarcity or conflict (Cabrera *et al.*, 2023; Urmston *et al.*, 2024). Historical air-transport operations are retained only as illustrations of the enduring coordination mechanism, not as evidence that past organizational arrangements are directly transferable to contemporary digital aviation supply chains (Armstrong, 2002). Strategic cooperation is therefore resilience-enhancing when responsibilities, data access, security, incentives, and emergency decision rights are defined before disruption.

Critical Sustainment concerns the capacity to preserve aircraft availability and continuing airworthiness when normal supply channels remain degraded for an extended period. It includes maintenance and repair capability, lifecycle and obsolescence management, assured access to critical components and technical data, protected stocks, qualified personnel, and the capacity to regenerate or substitute support resources. This cluster is distinctive in military aviation because platforms remain in service for decades, certified components may have few substitutes, and multinational industrial arrangements may constrain rapid replacement (Matthews and Al-Saadi, 2023; Ekström, 2025).

Critical Sustainment connects the other four resilience clusters over time. Structural Preparedness establishes stocks and protected capacity; Operational Intelligence detects shortages, failures, and obsolescence; Adaptive Response reallocates resources and maintenance priorities; and Strategic Cooperation provides access to allied production, repair, transport, and technical support. The cluster therefore captures the difference between recovering from an initial shock and maintaining a viable support system throughout a prolonged crisis.

5. Discussion

The findings provide a structured but preliminary taxonomy of four risk clusters and five clusters of resilience mechanisms relevant to military aviation supply chains. The contribution is not a claim that all military aviation programs face the same risk profile; rather, it organizes recurrent mechanisms that affect industrial production, maintenance, and sustainment across different national and organizational settings. Strategic dependency, inefficient management, cyber and component-integrity threats, and hostile external conditions can converge to reduce aircraft availability. Structural Preparedness, Adaptive Response, Operational Intelligence, Strategic Cooperation, and Critical Sustainment describe complementary capabilities for managing those vulnerabilities.

The taxonomy aligns with the broader resilience literature on redundancy, diversification, flexibility, readiness, response, and recovery (Kleindorfer and Saad, 2005; Han *et al.*, 2020). It also reflects defense-specific findings that military supply chains share several commercial vulnerabilities while facing distinctive governance, preparedness, sovereignty, and operational requirements (Lucas *et al.*, 2024; Ekström, 2025). Robustness and flexibility should therefore not be treated as synonyms. Robustness protects capacity against expected stress through stocks, redundancy, and hardened infrastructure; flexibility enables the supply chain to reconfigure when the original plan is no longer viable. Military aviation requires both, together with long-term sustainment.

The main theoretical contribution is the integration of risk sources with resilience capabilities in a sector where airworthiness, long platform lifecycles, technological obsolescence, multinational industrial structures, and operational readiness interact. The practical contribution is a diagnostic structure for defense managers: risk assessment should distinguish external shocks from internal management failures and deliberate threats, while resilience planning should connect stockpiles and capacity, information, reconfiguration, cooperation, and sustainment. In particular, Critical Sustainment extends the analysis beyond immediate response by emphasizing repair capability, maintenance continuity, technical workforce, obsolescence management, and access to mission-critical parts over prolonged disruptions.

The limitations affect both completeness and validity. Scopus and WoS overlap substantially and do not systematically cover grey literature, defense white papers, technical reports, NATO publications, or specialized repositories. Title-based queries favor precision over recall, the full-text requirement introduces availability bias, and a corpus of 20 studies cannot be assumed to represent the entire field. The global, mechanism-oriented synthesis also combines heterogeneous countries, eras, and functional contexts; civilian, historical, food, medical, maritime, and broader military evidence is therefore used only when the transfer mechanism is made explicit. Finally, the study reports thematic and semantic validation but no statistical intercoder reliability or quantitative effect estimates. The clusters should be regarded as an analytically grounded framework that requires testing with expanded searches, independent coding, and empirical military aviation cases.

6. Conclusion

This systematic review organizes supply-chain risks and resilience mechanisms identified in the defense and aerospace literature according to their relevance to the industrial, maintenance, and sustainment systems supporting military aviation. The taxonomy comprises four risk clusters—Physical/Cybersecurity, Strategic Dependency, Hostile External Environment, and Inefficient Management—and five higher-order clusters of resilience mechanisms—Structural Preparedness, Adaptive Response, Operational Intelligence, Strategic Cooperation, and Critical Sustainment. The categories clarify how disruptions can affect aircraft availability and how different capabilities contribute to preparation, response, recovery, and continued mission support.

The analysis indicates that risks interact rather than occur in isolation. A geopolitical shock may expose foreign-supplier dependence; a component shortage may be amplified by poor inventory visibility or delayed procurement; and a cyber or quality event may require both technical containment and allied industrial support. Resilience therefore depends on combining robustness, flexibility, information, cooperation, and long-term sustainment rather than relying on a single universal practice.

For policymakers and defense managers, the framework can support structured diagnosis and prioritization. Strategic stocks and redundant capacity should be aligned with component criticality; predictive systems should cover lower-tier suppliers and maintenance demand; emergency reconfiguration should be governed in advance; and international cooperation should include clear arrangements for information, production, repair, and access to critical items. Critical Sustainment is especially important because military aircraft remain in service for decades and must remain airworthy throughout prolonged disruptions.

The evidence base nevertheless remains limited by the two databases, title-field search strategy, full-text criterion, small corpus, heterogeneous national contexts, and incomplete coverage of grey literature and practitioner sources. Because the search did not include aviation-specific terms, it should not be interpreted as providing exhaustive coverage of the military-aviation literature. These constraints mean that the taxonomy is preliminary and that its relevance may vary across countries, alliances, platform types, and stages of the aircraft lifecycle.

Future studies should broaden the search using aviation-specific terms, specialized defense and aviation repositories, and grey literature, publish the coding matrix and codebook, use independent coders, and test the clusters through comparative cases, surveys, and quantitative models. Research should also examine how unmanned systems, defense electronics, open architectures, co-production, and multilevel alliance governance alter the balance between efficiency, sovereignty, readiness, and sustainment.

References

Achmadi, B. and Sutawidjaya, A.H. (2024), "The role and dynamics of actor relations in implementing defense industry-based policies: a comparative study of Indonesia and Brazil", *Journal of Ecohumanism*, Vol. 4 No. 1, pp. 1-11, doi: 10.62754/joe.v4i1.4216.

Ahn, J.K., Cho, K., Seo, K., Kim, H.-J. and Kim, S. (2025), "Comprehensive analysis and recommendation of supply chain risk management framework for the military domain", *IEEE Access*, Vol. 13, pp. 96813-96833, doi: 10.1109/ACCESS.2025.3573515.

Anuat, E., Van Bossuyt, D.L. and Pollman, A. (2022), "Energy resilience impact of supply chain network disruption to military microgrids", *Infrastructures*, Vol. 7 No. 1, p. 4, doi: 10.3390/infrastructures7010004.

Armstrong, D.A. and Kane, T.M. (2002), "Review of military logistics and strategic performance, by T.M. Kane", *The Journal of Military History*, Vol. 66 No. 3, pp. 921-922, doi: 10.2307/3093438.

Axios (2025), "Lockheed's DePietro: there's a 'speed mismatch' that needs fixing", 11 June, available at: https://www.axios.com/2025/06/11/joe-depietro-lockheed-martin-interview (accessed 25 August 2026).

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101, doi: 10.1191/1478088706qp063oa.

Brick, E.S. (2016), "Logística de defesa: uma subárea do conhecimento de importância estratégica para as ciências de gestão", *Revista Brasileira de Gestão e Desenvolvimento Regional*, Vol. 12 No. 2, pp. 301-331.

Cabrera, B., Santa, R., Tegethoff, T., Morante, D. and Ferrer, M. (2023), "Supply chain resilience in the Colombian defense sector before and during the COVID-19 pandemic: a comparative study", edited by Grima, S., *PLoS One*, Vol. 18 No. 3, e0282793, doi: 10.1371/journal.pone.0282793.

Chappell, A. and Peck, H. (2006), "Risk management in military supply chains: is there a role for six sigma?", *International Journal of Logistics Research and Applications*, Vol. 9 No. 3, pp. 253-267, doi: 10.1080/13675560600859276.

Dimitrova, S. and Terziev, V. (2015), "Financial provisioning - basis of strategic decisions of themanagement of resources for security and defence", *International Conference Knowledge-Based Organization*, Vol. 21 No. 2, Walter de Gruyter GmbH, pp. 294-299, doi: 10.1515/kbo-2015-0050.

Ekström, T. (2025), "Supply chain resilience – an empirical exploration of barriers and enablers in military settings", *Scandinavian Journal of Military Studies*, Vol. 8 No. 1, pp. 119-136, doi: 10.31374/sjms.350.

Ekström, T., Hilletofth, P. and Skoglund, P. (2020), "Differentiation strategies for defence supply chain design", *Journal of Defense Analytics and Logistics*, Vol. 4 No. 2, pp. 183-202, doi: 10.1108/JDAL-06-2020-0011.

Elvemo, L. (2025), "Supply chain resilience in military operations: a case study exploring command and control", *Scandinavian Journal of Military Studies*, Vol. 8 No. 1, pp. 178-199, doi: 10.31374/sjms.356.

Feldman, R. and Sanger, J. (2006), *The Text Mining Handbook*, Cambridge University Press, doi: 10.1017/CBO9780511546914.

Funo, K.A., Muniz, J., Jr, Marins, F.A.S. and Salomon, V.A.P. (2011), "Supply chain risk management: an exploratory research in Brazilian aerospace industry", *International Journal of Value Chain Management*, Vol. 5 Nos 3/4, pp. 265-280, doi: 10.1504/IJVCM.2011.043230.

Grimmer, J. and Stewart, B.M. (2013), "Text as data: the promise and pitfalls of automatic content analysis methods for political texts", *Political Analysis*, Vol. 21 No. 3, pp. 267-297, doi: 10.1093/pan/mps028.

Guest, G., MacQueen, K.M. and Namey, E.E. (2012), *Applied Thematic Analysis*, SAGE Publications, Thousand Oaks, CA, doi: 10.4135/9781483384436.

Gürtlich, G. and Lampl, S. (2022), "Resilience and military supply chain management", in Kummer, S., Wakolbinger, T., Novoszel, L. and Geske, A.M. (Eds), *Supply Chain Resilience, Springer Series in Supply Chain Management*, Springer, Cham, Vol. 17, pp. 337-352, doi: 10.1007/978-3-030-95401-7_29.

Han, Y., Chong, W.K. and Li, D. (2020), "A systematic literature review of the capabilities and performance metrics of supply chain resilience", *International Journal of Production Research*, Vol. 58 No. 15, pp. 4541-4566, doi: 10.1080/00207543.2020.1785034.

Hui, X., Li, K., Wang, C., Zhang, C. and Gu, Z. (2022), "Risk management of aerospace stand-alone device supply chain", *2022 International Conference on Industrial IoT, Big Data and Supply Chain (IIoTBDSC)*, IEEE, pp. 272-277, doi: 10.1109/IIoTBDSC57192.2022.00057.

Ivanov, D. and Dolgui, A. (2020), "Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. A position paper motivated by COVID-19 outbreak", *International Journal of Production Research*, Vol. 58 No. 10, pp. 2904-2915, doi: 10.1080/00207543.2020.1750727.

Kleczka, M., Vandercruysse, L., Buts, C. and Du Bois, C. (2024), "The spectrum of strategic autonomy in EU defence supply chains", *Defence and Peace Economics*, Vol. 35 No. 4, pp. 427-447, doi: 10.1080/10242694.2023.2180588.

Kleindorfer, P.R. and Saad, G.H. (2005), "Managing disruption risks in supply chains", *Production and Operations Management*, Vol. 14 No. 1, pp. 53-68, doi: 10.1111/j.1937-5956.2005.tb00009.x.

Krippendorff, K. (2019), *Content Analysis: An Introduction to its Methodology*, 4th ed., SAGE Publications, Thousand Oaks, CA, doi: 10.4135/9781071878781.

Laudares, A.D.C., Ricco, M.F.F. and Silveira dos Santos, R.A. (2019), "When does it end? Monte Carlo simulation applied to risk management in defense logistics' procurement processes", *Brazilian Journal of Operations and Production Management*, Vol. 16 No. 1, pp. 149-156, doi: 10.14488/BJOPM.2019.v16.n1.a14.

Lucas, R., Ekström, T., Fusaro, P., Hastings Roer, E. and Retter, L. (2024), *Toward Defense Supply Chain Disruption Management: A Research Agenda for Defense Supply Chain Resilience*, RAND Corporation, Santa Monica, CA, doi: 10.7249/RRA2504-1.

Matthews, R. and Al-Saadi, R. (2023), "Organisational complexity of the eurofighter Typhoon collaborative supply chain", *Defence and Peace Economics*, Vol. 34 No. 2, pp. 228-243, doi: 10.1080/10242694.2021.1987022.

Mejino-Lopez, J. and Wolff, G.B. (2025), "Boosting the European defence industry in a hostile world", *Intereconomics*, Vol. 60 No. 1, pp. 34-39, doi: 10.2478/ie-2025-0007.

Moher, D., Liberati, A., Tetzlaff, J. and Altman, D.G. (2009), "Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement", *PLoS Medicine*, Vol. 6 No. 7, e1000097, doi: 10.1371/journal.pmed.1000097.

Mongeon, P. and Paul-Hus, A. (2016), "The journal coverage of Web of Science and Scopus: a comparative analysis", *Scientometrics*, Vol. 106 No. 1, pp. 213-228, doi: 10.1007/s11192-015-1765-5.

Nagurney, A. (2023), "Defense-critical supply chain networks and risk management with the inclusion of labor: dynamics and quantification of performance and the ranking of nodes and links", *Springer Optimization and Its Applications*, Vol. 205, pp. 39-57, doi: 10.1007/978-3-031-39542-0_3.

Ng, I.C.L., Maull, R. and Yip, N. (2009), "Outcome-based contracts as a driver for systems thinking and service-dominant logic in service science: evidence from the defence industry", *European Management Journal*, Vol. 27 No. 6, pp. 377-387, doi: 10.1016/j.emj.2009.05.002.

Oksuz Gurdal, B. and Testik, O.M. (2025), "A framework for product life cycle management based digital twin implementation in the aerospace industry", *Applied Stochastic Models in Business and Industry*, Vol. 41 No. 2, e70001, doi: 10.1002/asmb.70001.

Panko, R.R. (2011), "Identity content assurance and tracking systems (ICATSs) for military supply chain risk management: a preliminary design", *2011 44th Hawaii International Conference on System Sciences*, pp. 1-6, doi: 10.1109/HICSS.2011.232.

Pettit, T.J., Fiksel, J. and Croxton, K.L. (2010), "Ensuring supply chain resilience: development of a conceptual framework", *Journal of Business Logistics*, Vol. 31 No. 1, pp. 1-21, doi: 10.1002/j.2158-1592.2010.tb00125.x.

Ponomarov, S.Y. and Holcomb, M.C. (2009), "Understanding the concept of supply chain resilience", *International Journal of Logistics Management*, Vol. 20 No. 1, pp. 124-143, doi: 10.1108/09574090910954873.

Reuters (2025a), "EU lending arm triples defence loan plan to 3 billion euros", 11 June, available at: https://www.reuters.com/business/finance/eu-lending-arm-triples-defence-loan-plan-3-billion-euros-2025-06-11/ (accessed 15 June 2025).

Reuters (2025b), "Paris airshow set for new jet orders despite conflict, tariff gloom", available at: https://www.reuters.com/business/aerospace-defense/paris-airshow-set-new-jet-orders-despite-conflict-tariff-gloom-2025-06-12/ (accessed 15 June 2025).

Sani, S., Schaefer, D. and Milisavljevic-Syed, J. (2022), "Strategies for achieving pre-emptive resilience in military supply chains", *Procedia CIRP*, Vol. 107, pp. 1526-1532, doi: 10.1016/j.procir.2022.05.186.

Sani Mohammed, S., Schaefer, D. and Milisavljevic-Syed, J. (2023), "Towards pre-emptive resilience in military supply chains: a compromise decision support model-based approach", *Production and Manufacturing Research*, Vol. 11 No. 1, 2220768, doi: 10.1080/21693277.2023.2220768.

Tang, C.S. (2006), "Perspectives in supply chain risk management", *International Journal of Production Economics*, Vol. 103 No. 2, pp. 451-488, doi: 10.1016/j.ijpe.2005.12.006.

Ti, C.R. (2022), "The strategic vulnerability of NATO blood supply logistics: a case study of Estonian national defence", *Defense and Security Analysis*, Vol. 38 No. 4, pp. 369-388, doi: 10.1080/14751798.2022.2076343.

Tranfield, D., Denyer, D. and Smart, P. (2003), "Towards a methodology for developing evidence-informed management knowledge by means of systematic review", *British Journal of Management*, Vol. 14 No. 3, pp. 207-222, doi: 10.1111/1467-8551.00375.

Turkina, E., Van Assche, A. and Kali, R. (2016), "Structure and evolution of global cluster networks: evidence from the aerospace industry", *Journal of Economic Geography,* Vol. 16 No. 6, pp. 1211-1234, doi: 10.1093/jeg/lbw020.

Urmston, A., Song, D. and Lyons, A. (2024), "The development of risk assessments and supplier resilience models for military industrial supply chains considering rare disruptions", *Logistics*, Vol. 8 No. 2, p. 57, doi: 10.3390/logistics8020057.

U.S. Government Accountability Office (2013), *Defense Acquisitions: DOD Efforts to Adopt Open Systems for its Unmanned Aircraft Systems Have Progressed Slowly, GAO-13-651*, Washington, DC, available at: https://www.gao.gov/products/gao-13-651 (accessed 25 August 2026).

Corresponding author
Rui Fernando Correia Ferreira can be contacted at: ruifernandof@gmail.com