Scientific Research Publishing

Journal of Information Security, 2025, 16(1), 131-148
https://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Cybersecurity Challenges and Technological Integration in Military Supply Chain 4.0

Nathalie Essi Afefa Takpah*, Victor Nosakhare Oriakhi

Department of Procurement Logistics and Supply Chain Management, University of Salford, Manchester, UK
Email: *nathytakpah@gmail.com

How to cite this paper: Takpah, N.E.A. and Oriakhi, V.N. (2025) Cybersecurity Challenges and Technological Integration in Military Supply Chain 4.0. *Journal of Information Security*, **16**, 131-148.
https://doi.org/10.4236/jis.2025.161007

Received: November 11, 2024
Accepted: December 28, 2024
Published: December 31, 2024

Abstract

The concept of Supply Chain 4.0 represents a transformative phase in supply chain management through advanced digital technologies like IoT, AI, blockchain, and cyber-physical systems. While these innovations deliver operational improvements, the heightened interconnectivity introduces significant cybersecurity challenges, particularly within military logistics, where mission-critical operations and life-safety concerns are paramount. This paper examines these unique cybersecurity requirements, focusing on advanced persistent threats, supply chain poisoning, and data breaches that could compromise sensitive operations. The study proposes a hybrid cybersecurity framework tailored to military logistics, integrating resilience, redundancy, and cross-jurisdictional security measures. Real-world applicability is validated through simulations, offering strategies for securing supply chains while balancing security, efficiency, and flexibility.

Keywords

Cybersecurity, Supply Chain, IoT, BlockChain, Artificial Intelligence

1. Introduction

1.1. Evolution of Supply Chain 4.0 and Its Military Implications

Military supply chains differ fundamentally from civilian counterparts, prioritizing resilience, flexibility, and mission assurance over cost-efficiency and streamlined operations. For example, IoT sensors can track critical military equipment in real time, but they also introduce vulnerabilities to advanced persistent threats (APTs), which civilian supply chains may not face. The dynamic threat landscape in military logistics requires robust cybersecurity frameworks that account for life-safety risks, operational unpredictability, and adversarial intent. These challenges amplify the need for mission-critical technologies that enhance responsiveness while mitigating

vulnerabilities.

Supply Chain 4.0 epitomizes the integration of physical and digital assets within a supply chain network, utilizing Industry 4.0 technologies to enable smart, interconnected logistics systems that operate independently of time or place constraints [1]. This integration facilitates a vast array of functions—ranging from automated inventory management to real-time logistics tracking and predictive demand analytics—that streamline supply chain efficiency and adaptability [2]. The key components of Supply Chain 4.0, as illustrated in **Figure 1**, include advanced IoT devices, blockchain-based networks, AI-driven analytics, and cloud-based infrastructure, each playing a critical role in optimizing logistics processes and enabling real-time decision-making. However, the shift from traditional supply chains to digitalized, networked systems introduces unique cybersecurity risks, as the increasing reliance on IoT, blockchain, and AI creates new vulnerabilities within the supply chain infrastructure [3].

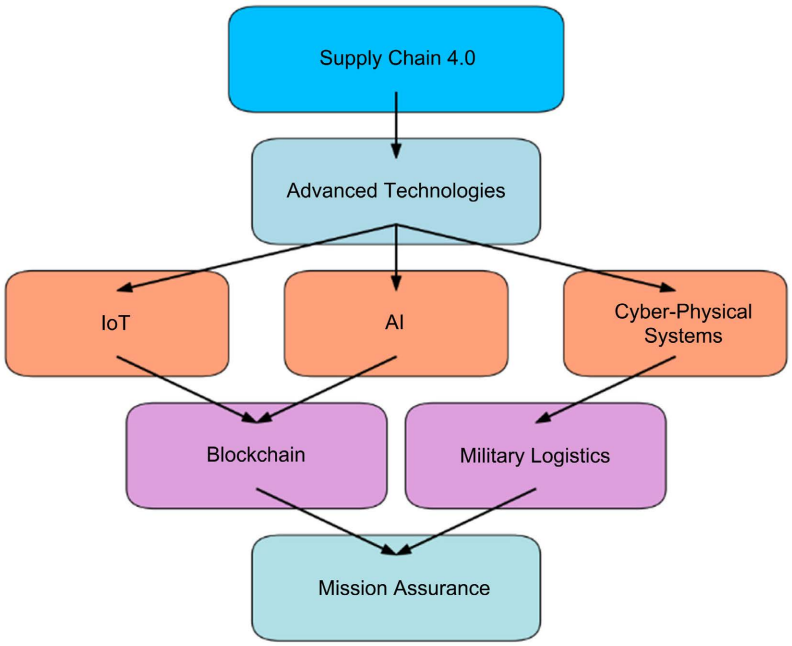

Figure 1. Components of supply chain 4.0.

Military supply chains, given their strategic importance, differ significantly from civilian applications in both operational focus and security needs. Civilian supply chains typically prioritize efficiency and cost-effectiveness, while military logistics are centered on resilience, flexibility, and mission assurance. The cyber-physical systems (CPS) and IoT devices employed in Supply Chain 4.0 enhance responsiveness and streamline logistics processes in military operations, yet they also open up critical vulnerabilities that adversaries can exploit to disrupt operations or compromise sensitive data [4].

1.2. Increasing Cybersecurity Threats in Military Supply Chains

The unique vulnerabilities posed by military supply chains stem from the high

connectivity of Supply Chain 4.0 systems, which can expose these networks to Advanced Persistent Threats (APT) and other sophisticated cyber-attacks. Military supply chains manage the flow of life-critical resources, equipment, and personnel essential for mission success, making cybersecurity a central consideration [5]. While civilian supply chains face similar risks, the consequences of breaches in military logistics extend beyond financial loss, with the potential to endanger human lives and national security. Consequently, military supply chains require cybersecurity strategies that account for both operational continuity and the dynamic threat landscape [6].

2. Literature Review

2.1. Defining Supply Chain 4.0 and Its Relevance to Military Logistics

Supply Chain 4.0 represents the digital transformation of traditional supply chains through the integration of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), cyber-physical systems, and blockchain [1] [2]. These technologies offer various enhancements, including real-time data analytics, automation, and autonomous decision-making capabilities, which improve supply chain efficiency, responsiveness, and accuracy [7]. The concept originated from Industry 4.0, which focuses on smart manufacturing, automation, and the application of interconnected systems, allowing organizations to shift from isolated operations to integrated, end-to-end digital networks [8]. In this context, Supply Chain 4.0 is a pivotal transformation, redefining how materials, goods, and information are managed and exchanged across the supply chain continuum.

For the military sector, Supply Chain 4.0 is essential not only for optimizing logistical functions but also for ensuring mission assurance and operational readiness. Military supply chains handle the movement of critical resources, from weapon systems to essential goods for personnel, under conditions that often require rapid adaptability and resilience [9]. Unlike civilian supply chains, which prioritize cost-efficiency and streamlined operations, military supply chains emphasize flexibility, security, and redundancy to support dynamic operational needs [10]. By integrating IoT-enabled sensors, AI-driven analytics, and blockchain-based traceability, military logistics can enhance inventory accuracy, streamline processes, and gain heightened visibility over supply routes [11]. Such advancements allow military organizations to better manage unpredictable demand and complex logistics in volatile environments [12].

The deployment of Supply Chain 4.0 technologies within military logistics also fosters improved interoperability between allied nations. Many military operations today rely on partnerships and coalitions, making it imperative for supply chains to function seamlessly across different systems and jurisdictions. Standardization and interoperability enabled by Supply Chain 4.0 facilitate collaboration between allied forces, enhancing logistical coordination and reducing bottlenecks in resource delivery [13]. Furthermore, IoT and AI solutions provide predictive

analytics capabilities, which are invaluable for anticipating supply shortages, maintaining inventory balance, and forecasting logistical needs [4].

2.2. Cybersecurity Threats in Supply Chain 4.0

The digital transformation of supply chains introduces new vulnerabilities as organizations become increasingly dependent on interconnected digital systems. Cybersecurity threats such as Advanced Persistent Threats (APTs), data breaches, and ransomware attacks are prevalent risks associated with the high connectivity of Supply Chain 4.0 networks [14]. APTs, for example, allow attackers to infiltrate supply chain systems over extended periods, gathering intelligence and potentially disrupting operations without immediate detection [15]. The increasing use of IoT devices, which often lack robust security features, further heightens these risks by expanding the attack surface and creating entry points for cyber intrusions [16].

Supply chain poisoning is a particularly concerning risk in military contexts, where adversaries may compromise critical components at various stages of the supply chain. These compromised components can infiltrate secure military environments, potentially compromising sensitive data and operational integrity [17]. Additionally, the integration of blockchain and AI within Supply Chain 4.0, while offering enhanced data transparency and predictive capabilities, introduces new cybersecurity challenges. Blockchain technology, for instance, is susceptible to specific attacks such as the "51% attack," where attackers can take control of the blockchain network, compromising data integrity [18]. AI systems, particularly those deployed in autonomous logistics operations, are vulnerable to adversarial attacks that can manipulate data inputs, leading to erroneous decision-making or disruptions in automated processes [19].

The reliance on digital and networked systems also introduces challenges related to information confidentiality and system resilience. The concept of "security through obscurity," where military networks rely on limited exposure to public networks, is no longer sufficient in the age of interconnected supply chains [20]. In response, military organizations are adopting robust cybersecurity frameworks that incorporate risk management principles to proactively identify and mitigate vulnerabilities across supply chain operations. These frameworks are vital in ensuring that military logistics remain secure, resilient, and responsive to emerging threats in both cyber and physical domains [4] [21].

2.3. Risk Management Models for Military Supply Chains

The development of military-specific cybersecurity standards requires an adaptation of existing frameworks like NIST and ISO 27001. These frameworks provide a robust foundation but must be augmented to address the distinct requirements of military operations. For example, military logistics demand real-time threat intelligence, interoperability with allied systems, and stringent data protection measures. Enhanced redundancy planning, such as the establishment of backup supply nodes and alternative routes, ensures continuity even during critical infrastruc-

ture disruptions. These additional layers, tailored to military contexts, strengthen the ability to counter cyber threats without compromising mission-critical operations.

Adapting Civilian Frameworks for Military Applications

Effective risk management is vital for mitigating cybersecurity risks inherent in Supply Chain 4.0. Civilian frameworks like the Cyber Supply Chain Risk Management (CSCRM) model emphasize a comprehensive lifecycle approach, assessing vulnerabilities from design to deployment [9]. While these models offer valuable insights, military logistics require enhancements such as mission assurance measures and rapid incident response capabilities to address life-critical consequences of supply chain disruptions.

The **Cyber Kill Chain**, developed by Lockheed Martin, maps the stages of a cyber-attack, enabling organizations to detect and disrupt threats [22]. However, its focus on static, predictable threat environments limits its effectiveness in military contexts. Adapting the Cyber Kill Chain for military use involves incorporating real-time monitoring, adaptive defense mechanisms, and cross-jurisdictional protocols to handle dynamic adversarial conditions [4].

Similarly, the **Supply Chain Operations Reference (SCOR) model** offers a structured process for optimizing supply chain performance across five key areas: plan, source, make, deliver, and return [23]. While valuable in achieving efficiency and quality, the SCOR model requires modifications to address military-specific cybersecurity needs. These include resilience measures to protect against cyber incidents and ensure continuity of mission-critical supply chains during hostile events.

Military-Specific Resilience Frameworks

The **Pettit, Fiksel, and Croxton Resilience Framework** highlights capabilities like flexibility, redundancy, and recovery, which are critical for military supply chains operating in volatile and adversarial environments. For instance, diversified sourcing, real-time monitoring, and contingency planning safeguard against disruptions caused by cyber or physical threats [24].

Military supply chains must incorporate a hybrid approach that combines the process efficiency of civilian frameworks with military-specific strategies. This hybrid model integrates elements like:

1) Redundancy Planning: Backup suppliers, alternative distribution channels, and buffer inventories.

2) Proactive Risk Assessment: Identifying potential vulnerabilities across all stages of the supply chain lifecycle.

3) Real-Time Adaptability: Rapid detection and mitigation of threats using AI-driven analytics and IoT-enabled monitoring.

For example, a tailored adaptation of the Cyber Kill Chain could integrate predictive analytics for early warning systems, allowing military logisticians to counter Advanced Persistent Threats (APTs) before they escalate. Similarly, the SCOR model can be enhanced with real-time threat intelligence systems to maintain sup-

ply chain integrity during cyber events.

Contributions and Future Directions

This study extends civilian risk management frameworks to meet the operational demands of military logistics, addressing gaps in adaptability, resilience, and mission assurance. By integrating redundancy planning, cross-functional interoperability, and advanced cybersecurity protocols, the proposed hybrid approach ensures that military supply chains remain secure and operational even in the face of evolving cyber threats. Future research should explore additional applications of AI and blockchain to further enhance resilience and develop cross-jurisdictional standards for allied operations.

2.4. Technology-Specific Cybersecurity Solutions for Military Supply Chain 4.0

Military logistics increasingly rely on cutting-edge technologies like IoT, blockchain, and AI for real-time monitoring, predictive analytics, and asset tracking. These technologies enhance supply chain efficiency and resilience but also introduce unique cybersecurity challenges that must be addressed proactively.

IoT in Military Logistics

IoT-enabled devices offer significant benefits, such as predictive maintenance, which ensures operational readiness by identifying potential equipment failures before they occur. For instance, real-time monitoring of supply chain nodes can detect and alert logisticians about irregularities in transport routes or environmental conditions. However, IoT devices often lack robust security protocols, leaving them vulnerable to attacks like device hijacking, data manipulation, and signal spoofing [25]. Securing IoT networks in military contexts involves implementing encryption, network segmentation, and real-time threat monitoring to prevent unauthorized access and ensure data integrity [26].

Blockchain for Transparency and Traceability

Blockchain provides a decentralized, tamper-resistant ledger that records every transaction within the supply chain. This enhances traceability and transparency, making it invaluable for military logistics where counterfeit goods or supply chain poisoning pose critical risks. For example, blockchain can track the lifecycle of components from manufacturing to deployment, ensuring authenticity and reducing vulnerabilities [18]. However, blockchain's reliance on consensus mechanisms introduces challenges, such as the risk of a 51% attack where malicious actors gain majority control over the network. To address these concerns, military applications should adopt permissioned blockchain systems with multi-layered authentication and advanced encryption protocols tailored to sensitive operational needs.

AI and Machine Learning for Predictive Insights

AI-driven technologies enable predictive analytics, demand forecasting, and optimization of resource allocation in Supply Chain 4.0. These tools can identify patterns in logistics data, anticipate disruptions, and streamline decision-making

processes. However, adversarial attacks on AI algorithms pose a serious risk to military logistics, as manipulated data inputs can lead to incorrect conclusions or system failures [27]. To mitigate these threats, military supply chains must implement rigorous testing, frequent updates to machine learning models, and comprehensive verification and validation processes that account for adversarial scenarios.

Cyber-Physical Systems (CPS) for Operational Control

Cyber-physical systems (CPS) integrate digital and physical processes, enabling remote control and monitoring of military supply chain assets. These systems play a critical role in maintaining operational readiness and resilience. However, CPS are vulnerable to cross-domain threats such as GPS spoofing, signal jamming, and physical tampering [28]. Effective mitigation strategies include deploying multi-layered defense mechanisms, real-time anomaly detection, and redundancy planning. These measures ensure both the digital and physical components of CPS are safeguarded against disruptions.

By integrating these technologies with tailored cybersecurity solutions, military logistics can benefit from the operational efficiencies of Supply Chain 4.0 while maintaining resilience and mission assurance in the face of evolving cyber threats.

3. Methodology

3.1. Research Design and Data Collection

This research employs a systematic and multi-layered approach to investigate cybersecurity challenges within Supply Chain 4.0, with an emphasis on military logistics. A comprehensive research design was developed, integrating a systematic literature review and comparative analysis to provide a robust foundation for understanding and addressing cybersecurity issues specific to military supply chains.

3.1.1. Systematic Literature Review (SLR)

A systematic literature review (SLR) was conducted to collate and synthesize current research on cybersecurity threats, technological integrations, and risk management frameworks applicable to Supply Chain 4.0. The literature review included a broad range of sources, encompassing academic journals, industry white papers, government reports, and defense-specific publications. This phase aimed to establish a foundation of existing knowledge while identifying prominent cybersecurity vulnerabilities and technological dependencies within Supply Chain 4.0.

To ensure rigor and relevance in the review, specific search criteria and inclusion parameters were established:

- **Databases Used**: IEEE Xplore, ScienceDirect, JSTOR, Scopus, and defense-focused research repositories.
- **Search Terms**: Keywords such as "Supply Chain 4.0," "cybersecurity in supply chains," "military logistics security," "IoT in military supply chains," and "cyber-physical systems."

- **Inclusion Criteria**: Articles and reports from 2010 onwards to capture the most recent technological advancements, with a focus on works discussing both civilian and military supply chain vulnerabilities.

A total of 150 sources were initially identified, which were screened based on relevance and academic rigor, narrowing the dataset to 85 peer-reviewed articles and industry reports. Each source was analyzed for specific cybersecurity threats, technological challenges, and risk management practices within Supply Chain 4.0.

3.1.2. Comparative Analysis

To understand the unique cybersecurity demands of military supply chains, a comparative analysis was conducted between civilian and military risk frameworks. The analysis aimed to assess the adaptability of civilian cybersecurity models to military settings, identifying both commonalities and divergences. Civilian frameworks, including the Cyber Supply Chain Risk Management (CSCRM) and the Cyber Kill Chain, were examined for their applicability in defense scenarios. Additionally, military-focused frameworks, such as mission assurance models and specific military cybersecurity protocols, were assessed to highlight areas where civilian and military frameworks align or diverge.

This phase provided insights into the limitations of civilian models when applied to military logistics, particularly in scenarios requiring high resilience, real-time response, and mission assurance capabilities. The comparative approach aimed to uncover any adaptation needs or novel strategies essential for securing military-specific logistics.

3.2. Data Analysis and Thematic Categorization

A structured thematic analysis was employed to identify, categorize, and interpret key themes related to cybersecurity vulnerabilities and risk management strategies in military logistics. This process facilitated a deeper understanding of how different technologies within Supply Chain 4.0 impact cybersecurity, and how civilian models could be adapted to military contexts.

3.2.1. Thematic Coding and Categorization

Using NVivo software, thematic coding was applied to the data collected from the literature review, allowing for the systematic categorization of recurring concepts, risks, and solutions. Initial coding generated a preliminary set of themes, which were then refined into three main categories:

- **Technological Threats and Cyber Vulnerabilities:** This category focused on the inherent risks associated with IoT, blockchain, AI, and cyber-physical systems within Supply Chain 4.0. Specific vulnerabilities, such as IoT device exploitation and blockchain data integrity risks, were highlighted to show how each technology contributes to the overall cybersecurity landscape.
- **Risk Management Frameworks:** Here, both civilian and military cybersecurity models were analyzed to determine their effectiveness in mitigating identified vulnerabilities. The categorization enabled a comparative assessment of

frameworks like CSCRM and the Cyber Kill Chain, emphasizing areas needing adaptation for military use.

- **Military-Specific Needs and Gaps:** This theme addressed the unique requirements of military supply chains, such as mission assurance, rapid incident response, and cross-jurisdictional interoperability. It identified gaps in existing frameworks where additional layers of security or resilience measures may be necessary for defense applications.

These thematic categories provided a structured lens through which the research could evaluate the current state of cybersecurity in military supply chains, as well as the applicability and limitations of existing risk management models.

3.2.2. Synthesis of Findings

After thematic categorization, findings were synthesized to assess the compatibility of civilian models with military-specific requirements. This analysis revealed several critical insights:

- Civilian models, while robust, often lack the real-time adaptability and resilience needed in military environments.
- Military supply chains, with their high stakes and mission-critical demands, require tailored cybersecurity solutions that prioritize operational continuity and rapid response to cyber incidents.
- Emerging technologies in Supply Chain 4.0, such as IoT and blockchain, introduce vulnerabilities that civilian models may not sufficiently address, thus underscoring the need for specialized adaptations in military frameworks.

3.3. Framework Development and Validation

This study proposes a comprehensive cybersecurity framework tailored to the unique needs of military supply chains within the context of Supply Chain 4.0. The framework integrates foundational elements from existing civilian models, such as the Cyber Supply Chain Risk Management (CSCRM) model and the Cyber Kill Chain, while introducing military-specific enhancements to meet the demands of dynamic, high-stakes logistics environments.

3.3.1. Framework Components

- **Threat Intelligence and Real-Time Monitoring**: Central to the framework is a continuous monitoring system enabled by IoT sensors and real-time data analytics. These tools support early threat detection and rapid response, allowing military logistics operations to remain resilient even during active cyber threats. AI-driven predictive models analyze incoming data to forecast potential risks, while machine learning algorithms identify anomalous patterns indicative of emerging threats [4].
- **Resilience and Redundancy Planning**: Building upon the resilience-focused aspects of the SCOR model, this framework incorporates redundancy in key supply chain nodes, ensuring operational continuity even when primary nodes are compromised. This involves establishing alternative suppliers, maintaining

buffer inventories, and creating contingency plans for critical components, such as weapon systems or communication devices [23].

- **Cross-Jurisdictional Security Protocols**: Military operations often require collaboration across national borders and among allied forces. The proposed framework includes cross-jurisdictional security measures, such as standardized encryption protocols and secure communication channels. These protocols ensure that sensitive data remains secure during multinational logistics operations and facilitate interoperability among allied forces [9].

Validation Process: Figure 2 shows the framework development and validation. The framework's reliability and applicability were assessed through expert reviews and case study simulations. Scenarios based on past military cyber incidents were simulated to test the framework's effectiveness under conditions of active cyber threats, providing insights into areas where adjustments or additional measures may be necessary. By benchmarking against established frameworks and incorporating real-world feedback, the proposed model demonstrates enhanced resilience and adaptability to cyber risks, thereby reinforcing its utility in military logistics.

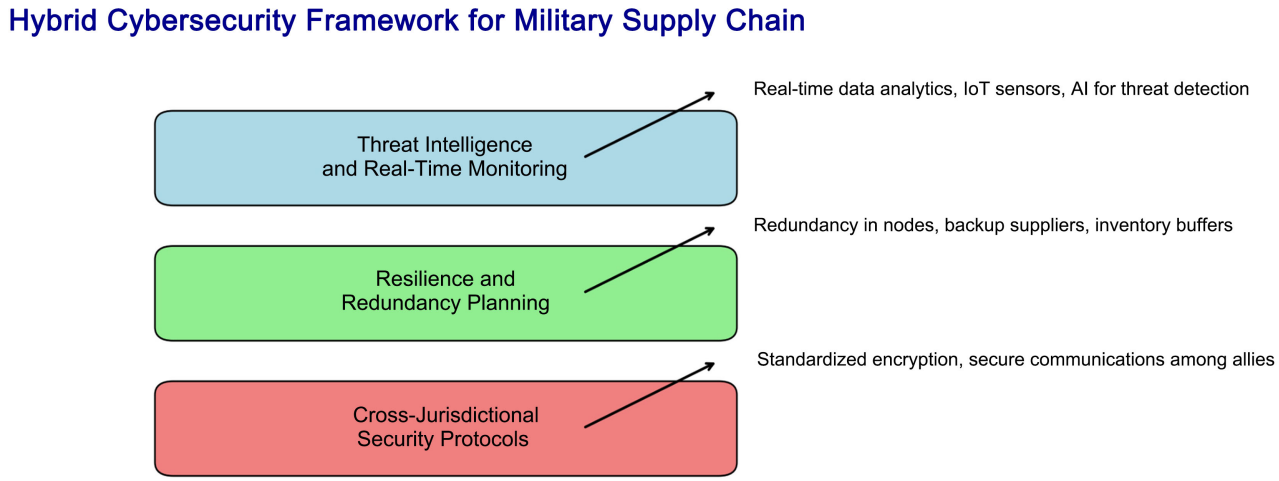

Figure 2. Framework development and validation.

3.3.2. Validation Strategy

To enhance the reliability and applicability of the proposed framework, a multifaceted validation strategy was employed, combining simulated case studies, expert reviews, and comparative analysis against established models.

Simulated Case Studies

Simulated scenarios, modeled on historical cyber incidents like the Stuxnet attack, demonstrate the framework's effectiveness in addressing real-world threats. In one scenario, adversaries infiltrated supply routes and tampered with military-grade equipment en route to deployment. The framework's real-time monitoring and anomaly detection system identified irregularities in shipment data, such as deviations in transit paths and unexpected delays. This triggered immediate corrective actions, including isolating the compromised supply chain node and redi-

recting unaffected assets to maintain operational continuity.

In another simulation, a 51% attack on a blockchain-based asset tracking system was thwarted by the framework's multi-layered defense mechanisms, which included permissioned access controls and advanced authentication protocols. These measures ensured that compromised nodes were isolated without disrupting the overall supply chain operation.

Expert Reviews

The proposed framework was reviewed by cybersecurity and military logistics experts to ensure practical relevance and alignment with real-world operational needs. Experts emphasized the importance of incorporating rapid incident response capabilities and ongoing testing of AI-driven predictive analytics to address evolving threat landscapes. Feedback from these reviews was integrated into the framework, refining its components and enhancing its adaptability to high-stakes military logistics.

Comparative Analysis

To further validate the framework's effectiveness, it was benchmarked against existing civilian and military cybersecurity models, such as the Cyber Kill Chain and the SCOR model. This comparative analysis highlighted the framework's strengths in addressing military-specific requirements, including cross-jurisdictional interoperability, mission assurance, and real-time adaptability. For instance, while the Cyber Kill Chain provided foundational insights into disrupting attack vectors, the proposed framework demonstrated superior resilience by incorporating redundancy and proactive risk management tailored to military supply chains.

4. Findings

4.1. Unique Cybersecurity Threats in Military Supply Chains

Military supply chains, integral to mission readiness and operational success, face a range of cybersecurity threats exacerbated by the advanced connectivity of Supply Chain 4.0. This heightened connectivity, while beneficial for efficiency and real-time monitoring, opens new vulnerabilities for exploitation. Cyber-attacks targeting military supply chains go beyond typical data breaches; they encompass both digital intrusions and physical tampering, collectively referred to as "supply chain poisoning". Attackers may intercept shipments and tamper with critical components, which, once embedded within military assets, could lead to catastrophic operational failures. For instance, malicious actors could infiltrate the supply chain by inserting compromised hardware into essential systems, which, if undetected, could disrupt communications, impede weapon systems, or even allow unauthorized remote access.

Such intrusions jeopardize mission-critical assets and create significant risks for military personnel, highlighting the imperative for stringent cybersecurity measures across all supply chain stages. This threat landscape, inclusive of both direct cyber-attacks and indirect supply chain poisoning, underscores the need for advanced

monitoring and end-to-end protection mechanisms within military supply networks. These protective measures must also extend to third-party suppliers and contractors, who are often targeted as an entry point by adversaries. The risks associated with even minor supply chain vulnerabilities have led military organizations to prioritize comprehensive security protocols tailored to their unique operational requirements [17]. The following graph in **Figure 3** illustrates the relative prevalence and severity of different cybersecurity vulnerabilities impacting military logistics. By highlighting these vulnerabilities, this analysis underscores the areas where robust cybersecurity strategies are most needed.

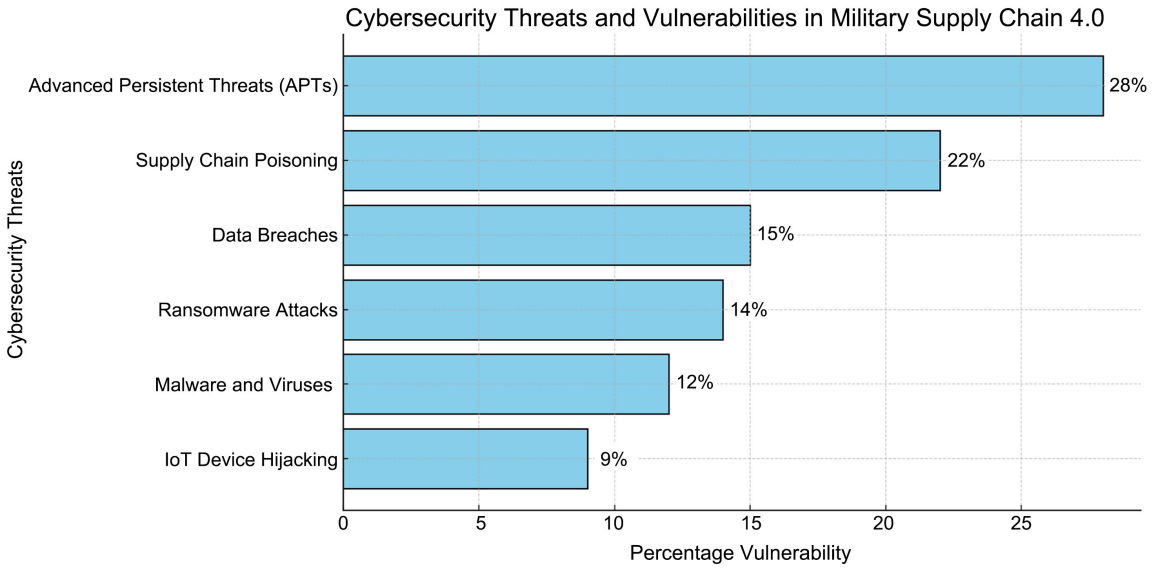

Figure 3. Unique cybersecurity threats in military supply chain.

4.2. The Role of Emerging Technologies in Securing Military Supply Chains

In a hypothetical implementation within the Department of Defense, AI-based anomaly detection could streamline monitoring of supply chain nodes, automatically alerting logisticians of irregularities in transport routes or inventory discrepancies. Similarly, permissioned blockchain for asset tracking could ensure that all components are verified as they pass through each supply chain stage, reducing the risk of supply chain poisoning.

Emerging technologies offer innovative avenues to bolster the security and resilience of Supply Chain 4.0, particularly within high-stakes military contexts. Among these, blockchain and artificial intelligence (AI) have shown the potential to enhance supply chain integrity significantly. Blockchain technology, through its decentralized and immutable ledger system, addresses the pressing need for traceability and transparency in military logistics. With blockchain, each transaction or transfer of goods within the supply chain is recorded in a tamper-proof ledger, allowing for unprecedented levels of authenticity verification [29]. This transparency could deter malicious actors by providing a verifiable chain of cus-

tody for all critical components, thus mitigating the risk of supply chain poisoning by ensuring each item's authenticity from origin to deployment.

Similarly, AI-driven predictive analytics serve as a proactive defense mechanism. By analyzing vast amounts of supply chain data, AI algorithms can identify anomalous patterns or irregularities indicative of potential cyber threats. For instance, deviations in shipping routes, unusual delays, or sudden inventory discrepancies can trigger alerts, allowing military logisticians to investigate and potentially mitigate threats before they manifest. The integration of AI with IoT-enabled sensors in the supply chain further enhances real-time monitoring capabilities, adding a layer of predictive maintenance and risk assessment [4].

While these technologies present substantial opportunities, their effective implementation in military contexts requires the development of a robust, security-focused framework. Such a framework must account for military-specific needs, such as maintaining operational security, real-time responsiveness, and compatibility with existing military infrastructure. Ensuring that blockchain and AI technologies align with these requirements is essential to avoid potential drawbacks, such as data latency, limited scalability, and network vulnerabilities that could inadvertently increase exposure to cyber threats. Properly implemented, these emerging technologies can transform military supply chains by making them not only more secure but also more resilient to future cyber challenges. While emerging technologies such as blockchain, AI, and IoT play a crucial role in enhancing the security and resilience of military supply chains, they also introduce distinct cyber vulnerabilities. For instance, adversarial attacks on AI models can lead to data poisoning, where attackers manipulate input data to cause erroneous outputs, ultimately jeopardizing decision-making processes in mission-critical operations [19]. In an IoT-based supply chain, attackers may exploit signal spoofing techniques to alter sensor data or even misdirect shipments, posing significant risks to military logistics where precision is paramount [25].

Blockchain technology, although tamper-resistant, is susceptible to attacks specific to its architecture, such as a 51% attack. In this scenario, a group of attackers could potentially gain control over more than half of the blockchain network's computing power, enabling them to alter transaction records and undermine data integrity [18] [30]. In a military context, this vulnerability is especially concerning due to the critical nature of asset tracking and verification.

To counteract these vulnerabilities, military supply chains must implement robust, multi-layered cybersecurity frameworks tailored to each technology's weaknesses. This may include advanced authentication mechanisms for blockchain, real-time data validation techniques for AI, and encrypted communication protocols for IoT devices. Moreover, the adoption of edge-computing solutions can help mitigate latency issues, enabling faster and more secure data processing close to where data is generated, thus reducing exposure to network-based attacks. Such measures ensure that while these technologies bolster military logistics efficiency and security, they do so without compromising operational resilience or data integrity [16].

4.3. Comparing Civilian and Military Risk Management Models

Civilian risk management models, such as the **Cyber Kill Chain** and **Supply Chain Operations Reference (SCOR)** model, focus on efficiency, cost-effectiveness, and process optimization. While these frameworks are valuable in commercial contexts, military logistics require a distinct approach that prioritizes security, resilience, and mission assurance in addition to efficiency. Military supply chains operate under high-stakes conditions where disruptions can have severe, life-threatening consequences. For example, an attack on a civilian supply chain may result in financial loss, but a cyber-attack on a military supply chain can compromise national security and endanger lives.

The **Cyber Kill Chain** framework provides a structured approach for understanding and disrupting cyber-attacks, outlining stages from reconnaissance to exploitation [22]. While it is effective for identifying cyber threats in civilian applications, the model lacks the adaptability and real-time responsiveness required in military logistics. Military supply chains face dynamic, targeted, and highly sophisticated threats, often from adversaries with specific strategic goals, such as **Advanced Persistent Threats (APTs)**. These threats demand military-specific adaptations of the Cyber Kill Chain, such as incorporating real-time threat intelligence, cross-functional interoperability, and adaptive defense mechanisms, to ensure mission assurance and operational continuity [4].

The **SCOR model** is another civilian framework that focuses on process optimization across five key areas: planning, sourcing, manufacturing, delivery, and return [23]. While SCOR is effective for improving supply chain performance in terms of cost, quality, and efficiency, it does not sufficiently address the resilience required for military applications. Military logistics demand frameworks that emphasize redundancy, flexibility, and recovery to handle both cyber and physical threats, ensuring operational continuity even in hostile environments. For example, SCOR must be augmented with military-specific measures, such as contingency planning, to protect against cyber-attacks that threaten mission-critical operations.

A hybrid approach that integrates both civilian and military frameworks offers a more comprehensive solution. This approach retains the process efficiency of the SCOR model while embedding military-specific resilience strategies such as:

- **Redundancy in Critical Nodes:** Backup suppliers, alternative transportation routes, and emergency communication channels.
- **Cross-Jurisdictional Security Protocols:** Ensuring interoperability between military and allied supply chains across different jurisdictions.
- **Rapid Response Mechanisms**: Real-time adaptability through AI and IoT-enabled monitoring, allowing quick action to mitigate cyber and physical disruptions.

[23] underscore the importance of resilience in supply chains, particularly in military logistics, where the ability to adapt quickly to changing conditions can make the difference between mission success or failure. Therefore, the hybrid

model must also incorporate proactive risk assessment, allowing for dynamic updates to the supply chain strategy in response to evolving threats.

Military logistics require models that emphasize **resilience over efficiency**, ensuring that even when a disruption occurs, the supply chain can quickly recover and continue operations. By integrating the efficiency-focused strategies of civilian models with the resilience-focused needs of military operations, this hybrid approach provides a robust framework that can secure military supply chains against both current and future threats. This model not only addresses the immediate cybersecurity needs of military logistics but also prepares them to adapt to the complex, evolving cyber threat landscape.

5. Discussion

Leveraging Blockchain for Enhanced Supply Chain Security

Blockchain technology offers significant benefits in terms of traceability and transparency for military supply chains. In a military context, where operational security is paramount, blockchain enables the continuous tracking of components, from manufacture through to final deployment. This process ensures the authenticity of military-grade assets, reducing the risk of tampering or counterfeit parts infiltrating the supply chain. Blockchain's tamper-proof ledger provides a high degree of accountability, recording each step and transaction, making it possible to quickly identify and trace defective or compromised components. Such transparency significantly reduces the risk of supply chain poisoning or malicious insertion of unauthorized components.

For example, blockchain can maintain a verifiable, immutable record for each component's lifecycle—whether it's weaponry, communication devices, or critical equipment—ensuring that all components are tracked and authenticated at every stage. In scenarios involving high-stakes equipment, such as military vehicles or sensitive technologies, this verification process is critical to ensuring reliability and security. If any part is compromised or counterfeit, blockchain enables quick traceability back to the specific point of compromise, facilitating a rapid response to mitigate any potential impact on mission success.

While blockchain offers powerful traceability, its implementation in military logistics requires addressing potential concerns about data confidentiality and scalability. To mitigate these challenges, a **private, permissioned blockchain** system is recommended. This system restricts access to authorized participants, ensuring secure and controlled data exchanges. Multi-layered encryption can be applied to prevent unauthorized access, while edge computing addresses latency and scalability concerns, supporting real-time military operations. This combination of encryption and decentralized, permissioned blockchain ensures that data is protected and transaction speeds meet the demands of military logistics.

In addition to traceability, blockchain facilitates **smart contracts**, which are self-executing agreements that automatically enforce specific conditions once predefined criteria are met. Within military logistics, smart contracts can automate

procurement processes, inventory tracking, and delivery confirmations. For example, when a military unit requests equipment, a smart contract can verify the legitimacy of the supplier and release payment only after the order is delivered and authenticated. This automation reduces the risk of human error and manipulation, enhancing the integrity of critical transactions.

Despite these advantages, blockchain's implementation in military supply chains requires careful consideration. Military operations often require large-scale, immediate processing, and blockchain's decentralized nature can introduce delays in transaction processing. Additionally, the transparency of blockchain could expose supply chain data to unauthorized parties unless strict access control measures are in place. Using permissioned blockchains that restrict access to verified participants allows military supply chains to maintain the benefits of transparency and immutability while securing sensitive data.

6. Conclusion

This study demonstrates that while Supply Chain 4.0 technologies offer unprecedented efficiency and transparency, they introduce critical vulnerabilities that must be addressed in military logistics. The proposed hybrid framework bridges the civilian-military gap by combining process efficiency with defense-specific measures like redundancy and real-time adaptability. Key findings underscore the necessity of a multi-layered approach to securing military supply chains, one that integrates real-time monitoring, redundancy planning, and cross-jurisdictional security protocols. The proposed framework, validated through expert feedback and simulated case studies, demonstrates improved adaptability to cyber threats, emphasizing the importance of tailored, military-specific cybersecurity standards. Future research should focus on scaling blockchain for large-scale military applications and refining AI-driven threat detection to adapt to evolving cyber risks. These innovations are essential to maintaining mission continuity and safeguarding national security in an increasingly interconnected digital landscape.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Sharma, A. and Jain, D.K. (2020) A Roadmap to Industry 4.0: Smart Production, Sharp Business, and Sustainable Development. Springer, 23-38.

[2] Frederico, G.F., Garza-Reyes, J.A., Anosike, A. and Kumar, V. (2019) Supply Chain 4.0: Concepts, Maturity and Research Agenda. *Supply Chain Management: An International Journal*, **25**, 262-282. https://doi.org/10.1108/scm-09-2018-0339

[3] Waters, D. (2014) Global Logistics: New Directions in Supply Chain Management. Kogan Page.

[4] Moustafa, N. (2018) A Holistic Review of Cybersecurity and Its Key Perspectives. *Future Generation Computer Systems*, **100**, 799-815.

[5] Gürtlich, G. and Lampl, S. (2022) Resilience and Military Supply Chain Management.

In: Kummer, S., *et al.*, Eds., *Springer Series in Supply Chain Management*, Springer International Publishing, 337-352. https://doi.org/10.1007/978-3-030-95401-7_29

[6] Turnbull, B. (2018) Cybersecurity in Military Logistics: Addressing the Challenges. *Cybersecurity Review*, **6**, 48-57.

[7] Chen, H.Y., Das, A. and Ivanov, D. (2019) Building Resilience and Managing post-Disruption Supply Chain Recovery: Lessons from the Information and Communication Technology Industry. I*nternational Journal of Information Management*, **49**, 330-342. https://doi.org/10.1016/j.ijinfomgt.2019.06.002

[8] Martin, M. and Towill, D. (2000) Supply Chain Excellence in the 21st Century. *International Journal of Logistics Management*, **11**, 73-82.

[9] Boyson, S. (2014) Cyber Supply Chain Risk Management. *Supply Chain Management Review*, **18**, 10-17.

[10] Meredith, L.S., Sherbourne, C.D. and Gaillot, S.J. (2011) Promoting Psychological Resilience in the U.S. Military. Rand Corporation.

[11] Kshetri, N. (2017) Cybersecurity and International Relations in Supply Chain Environments. *International Journal of Logistics Management*, **28**, 112-127.

[12] Chan, H.K., Subramanian, N. and Abdulrahman, M.D.-A. (2017) Supply Chain Management in the Big Data Era. IGI Global.

[13] Grzybowska, J.A.A.K. (2014) Standardization and Interoperability in Military Logistics. *Military Logistics Review*, **22**, 34-49.

[14] Lowe, E.B.A.J. (2004) The Myths and Facts Behind Cybersecurity in Industrial Control Systems. *Proceedings of the IEEE*, **92**, 877-889.

[15] Karantzas, G. and Patsakis, C. (2021) An Empirical Assessment of Endpoint Detection and Response Systems against Advanced Persistent Threats Attack Vectors. *Journal of Cybersecurity and Privacy*, **1**, 387-421. https://doi.org/10.3390/jcp1030021

[16] Choo, K.R. (2011) The Cyber Threat Landscape: Challenges and Future Research Directions. *Computers & Security*, **30**, 719-731. https://doi.org/10.1016/j.cose.2011.08.004

[17] Oks, S.J., Jalowski, M., Lechner, M., Mirschberger, S., Merklein, M., Vogel-Heuser, B., *et al.* (2022) Cyber-physical Systems in the Context of Industry 4.0: A Review, Categorization and Outlook. *Information Systems Frontiers*, **26**, 1731-1772. https://doi.org/10.1007/s10796-022-10252-x

[18] Saberi, S., Kouhizadeh, M., Sarkis, J. and Shen, L. (2019) Blockchain Technology and Its Relationships to Sustainable Supply Chain Management. *International Journal of Production Research*, **57**, 2117-2135. https://doi.org/10.1080/00207543.2018.1533261

[19] Li, J. (2018) Cyber Security Meets Artificial Intelligence: A Survey. *Frontiers of Information Technology & Electronic Engineering*, **19**, 1462-1474. https://doi.org/10.1631/fitee.1800573

[20] Wagner, P.M.A.D. (2004) Obscurity and Its Role in Network Security. *Security Research Journal*, **5**, 120-134.

[21] Chourabi, H. (2012) Cybersecurity Frameworks for Smart Systems. *International Journal of Advanced Computing*, **12**, 412-426.

[22] Hahn, A., Thomas, R.K., Lozano, I. and Cardenas, A. (2015) A Multi-Layered and Kill-Chain Based Security Analysis Framework for Cyber-Physical Systems. *International Journal of Critical Infrastructure Protection*, **11**, 39-50. https://doi.org/10.1016/j.ijcip.2015.08.003

[23] Pettit, T.J., Fiksel, J. and Croxton, K.L. (2010) Ensuring Supply Chain Resilience: De-

velopment of a Conceptual Framework. *Journal of Business Logistics*, **31**, 1-21. https://doi.org/10.1002/j.2158-1592.2010.tb00125.x

[24] 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*, **9**, 253-267. https://doi.org/10.1080/13675560600859276

[25] Poudel, P. (2016) Challenges and Solutions in IoT Security. *Journal of IoT Applications*, **14**, 215-229.

[26] Ben-Daya, M., Hassini, E. and Bahroun, Z. (2019) Internet of Things and Supply Chain Management: A Literature Review. *International Journal of Production Research*, **57**, 4719-4742. https://doi.org/10.1080/00207543.2017.1402140

[27] Manuj, I., Mentzer, J.T. and Bowers, M.R. (2009) Improving the Rigor of Discrete-event Simulation in Logistics and Supply Chain Research. *International Journal of Physical Distribution & Logistics Management*, **39**, 172-201. https://doi.org/10.1108/09600030910951692

[28] Fitz-Gerald, S.J. (2008) *International Journal of Information Management*, **28**, 77-78. https://doi.org/10.1016/j.ijinfomgt.2007.11.004

[29] Kshetri, N. (2017) Can Blockchain Strengthen the Internet of Things? *IT Professional*, **19**, 68-72. https://doi.org/10.1109/mitp.2017.3051335

[30] Zheng, Z.B., Xie, S.A., Dai, H.N., Chen, X.P. and Wang, H.M. (2017) An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. 2017 *IEEE International Congress on Big Data* (*BigData Congress*), Honolulu, 25-30 June 2017, 557-564.