systems

MDPI

*Article*

# Developing DEFCHAIN: A Dynamic Framework for Cybersecurity Risk Assessment in Military Supply Chains

**Mihael Plevnik [1,2,*] and Bojan Rupnik [2]**

[1] Ministry of Defence, Slovenian Armed Forces, SI-1000 Ljubljana, Slovenia
[2] Faculty of Logistics, University of Maribor, SI-3000 Celje, Slovenia; bojan.rupnik@um.si
* Correspondence: miha.plevnik@gmail.com; Tel.: +386-31-306-079

**Abstract**

In this article, we employed a systematic approach to risk assessment and the adaptation of security measures to explore possibilities for more effective cybersecurity in the supply chains of the armed forces. Our focus was on developing a model with quantified indicators that, on one hand, enable dynamic monitoring of the security status and timely threat detection, while, on the other hand, enhance the resilience of supply chains against cyber threats. Our findings indicate that applying this model enables a comprehensive security risk assessment, the adaptation of protective measures to operational requirements, and the optimization of resources to ensure the uninterrupted functioning of the armed forces. Future research will focus on validating the model in real-world scenarios and adapting it to the specific needs of different organizations.

**Keywords:** military logistics; security model; supply chains; cyber security; risk assessment; resilience

## 1. Introduction

Ensuring cybersecurity in the supply chains of armed forces is becoming increasingly complex and demanding due to rising cyber threats, automation and digitalization of military systems, and dependence on external suppliers. While new technological capabilities bring many benefits, they also introduce significant risks to system operations. Increased social engineering activity, vulnerabilities in information systems, and insecure software within the supply chain pose risks that can compromise the integrity of operations, including those of armed forces. Supply chain security is therefore no longer merely a logistical challenge but requires a comprehensive approach that integrates technical, organizational, regulatory, and strategic measures to reduce risks and enhance resilience against cyberattacks. This need is particularly acute in military environments, where supply chains fundamentally differ from those in the commercial sector. Unlike economic supply chains, which prioritize cost-efficiency, speed, and competitiveness, military supply chains are mission-critical systems designed to ensure operational readiness, continuity, and resilience in crisis and conflict scenarios. They operate under classified conditions, require compliance with strict national and allied security standards, and include specific mechanisms such as supplier vetting, protection against malicious code, and contractual cybersecurity obligations. Risk management in the defence context must account not only for technological vulnerabilities but also for geopolitical threats, deliberate adversarial ac-

Academic Editor: Ben Clegg

Received: 25 December 2025
Revised: 20 January 2026
Accepted: 26 January 2026
Published: 27 January 2026

tions, and the need for interoperability in multinational operations. As such, military supply chains emphasize reliability, redundancy, and secure functionality even under degraded or contested conditions—demands that far exceed those typically encountered in commercial logistics systems.

Despite existing security policies and international standards such as ISO 28000 (security management systems for the supply chain), NIST SP 800-161 (supply chain risk management practices for federal systems), the Cyber Resilience Act (CRA) (focused on software product security in the EU), and the Cybersecurity Maturity Model Certification (CMMC) (cybersecurity requirements for DoD contractors), the challenge remains: how to effectively and holistically manage cybersecurity risks in military supply chains. These frameworks provide valuable guidelines for specific domains—ISO 28000 emphasizes security planning and resilience, NIST SP 800-161 details federal acquisition risk management, CRA addresses software vulnerabilities and post-market obligations, and CMMC defines maturity levels for contractor compliance—but none of them offers an integrated, operationally adaptable model that would align tactical needs, geopolitical risk exposure, and cybersecurity assurance in the defence logistics environment. Most research focuses on individual aspects of protection [1–5], such as threat identification, supplier evaluation, or software integrity, but fails to provide a comprehensive and dynamic framework that supports systematic risk assessment and real-time adaptation of security measures in response to evolving technological, legal, and adversarial contexts. The research gap thus lies in the absence of a domain-specific, process-driven, and factor-based model tailored for military supply chains—one that operationalizes cybersecurity as a quantifiable and situationally responsive component of defence logistics. The aim of this article is to address this gap by developing an enhanced model for assessing cybersecurity in military supply chains, one that considers a broad range of factors—from supplier trust and transit security to contractually embedded assurance measures and responsiveness to multi-domain operational demands.

The research addresses two fundamental questions: (1) which categories and measures influence the cybersecurity of military supply chains, and how can they be quantified to improve risk assessment and enhance security management, and (2) how can systematic risk evaluation and the application of a cybersecurity model contribute to timely threat identification, forecasting future cybersecurity states, and dynamically adapting security measures.

This article proposes a structured approach to cybersecurity risk evaluation in supply chains by introducing the Defensive Evaluation Framework for Cybersecurity in Supply Chains (DEFCHAIN). While existing risk management frameworks, such as ISO 28000 and NIST SP 800-161, provide essential guidelines for security planning and federal acquisition, they primarily function as static compliance-based models. DEFCHAIN extends these baselines by providing an integrated system that transitions from periodic assessment to dynamic, mathematically grounded risk evaluation. The framework's incremental contribution lies in its ability to adjust the priority of security measures in response to evolving threat levels, regulatory changes, and geopolitical risks. Unlike conventional weighted indices that rely on fixed parameters, DEFCHAIN introduces a regime-dependent mechanism where the importance of specific security dimensions shifts based on predefined risk thresholds. This approach enables the quantification and prioritization of cyber threats, supports scenario-based simulations, and transforms cybersecurity from a static compliance objective into an evolving operational capability. While developed for the high-assurance requirements of military logistics, the model's architecture is designed to be transferable to critical civilian sectors, aligning real-time risk management with national security and societal continuity.

https://doi.org/10.3390/systems14020132

A systematic approach to evaluating cybersecurity in supply chains enables a better understanding of critical vulnerabilities and optimization of protective measures in real time. By integrating quantitative risk assessment methods, this research offers both theoretical and practical solutions for enhancing the cybersecurity of military supply chains—solutions that can be applied to the development of security policies and operational strategies. The article presents a dynamic, factor-based, mathematically defined model that allows real-time adaptation of cybersecurity measures based on perceived risks and external influences. Through the use of weighted indicators and continuous feedback (sensing–understanding–directing), the model enables not only the detection and analysis of threats but also automated adjustment of protection strategies. This contributes to ensuring the uninterrupted execution of military operations, even under conditions of degraded functionality or active adversarial threats, by strengthening resilience, optimizing resource allocation, and enabling command to proactively respond to cyber incidents.

## 2. Materials and Methods

The research applies a mixed-methods approach that combines a structured review of existing scientific and professional literature with the development of a mathematically grounded cybersecurity assessment model tailored to military supply chains. The literature review was conducted using predefined analytical criteria derived from the conceptual foundations of the DEFCHAIN framework. Each source was examined for the presence of quantifiable indicators, dynamic security processes, external contextual influences, and applicability to defence or other critical sectors. This systematic analysis revealed relevant theoretical building blocks, identified methodological gaps in existing work, and guided the formulation of the model's structural components.

Building on the insights obtained from the review, a comprehensive set of factors and indicators was defined to evaluate cybersecurity across three core dimensions: supplier trust, in-transit security, and organizational cybersecurity. These indicators were qualitatively assessed and subsequently transformed into a unified four-level numerical scoring system, enabling consistent comparison and integration across categories. The scoring methodology employs a percentage-based scale to ensure transparency and comparability between indicators, factors, and aggregated risk outcomes.

The mathematical structure of the DEFCHAIN model was developed to reflect the dynamic and interconnected nature of cybersecurity in supply chains. It uses weighted parameters to capture the relative importance of each security dimension and incorporates time-dependent variations in perceived risk. The model further integrates external influences—such as geopolitical conditions, regulatory environments, and resource availability—by quantifying them and embedding their effects directly into the overall cybersecurity evaluation.

The methodological design emphasizes an iterative and process-oriented logic based on the sensing–understanding–directing framework, which supports continuous adaptation of security priorities. The resulting model allows for systematic assessment of cybersecurity posture, identification of vulnerabilities, and dynamic adjustment of protective measures, providing a robust analytical foundation for evaluating and improving the resilience of military supply chains.

The sensing–understanding–directing cycle is defined at an analytical level and does not prescribe specific security tools or data sources. Inputs from systems such as SIEM or IDS/IPS are treated as abstracted risk signals that inform perceived risk values, while update cycles and triggering conditions are scenario-dependent and defined by the organizational context rather than fixed model parameters.

https://doi.org/10.3390/systems14020132

Model validation in this study focuses on structural consistency, behavioural verification, sensitivity analysis, and scenario-based simulation, rather than empirical performance evaluation. Empirical validation using real military supply chain data is outside the scope of this work due to classification constraints and is envisaged as a future application using proxy, aggregated, or declassified inputs. A complete illustrative worked example demonstrating the full computational flow of the DEFCHAIN model—from indicator scoring to composite risk evaluation—is provided in Appendix A.

## 3. Literature Review

The literature review follows a structured methodology based on nine analytical categories, offering a comprehensive and multidimensional examination of the topic. The Model with Indicators and Factors category covers theoretical and empirical models; Qualitative and Quantitative Indicators address measurement methods. Dynamic Analysis focuses on risk evolution over time, while External Environment considers contextual and geopolitical influences. In-Transit Security explores vulnerabilities during transport. Advanced Technologies looks at the impact of emerging solutions, and Modularity and Expandability assess system flexibility. The Military Context addresses cybersecurity in defence settings, and Cross-Sector Adaptability examines the transferability of practices to other domains. This structure supports consistent analysis and helps identify research gaps.

While foundational concepts in supply chain risk management and military cybersecurity largely originate from earlier work (2015–2020), more recent studies (2021–2024) primarily extend these frameworks through technological, regulatory, and contextual refinements rather than proposing fundamentally new conceptual models. Accordingly, both foundational and recent literature are integrated to ensure theoretical continuity and contemporary relevance.

Global supply chains, though essential to the modern economy, face growing cybersecurity risks due to digitalization and interdependence. The Model with Indicators and Factors category includes diverse approaches to managing these risks and improving resilience. CISA [3] and NIST [4] present a six-phase lifecycle for ICT supply chains, offering a risk management model based on C-SCRM and SSDF frameworks. Bartol [5] emphasizes buyer–supplier expectations in public services and outlines ten key practices, including asset identification and supplier risk assessment. Expanding on earlier work, Kaur et al. [6] propose an integrated model for optimizing supplier selection and investment in cyber resilience, arguing that organizational investment alone is insufficient. Hou et al. [7] introduce the SEISMIC framework for ICS supply chains, addressing technical, human, and organizational risks. Davis [8] offers an information-centric model to enhance cyber resilience, noting the attractiveness of supply chains to attackers, while Boyes [9] underlines the challenges of IT-dependent resilience. Amaral and Gondim [10] propose applying Zero Trust architecture to mitigate insider threats in supply chains. Pandey et al. [11] classify cyber risks into supply, operational, and demand categories, warning that ICT, while enhancing efficiency, also introduces vulnerabilities. Yeboah-Ofori and Islam [12] present a threat modelling framework incorporating actors, targets, and TTPs to analyze organizational supply chain threats. In a related study, Yeboah-Ofori et al. [13] highlight the role of cyber threat intelligence (CTI) in proactively identifying and countering threats in cyber supply chain systems. Together, these studies provide a diverse set of models and frameworks, from general guidelines to proactive intelligence strategies, contributing to a comprehensive understanding of supply chain cybersecurity. These approaches provide valuable foundations for identifying supply chain cybersecurity factors, but they do not offer a unified, dynamic, and quantitatively formalized evaluation framework, which is addressed by the DEFCHAIN model.

https://doi.org/10.3390/systems14020132

The Qualitative and Quantitative Indicators category examines how cyber supply chain risks are measured using regulatory, methodological, and empirical approaches. Cantrell [14] highlights the impact of new regulations (e.g., EU CRA, NIS2, U.S. CMMC) on improving cyber supply chain risk management, offering a qualitative view of regulatory pressures. Prevalent [15] complements this with practical indicators drawn from ISO and NIST standards, supporting automated assessments of third-party risk. The Danish CFCS and Digital Government Agency [16] provide guidelines for outsourced IT services, emphasizing proactive supplier risk management through audits and controls. Similarly, the UK Cabinet Office [17] proposes a public-sector risk management framework using both qualitative and quantitative tools, including CCfAR and SoA scoring. Creazza et al. [18] introduce a quantitative perspective via ANOVA analysis in the FMCG sector, highlighting the role of logistics providers. Lewis et al. [19] examine cybersecurity breaches in UK SMEs and propose a taxonomy for secure information exchange, combining metrics with insights on data-sharing barriers. Del Giorgio Solfe [20] offers empirical evidence from the UAE pharmaceutical sector on how cyber risks affect digital operations. Latif et al. [21] conduct a systematic literature review, identifying four research domains (e.g., IoT, network security) and providing a qualitative synthesis of trends. Finally, Yeboah-Ofori et al. [22] apply a net present value analysis to evaluate cybersecurity investments, offering financial metrics for decision-making. Collectively, these studies present a well-rounded view of how cyber supply chain risks are assessed through standards, audits, statistical methods, financial analysis, and regulatory frameworks. While existing studies propose diverse qualitative and quantitative indicators, they typically treat them as static assessment tools rather than components of a dynamic, adaptive evaluation process, which limits their ability to reflect evolving risk conditions over time.

The Dynamic Analysis category addresses the evolving nature of cyber threats in supply chains and the need for adaptive responses. Herr et al. [2] examine the growing risk of software supply chain attacks, identifying five trends—such as hijacked updates and state actor involvement—that illustrate how threats continuously change. Bradshaw [23] adds a global dimension by analyzing the role of CSIRTs in international cooperation. While agreeing with Herr on threat evolution, he emphasizes cross-border collaboration and highlights barriers such as legal and commercial constraints. Urciuoli [24] contributes a complementary perspective by focusing on ICT-based strategies for real-time risk monitoring and response. Unlike Herr and Bradshaw, who emphasize threat patterns and coordination, Urciuoli underlines the strategic role of technology in enhancing supply chain resilience. Together, these works highlight the dynamic and adaptive nature of cybersecurity in supply chains, underscoring the importance of both international cooperation and technological capabilities in managing shifting risks. This body of work highlights the evolving nature of supply chain cyber threats, underscoring the need for models capable of representing time-dependent risk adaptation, which directly motivates the dynamic structure of DEFCHAIN.

The Consideration of the External Environment category examines how external factors shape cybersecurity in supply chains and supports a holistic perspective. Pellathy and Burnette [25] argue that while most cyber incidents originate from third parties, organizations focus too narrowly on internal controls. They propose four risk strategies, emphasizing shared responsibility across the supply chain. Levite [26] adds a geopolitical dimension, analyzing how state and non-state actors exploit ICT/OT supply chains throughout the product lifecycle. He proposes a normative framework to mitigate such interference. Lamba et al. [27] explore risks linked to SCM information systems and technologies like IoT and cloud, calling for automation due to the limits of manual oversight. Boiko et al. [28] build on this by stressing the role of information security in integrating suppliers and

customers, reinforcing concerns over external technological vulnerabilities and attack vectors. Together, these contributions highlight the importance of addressing external risks—whether geopolitical, technological, or systemic—to ensure comprehensive and resilient supply chain cybersecurity. These findings reinforce the importance of explicitly incorporating external and geopolitical factors into cybersecurity assessments, a dimension that is formalized within the DEFCHAIN framework.

The In-Transit Security category focuses on cybersecurity risks during the transportation phase of supply chains, especially in logistics and maritime sectors. Odimarha et al. [29] highlight vulnerabilities arising from system interconnectivity and the high value of goods, identifying threats such as ransomware and recommending measures like encryption and adherence to GDPR and ISO 27001. Sarumi and Okunoye [30] expand on this by presenting detailed cybercrime scenarios—including weapons smuggling and pharmaceutical sabotage—that expose weaknesses in the information layer of supply chains. While Odimarha et al. [29] focus on broad preventive practices, Sarumi and Okunoye [30] provide concrete illustrations of targeted attacks during transit. Together, these studies underscore the importance of securing digital infrastructure during transport and demonstrate the need for both technical safeguards and scenario-based threat awareness to address in-transit cybersecurity risks.

The Advanced Technologies category examines how innovations simultaneously introduce new cybersecurity risks and offer security-enhancing solutions. Herr et al. [31] analyze the Sunburst attack, where sophisticated malware embedded in Orion software compromised thousands of organizations, illustrating the destructive potential of advanced exploits. Martínez and Durán [32] also examine the SolarWinds breach, linking vulnerabilities to reused open-source code and recommending Zero Trust, MFA, blockchain, and DevSecOps practices. Department of the Environment, Climate and Communications [33] outlines technological safeguards for securing electronic communication networks, aligning mitigation efforts with international standards (ISO/IEC, NIST). Hammi et al. [34] review security threats in digital supply chains and propose countermeasures like blockchain, AI, and digital signatures to address risks stemming from rapid ICT growth. Similarly, Adenekan et al. [35] advocate advanced technologies and proactive strategies such as secure software development and Ze Trust. Zhang et al. [36] explore IoT, cloud, and blockchain in digital supply chains, emphasizing that while these tools increase efficiency, they also reduce traditional security boundaries. Gupta et al. [37] focus on cyber-physical system risks in additive manufacturing, highlighting vulnerabilities unique to 3D printing and the merging of virtual and physical supply chains. Finally, Sobb et al. [38] examine Supply Chain 4.0, focusing on risks in military contexts from integrated technologies like AI, IIoT, and smart contracts. Together, these studies reveal that advanced technologies are both a source of new vulnerabilities and an essential part of resilient cybersecurity strategies in modern supply chains, highlighting the need for evaluation models capable of capturing both technological risk exposure and adaptive security responses, as reflected in the DEFCHAIN framework.

The Modularity and Expandability via Architecture category explores how flexible system architectures enhance supply chain cybersecurity. Leligou et al. [39] introduce the FISHY platform, which uses machine-based tools and blockchain within a modular, scalable design validated through the MITRE ATT&CK framework [40], demonstrating strong protection against future threats. Masip-Bruin et al. [41] expand on the architectural principles behind FISHY, focusing on ICT and IoT environments. Their solution integrates services and DLT to address system vulnerabilities and coordination issues. Together, these studies highlight how modular and expandable architectures improve resilience and adaptability in complex supply chain systems, enabling effective responses to evolving

cyber threats, and underscore the value of frameworks that support modular evaluation and future extensibility, as reflected in the design of the DEFCHAIN model.

The Military Context category explores the specific cybersecurity challenges within defence systems and the broader impact of cyber threats on national security. Hammock [42] compares Cold War submarine tactics with modern cyber operations, highlighting NATO's operational understanding of cyberspace and its geopolitical implications. Kramer and Teplinsky [43] propose a hybrid deterrence model with cyber sanctions and authorized private-sector defence, shifting from a purely military response to broader strategic engagement. Falk [44] examines Sweden's security-protected procurement processes, finding they enhance C-SCRM despite challenges for SMEs. Reinsch et al. [45] focus on semiconductor supply chains and advocate for international cooperation and "friend-shoring" strategies. Carter [46] highlights the inseparability of cybersecurity and military logistics in the U.S. Department of Defence supply chains. Rosenzweig and Waldron [47] provide a strategic analysis of U.S. defence policy, emphasizing risks from China and Russia and the importance of supply chain integrity. Sanchez and Ebner [48] focus on legal obligations for defence contractors and offer regulatory recommendations. Rahayu et al. [1] propose using blockchain to counter counterfeit parts in military spare parts logistics. Coufalíková et al. [49] suggest a Zero Trust-based strategy for protecting defence supply chains, referencing threats like Solarigate. Together, these works span operational, strategic, legal, and technological dimensions of military cybersecurity, offering comprehensive insight into protecting defence supply chains and highlighting the need for integrated assessment models capable of capturing these dimensions within a unified analytical framework, as pursued by the DEFCHAIN model.

The Cross-Sector Adaptability category explores how cybersecurity practices and frameworks for supply chains can be transferred across industries and government sectors. Burnson [50] highlights the U.S. manufacturing sector's lack of preparedness for Industry 4.0 threats and recommends learning from mature sectors like finance. Warrick et al. [51] emphasize the importance of adaptable public–private partnerships for U.S. homeland security, extending the idea of cross-sector collaboration. Bartol [52] focuses on the development of flexible cybersecurity standards, noting that many practices were adapted from other disciplines. Wallis and Dorey [53] describe the creation of a cybersecurity community in the energy sector, stressing collaborative approaches within and between organizations. Wallis et al. [54] analyse the NIS Directive's implementation in the UK, advocating a balance between oversight and cooperation and highlighting its cross-sector applicability despite indirect regulation of supply chains. Together, these studies demonstrate that collaborative, adaptable approaches—whether regulatory, strategic, or technical—are essential for strengthening cybersecurity across sectors and for enabling the transferability of security practices between different operational domains.

In summary, existing research addresses multiple dimensions of supply chain cybersecurity, including governance, technology, regulation, and sector-specific risks. However, the literature lacks an integrated framework that combines dynamic risk adaptation, quantitative aggregation of heterogeneous indicators, and explicit modelling of external influences, particularly in military supply chains. This gap provides the basis for the DEFCHAIN model proposed in this study.

## 4. Results

This section presents the DEFCHAIN model and reports the results of its analytical and simulation-based evaluation. First, we describe the model structure and its three core components—supplier trust (S), security in transit (T), and organizational cybersecurity (O)—together with the indicator system and the rule-based ordinal scoring methodology

used to transform qualitative assessments into computable inputs. We then report the outcomes of the internal validation of mathematical consistency and numerical behaviour across the defined parameter domain, followed by scenario-based simulations used to examine dynamic response patterns, parameter sensitivity, and stability of CS(t) under controlled conditions. Finally, we provide a focused analysis of the logistic weighting function, highlighting how responsiveness ($\lambda$) and threshold ($\theta$) shape regime-dependent model behaviour.

### *4.1. Adaptive Cybersecurity Model: The DEFCHAIN Framework*

Ensuring cybersecurity in armed forces supply chains demands a comprehensive and adaptive approach to managing risks and safeguarding critical elements. In a security environment marked by rapidly evolving threats, static models no longer provide sufficient resilience. To address this, we developed DEFCHAIN—a dynamic cybersecurity framework tailored to the unique characteristics of military supply chains. Unlike commercial systems, military logistics operate in sensitive, often contested environments, where secure handling of classified information, geopolitical exposure, and strict compliance with defence and NATO standards are essential. Reliability, redundancy, and interoperability take precedence over efficiency and speed, and operations frequently span multinational and multi-domain contexts.

DEFCHAIN addresses these challenges by combining mathematically grounded assessment with operational processes specifically adapted to defence logistics. The model is built on three interconnected components: (1) factors and indicators, (2) a dynamic evaluation process, and (3) external influences. Together, they enable context-aware decision-making and continuous reassessment of cyber posture. Using a feedback loop—sensing, understanding, and directing—DEFCHAIN prioritizes vulnerabilities, supports timely mitigation, and sustains supply continuity even under hostile or degraded conditions. Its modular and scalable architecture also allows application across different operational levels, making it suitable for both military and civilian settings.

The model ($CS$) incorporates (see Figure 1) quantified evaluation of categories and measures—trust in suppliers ($S$), security in transit ($T$), and organizational cybersecurity ($O$)—which enables an objective analysis of the security posture and identification of key vulnerabilities (see Equation (1)). It also includes a repeatable information processing procedure that allows for the adjustment of security measures based on the results of previous risk assessments and threat evaluations. Additionally, it takes into account the influence of external factors such as geopolitical conditions, resource availability, and organizational resilience, thereby providing a comprehensive risk assessment.

$$CS = f(S, T, O) \quad (1)$$

### *4.2. Factors and Indicators*

To enable a comprehensive assessment of cybersecurity in armed forces supply chains, we defined factors and indicators that allow for the quantifiable evaluation of security risks and capabilities. We employed a methodological framework based on the Deming cycle of continuous improvement (PDCA—Plan, Do, Check, Act), which ensures a systematic approach to managing security risks. The factors and indicators are not static values, but dynamic parameters that adapt to changes in the security environment, technological infrastructure, and operational requirements.

We propose three key factors that together form the framework for assessing supply chain resilience:

1. Trust in the supplier–including elements such as supplier reliability, compliance with standards, and prior verification procedures (see Table 1).

2. Security in transit–focusing on the protection of communication channels, data integrity, and monitoring during the transfer of goods or information (see Table 2).
3. Organizational cybersecurity–covering incident response capabilities, operational security measures, internal protocols, and cyber hygiene practices (see Table 3).

Each factor is subdivided into several indicators that define specific security aspects in more detail. These factors and indicators were initially evaluated qualitatively, allowing for classification into four groups. This qualitative assessment was then converted into quantitative data using a four-level scale, enabling comparability between factors and indicators and integration of the results into a broader mathematical model for cybersecurity analysis.

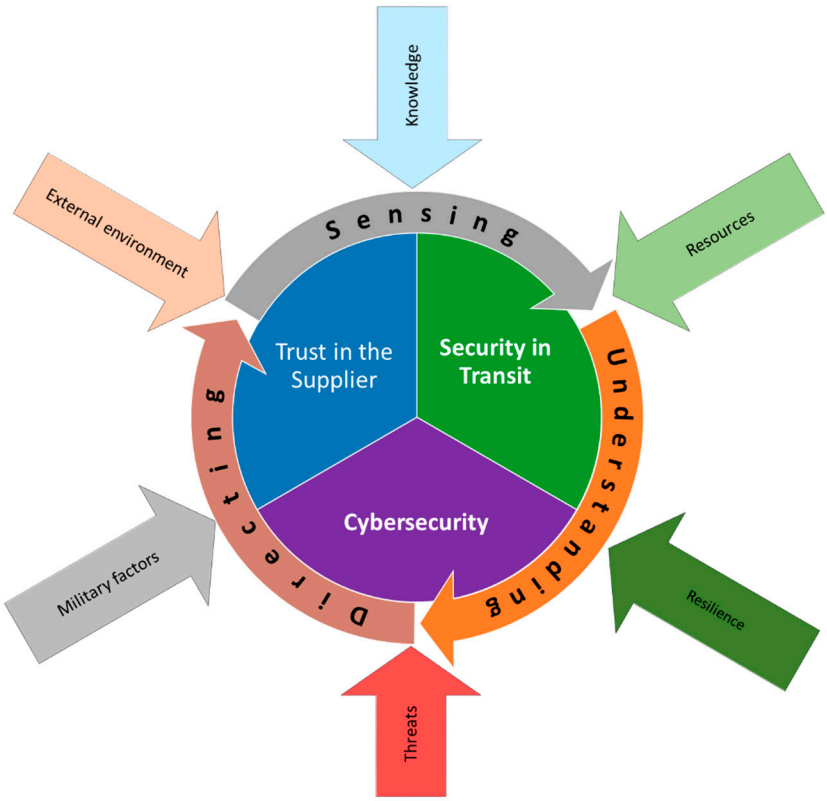


**Figure 1.** Cybersecurity model for armed forces supply chains.

The model supports dynamic assessment, where changes in one factor can affect the values of others. This ensures that the model adapts to the current security situation. By doing so, it surpasses static risk assessment approaches and enables proactive management of cybersecurity in supply chains, which is critical for the resilience of armed forces against modern threats in the cyber domain.

**Table 1.** Trust in supplier indicators.

| Factors | Indicators |
|---|---|
| 1. Trust in Supplier | 1.1. Certifications and Compliance |
| | 1.2. Financial Stability and Long-Term Reliability |
| | 1.3. Contracts |
| | 1.4. Sub-supplier |
| | 1.5. Risk Management and Preparedness Plans |
| | 1.6. Response and Recovery Plans |
| | 1.7. Technical Requirements |

| | |
|---|---|
| | 1.8. Insider Threat Protection |
| | 1.9. Cybersecurity Education and Training |
| | 1.10. Transparency and Collaboration |
| | 1.11. Physical Security |

The cybersecurity of suppliers ($S$), including their sub-suppliers and associated transport links, is represented in Equation (2). $S_i$ denotes the cybersecurity level of supplier $i$, while $S_{ij}$ represents the cybersecurity level of sub-supplier $j$, who is associated with supplier $i$. The term $T_{ij}$ refers to the in-transit security between supplier $i$ and their corresponding sub-supplier $j$. The variable mi indicates the number of sub-suppliers associated with supplier $i$, and $n$ represents the total number of primary suppliers in the supply chain.

$$S = \sum_{i=1}^{n} \left( S_i + \sum_{j=1}^{mi} (S_{ij} + T_{ij}) \right) \quad (2)$$

In practical application, the variables $S_i$, $S_{ij}$, and $T_{ij}$ are not directly measured quantities, but composite ordinal scores derived from documented and observable evidence using the rule-based scoring methodology defined in Section 4.3. Specifically, $S_i$ and $S_{ij}$ represent aggregated indicator scores reflecting supplier and sub-supplier cybersecurity posture (e.g., certifications, access control, vulnerability management, incident response capability, and contractual safeguards), while $T_{ij}$ captures the security of the in-transit relationship based on indicators related to transport security controls, data integrity mechanisms, monitoring, and contractual provisions.

In simulation experiments, representative values of these variables are assumed to analyze model behaviour and sensitivity. In real-world deployment, the same scoring framework would be instantiated through evidence-based assessment, ensuring traceability from observable conditions to model inputs.

This formulation captures the hierarchical and interconnected nature of supply chains by including both direct suppliers and their extended supply networks. It allows for a detailed assessment of trust by aggregating cybersecurity performance across all levels of the supplier structure and the links between them. As such, it supports a nuanced evaluation of supply chain exposure to cyber risks originating from third parties.

**Table 2.** Security in transit indicators.

| Factors | Indicators |
|---|---|
| 2. Security in Transit | 2.1. Encryption and Communication Protection |
| | 2.2. Data Integrity and Authenticity Verification |
| | 2.3. Authentication and Access Control |
| | 2.4. Prevention of Attacks During Transit |
| | 2.5. Monitoring and Anomaly Detection |
| | 2.6. Segmentation and Security in Code Distribution |
| | 2.7. Physical Security of Supply Chains |
| | 2.8. Redundancy and Availability Assurance |
| | 2.9. IoT and Edge Device Security |
| | 2.10. Use of Advanced Technologies |
| | 2.11. Incident Planning and Response in Transit |

The level of security in transit, referring to the protection of data, goods, and communications between suppliers and the organization, is expressed in Equation (3). $T_i$ represents the in-transit security between supplier $i$ and the organization. The variable $n$ denotes the total number of suppliers in the supply chain.

$$T = \sum_{i=1}^{n} T_i \quad (3)$$

This equation provides a cumulative assessment of transit-related security, aggregating the level of protection across all supply paths. It highlights the importance of secure transmission channels and the need to evaluate each supplier's delivery route individually, as vulnerabilities in any single transit link can compromise the integrity of the entire supply chain. The model thus emphasizes a holistic view of transport security as a key component of overall supply chain cybersecurity.

**Table 3.** Organizational cybersecurity.

| Factors | PDCA Cycle | Indicators |
|---|---|---|
| 3. Cybersecurity | 3.1. Planning | 3.1.1. Management and Strategic Planning |
| | | 3.1.2. Risk and Resilience Management |
| | | 3.1.3. Minimum Cybersecurity Requirements |
| | | 3.1.4. Business Continuity |
| | | 3.1.5. Compliance, Legal Frameworks, and Regulations |
| | 3.2. Implementation | 3.2.1. Physical Security and Data Protection |
| | | 3.2.2. Establishment and Management of Security Architecture |
| | | 3.2.3. Application Protection |
| | | 3.2.4. Data Loss Prevention |
| | | 3.2.5. Monitoring of C4I System Operations |
| | | 3.2.6. Cyber Incident Response |
| | | 3.2.7. IoT Device Protection |
| | | 3.2.8. Solution Verification and Security Testing |
| | | 3.2.9. Security Operations Management–SOC |
| | 3.3. Verification | 3.3.1. Preventive Measures and Updates |
| | | 3.3.2. Penetration Testing and Attack Simulations |
| | | 3.3.3. Identity and Privileged Account Management |
| | | 3.3.4. Security Practice Audits |
| | | 3.3.5. Monitoring Security Logs |
| | 3.4. Improvement | 3.4.1. Education, Training, and Awareness |
| | | 3.4.2. Exercises and Testing |
| | | 3.4.3. Change Management |
| | | 3.4.4. Implementation of Threat Indicators |
| | | 3.4.5. Collaboration and Researching New Technologies |

### *4.3. Scoring Methodology for Risk Indicators*

The transformation of qualitative indicator assessments into quantitative inputs for the DEFCHAIN model was conducted using a structured, rule-based scoring methodology. Each indicator was evaluated against a predefined set of descriptive criteria and subsequently mapped to a discrete numerical value, ensuring consistency, reproducibility, and interpretability of the scoring process (see Table 4).

**Table 4.** An illustrative example of the scoring logic applied to a supplier certification indicator.

| Risk Level | Score | Colour | Qualitative Description |
|---|---|---|---|
| Low risk | 5 | Green | The supplier holds multiple certifications across different domains (e.g., information security, resilience, risk management). Certifications are valid, regularly reviewed, and updated, and include advanced or sector-specific standards. |
| Medium risk | 3 | Yellow | The supplier holds at least one key certification; coverage is incomplete across security domains. Certifications are valid but not systematically reviewed or updated; the maturity level is basic to intermediate. |
| High risk | 1 | Orange | The supplier demonstrates minimal compliance, typically limited to a single general certification not tailored to specific security requirements. Validity checks and audits are infrequent or absent. |
| Critical risk | 0 | Red | The supplier holds no valid certifications, does not conduct compliance audits, and does not apply standardized security practices, indicating a high likelihood of security deficiencies. |

Rather than assigning numerical values subjectively, each indicator score was derived from a detailed qualitative description specifying observable organizational practices, compliance status, and verification mechanisms. In this way, numerical scores represent explicit operational conditions and documented evidence rather than implicit judgement or expert intuition alone.

A four-level ordinal scale was adopted to represent increasing levels of cybersecurity risk:

- 5 points (low risk, green)—evidence of advanced and systematically maintained security practices;
- 3 points (medium risk, yellow)—partial coverage of relevant security requirements with limited maturity;
- 1 point (high risk, orange)—minimal or superficial compliance with security standards;
- 0 points (critical risk, red)—absence of verifiable security practices or non-compliance with basic requirements.

Although the numerical labels of the ordinal scale are non-linear (5–3–1–0), this design does not imply proportional differences in risk magnitude. Rather, it intentionally encodes the asymmetry of operational consequences across risk categories, where movement toward high and critical risk states entails disproportionate impact on mission assurance. Accordingly, a score of 0 is not interpreted as a neutral or missing value, but as a critical condition reflecting demonstrably deficient security practices, the absence of verifiable security assurance, or the lack of support for the required security mechanism by the supplier, the organization, or the transit environment.

Conceptually, treating missing evidence as an "unknown" state would render the aggregation step undefined, as the DEFCHAIN model relies on complete numerical inputs to ensure deterministic, auditable, and reproducible computation of component and composite scores. In this sense, an "unknown" indicator state is operationally equivalent to a critical-risk condition for decision-support purposes, as both imply insufficient assurance for mission-critical reliance.

From a computational perspective, no alternative sensitivity analysis is defined for an "unknown" category, because excluding missing indicators or imputing neutral values

would change the mathematical structure of the aggregation function and violate the model's requirement for complete numerical inputs. Accordingly, the conservative assignment of missing values to 0 is not a tunable parameter but a structural design choice that ensures deterministic, auditable computation rather than an empirical assumption about underlying cybersecurity weakness.

From a security-assurance perspective, imputing missing indicators with neutral or average scores (e.g., 1 or 3) would introduce a systematic optimism bias by implicitly assuming partial compliance in the absence of verifiable evidence. In high-assurance military and defence environments, such assumptions are methodologically unsound, as they can conceal critical vulnerabilities behind documentation gaps. The conservative assignment of missing values to 0 therefore operationalizes a fail-safe design principle that prioritizes decision safety over score optimism and preserves the integrity of risk-based classification outcomes.

The impact of this non-linear spacing emerges only through subsequent aggregation and dynamic weighting within the DEFCHAIN model. At the indicator level, scores preserve ordinal ordering; their amplified effect is realized during later stages of risk integration and adaptation, rather than being embedded directly in the scoring scale itself.

While individual indicators are scored on a discrete ordinal scale {0, 1, 3, 5}, the aggregated component scores for S, T, and O are not used directly in raw point form for the dynamic computation. To ensure comparability across components with different numbers of indicators, each component score is converted into a percentage value prior to aggregation.

For each component, the raw score is divided by the maximum achievable score implied by the number of indicators assigned to that component and the maximum indicator value (5). The resulting percentage expresses the relative maturity of that component on a common 0–100 scale and is used as the numerical input for the weighted aggregation in Equation (4). Given the defined indicator structure, the normalization and aggregation scheme yield a maximum achievable S/T/O contribution of 300 points and a theoretical maximum static composite score of 330 points when the external factor Z is included as an additive contextual term.

If relevant data for a given indicator are unavailable or cannot be verified, the indicator is assigned a score of 0 (critical risk). In the context of military and defence supply chains, the absence of verifiable information implies an inability to confirm compliance with mandatory security requirements and therefore represents an elevated operational risk rather than a neutral condition. This conservative assumption reflects the security principle that lack of evidence cannot be interpreted as evidence of compliance, particularly in high-assurance environments.

In addition to its numerical role within the DEFCHAIN model, the scoring system incorporates a four-level color-coded scale to support operational decision-making. The colour mapping provides an intuitive visualization of risk concentrations within dashboards and command-level monitoring environments, enabling rapid identification of problematic areas without reliance on detailed numerical analysis.

The four-level structure aligns with colour-coded risk representations commonly used in security operations centres and command-and-control systems. Limiting the number of discrete risk states supports rapid situational awareness, reduces cognitive load, and facilitates unambiguous escalation and response decisions under time-critical conditions. The colour scheme does not influence the underlying mathematical computation but functions as an operational visualization layer that complements the quantitative assessment.

### *4.4. Evidence Rubric for Indicator Scoring and Verification*

While Section 4.3 defines the ordinal scoring logic and the conservative treatment of missing evidence, practical application of the model requires explicit clarification of acceptable evidence types and verification mechanisms. To this end, the study specifies representative evidence categories for each indicator type and formalizes the decision rule linking evidence presence, evidence quality, and score assignment (see Table 5).

In cases where relevant data for a given indicator are unavailable or cannot be verified, the model applies a missing-evidence penalty by assigning a score of 0 (critical risk). This conservative assumption ensures that, in high-assurance military environments, lack of evidence is not misinterpreted as compliance.

**Table 5.** Evidence rubric for indicator scoring and verification.

| Indicator (Example) | Acceptable Evidence Types | Scoring Rule | Verification Method |
|---|---|---|---|
| Supplier certifications | Valid certificates, audit reports | 5 = multiple valid; 3 = single valid; 1 = expired/partial; 0 = none | Document review |
| Cybersecurity clauses | Signed contracts, annexes | 5 = comprehensive; 3 = partial; 1 = generic; 0 = absent | Legal and policy review |
| Access control | IAM configs, MFA settings | 5 = MFA + RBAC; 3 = RBAC only; 1 = basic auth; 0 = unmanaged | Technical inspection |
| Incident response | IR plans, exercise reports | 5 = tested; 3 = documented; 1 = ad hoc; 0 = none | Policy and exercise review |
| Log monitoring | SIEM dashboards, retention configs | 5 = centralized; 3 = partial; 1 = local only; 0 = none | System artefact review |

### *4.5. Process*

Unlike most existing cybersecurity and risk management models, which rely on cyclic frameworks such as OODA (Observe–Orient–Decide–Act) or PDCA (Plan–Do–Check–Act), our approach is specifically tailored to the operational demands of military supply chains. These systems operate in dynamic, unpredictable, and adversarial environments where threats evolve rapidly, and linear decision cycles may be too slow or rigid. By applying the process of (1) sensing, (2) understanding, and (3) directing [55-56], we enhanced the cybersecurity model for supply chains, enabling improved detection, analysis, and risk management in complex supply systems. An important feature of this approach is that the phases are not executed linearly but operate in dynamic interdependence. This means that findings from any phase can serve as input for any other phase—not only for the one that logically follows in a classical scheme, but also for previous phases. Such an approach enables iterative adaptation and continuous improvement of the security model based on new insights and analyses, which is critical in ensuring resilient and mission-ready supply chains under military conditions.

In the sensing phase, the focus is on data collection and the identification of threats, vulnerabilities, and anomalies within the supply chain. This includes monitoring the security practices of suppliers and subcontractors, verifying compliance with security certifications, and observing network traffic and in-transit transactions. At the organizational level, it is necessary to conduct penetration testing, analyze security incident logs, and utilize advanced technologies such as SIEM (Security Information and Event Management) and IDS/IPS (Intrusion Detection/Prevention Systems), which enable real-time de-

tection of suspicious activity. Findings from this phase can directly impact the understanding phase, where data is analyzed but can also trigger a return to the sensing phase to adjust data collection methods.

The understanding phase involves the analysis and interpretation of collected data, enabling the organization to gain insight into risk patterns and potential attacks. This phase focuses on assessing supply chain vulnerabilities, modelling potential attack scenarios, and analyzing the behaviour of actors within the chain, including insider threats. Importantly, the findings from the understanding phase not only support the directing phase but may also prompt a revision of the sensing phase—for example, by identifying additional data that needs to be monitored.

In the directing phase, coordinated actions are taken based on the analyzed data to ensure cybersecurity in the supply chain. This includes implementing appropriate security measures, enhancing the architecture of the supply chain information systems, updating supplier contracts with cybersecurity clauses, and conducting joint testing with key partners. During transit, mechanisms for verifying transactions and ensuring the integrity and confidentiality of communications are applied. The measures adopted in the directing phase can influence the perception of risks and may lead to renewed analysis in the understanding phase or adjustments to the sensing methods.

By incorporating the process component, the cybersecurity model for supply chains evolves from a static structure into a dynamic system capable of real-time adaptation, as expressed in Equation (4). This transformation enables proactive risk management, enhances supply chain resilience, and improves protection against emerging cyber threats. Furthermore, it ensures that any new input—whether a data point, vulnerability, or external change—can influence all phases of the model, regardless of their original order.

In this dynamic formulation, cybersecurity $CS(t)$ at time $t$ is defined as a weighted sum of three core components: trust in suppliers ($S$), in-transit security ($T$), and internal cybersecurity measures ($O$). Each component is assigned a time-dependent weight—$w_S(t)$, $w_T(t)$, and $w_O(t)$, respectively—reflecting its relative importance at a given moment.

$$CS(t) = w_S(t)S + w_T(t)T + w_O(t)O \quad (4)$$

This dynamic approach enables the DEFCHAIN model to continuously respond to changing threat landscapes, evolving supplier risks, and shifts in operational or geopolitical environments.

The weights $w_S(t)$, $w_T(t)$, and $w_O(t)$ are not constant but change according to the perceived risk level $R(t)$, where $R(t)$ is based on real-time data from the sensing phase.

To calculate the dynamic weights used in the cybersecurity model, a logistic function is applied, as shown in Equation (5). This function allows the weight $w_i(t)$ to adapt in real time based on the perceived level of risk Ri(t) for each security factor I ∈ {$S$, $T$, $O$}, corresponding, respectively, to suppliers ($S$), in-transit security ($T$), and internal organizational protection ($O$).

These component-specific risk signals may take different values at the same time step, depending on situational conditions in each security dimension. Importantly, these risk inputs are treated as exogenous within a given evaluation cycle and are not updated based on the outputs of the model (including Z or $CS(t)$) until the next sensing phase, thereby avoiding circular causality.

The external-factor risk R(Z) is treated as a separate, dimension-specific input used solely in the computation of Z via Equation (7) and is not assumed to be numerically equal to R(S), R(T), or R(O). Its influence on perceived risk is incorporated only in subsequent evaluation cycles through updated sensing and understanding phases, rather than through immediate feedback within the same computational step.

Based on the previously defined logistic function, the weights were determined as follows:

- If the risk is low $Ri(t) \ll \theta i$, the weight $wi(t)$ remains low, as there is no reason to increase security.
- If the risk exceeds the threshold $Ri(t) \approx \theta i$, the weight rapidly increases and security measures become more important.
- If the risk is very high $Ri(t) \gg \theta i$, the weight approaches 1 (maximum influence), meaning that immediate action is required.

The steepness of the logistic curve is governed by the parameter $\lambda$, which controls how sensitively the weight responds to changes in risk. A higher value of $\lambda$ results in a sharper transition from low to high weighting as risk increases.

The incremental contribution of DEFCHAIN over conventional weighted indices is its dynamic weighting regime. By employing a logistic function, the model captures the non-linear escalation of risk, where specific security indicators gain disproportionate weight only when a critical risk threshold $\theta$ is breached. This distinguishes the framework from static scoring methods by allowing the system to prioritize different security dimensions based on real-time threat intensity:

$$w_i(t) = \frac{1}{1 + e^{-\lambda(R_i(t) - \theta_i)}} \quad (5)$$

This formulation ensures that the DEFCHAIN model remains responsive to fluctuating risk conditions by dynamically adjusting the influence of each security dimension according to current threat levels.

To support the proactive and forward-looking character of the DEFCHAIN model, the adjustment of cybersecurity measures over time is formalized through a differential equation, presented as Equation (6). This formulation enables the dynamic forecasting of how the overall cybersecurity level $CS(t)$ evolves in response to current risk conditions R(t), thereby facilitating timely and adaptive decision-making.

The equation expresses the rate of change in cybersecurity as the product of two terms: the gap between the current cybersecurity level $CS(t)$ and the theoretical maximum cybersecurity potential $CS_{max}$, and the perceived system-wide risk $R(t)$. The parameter $k$ denotes the adaptation speed, indicating how quickly cybersecurity capabilities within the supply chain adjust in response to emerging threats. A higher value of $k$ corresponds to a faster response and greater adaptability, whereas a lower value reflects more gradual improvements.

$$\frac{dCS(t)}{dt} = k(CS_{max} - CS(t)) \cdot R(t) \quad (6)$$

This dynamic formulation ensures that, as perceived risk increases, the system accelerates its progression toward the optimal cybersecurity state. Conversely, when risk is low, or the current level $CS(t)$ is close to $CS_{max}$, the adjustment becomes more gradual. It reinforces the core DEFCHAIN principle that cybersecurity in supply chains should not remain static but be continuously recalibrated based on real-time threat dynamics.

Ultimately, the use of this differential equation enables both real-time adjustment and strategic foresight. It allows decision-makers to anticipate the future security posture of the supply chain and implement timely interventions—well before critical thresholds are reached.

### *4.6. Parameterization and Discriminative Behaviour of the Dynamic Weighting Mechanism*

The logistic weighting function in the DEFCHAIN model is parameterized using two primary control variables: responsiveness ($\lambda$) and the risk threshold ($\theta$). These parameters

are not intended as empirical estimates derived from historical data; rather, they function as structural controls that encode specific organizational response postures and decision doctrines. Component-specific values of ($\lambda$, $\theta$), therefore, reflect analytical assumptions regarding how rapidly, and at what perceived risk level, different security dimensions are prioritized. For example, a lower threshold $\theta$ for in-transit security (T) relative to organizational cybersecurity (O) reflects a doctrinal assumption that prioritizes immediate logistical integrity over internal process maturity during periods of heightened environmental volatility.

In the worked example, weights approaching unity (e.g., $w \approx 0.95$–$0.98$) occur under elevated environmental risk conditions. This behaviour is intentional: once perceived risk exceeds the component-specific threshold, the model transitions from proportional weighting to a regime of priority dominance, ensuring that the affected component exerts a strong influence on the composite score. Importantly, discriminative power in DEFCHAIN does not arise from absolute weight magnitude alone, but from the interaction between dynamic weights and heterogeneous static baseline scores (S, T, O). Even when multiple weights approach unity, differences in underlying component conditions continue to produce differentiated composite outcomes.

Environmental risk inputs R(t) are evaluated on a bounded ordinal scale, with representative values spanning low (≈0.10), elevated (≈0.40), and high-to-critical (≈0.75) conditions. Sensitivity analysis shows that material changes in dynamic weighting occur primarily in the transition region around $\theta$. When $R(t) \ll \theta$, the model behaves quasi-statically, whereas when $R(t) \gg \theta$, it enters a regime of sustained prioritization. Consequently, the purpose of the dynamic weighting mechanism is not continuous fine-grained modulation across the entire risk spectrum, but a stable, regime-dependent reconfiguration of component importance under escalating threat conditions.

### *4.7. External Factors*

The cybersecurity of supply chains is subject to numerous external factors, which are not merely static parameters but dynamically interact and change depending on circumstances. We identified the following external factors: (1) resources, (2) knowledge, (3) threats, (4) military factors, (5) resilience, and (6) external environment. These factors do not operate independently but are in constant interaction, where a change in one can affect the others.

For example, a negative external factor may represent heightened geopolitical tension or legal uncertainty affecting supplier access, while a positive factor may reflect strong alliance-based cooperation, regulatory alignment, or shared threat intelligence that mitigates overall supply chain risk.

Each of these factors was quantified using a scoring system based on a unified evaluation framework, which ensures the comparability of results and enables their integration into a broader mathematical model for security risk assessment. This allows for dynamic monitoring of the impact of individual factors and their inclusion in decision-making, enabling organizations to proactively adapt their security strategies based on current conditions and future trends.

External factors play an important role in shaping the cybersecurity posture of supply chains, particularly in military and defence contexts. Each factor—ranging from available resources to geopolitical dynamics—can act either as an enabler or as a constraint. When favourable, these conditions can enhance system resilience, improve detection and response capabilities, and support coordinated action across domains. However, when unfavourable or misaligned, they may introduce vulnerabilities, create bottlenecks in coordination, and limit the effectiveness of cybersecurity strategies. A comprehensive un-

derstanding of these factors and their dual potential is essential for assessing risk, designing adaptive security models, and ensuring the continuity and integrity of supply chain operations under both normal and contested conditions.

To account for the influence of contextual and environmental conditions within the DEFCHAIN model, external factors were mathematically integrated to either mitigate or intensify the perceived cybersecurity risk. Specifically, positive factors—denoted as R5 and R3, such as supportive regulations or allied cooperation—contribute to lowering the effective risk, while negative factors—represented by R1 and R0, such as legal ambiguity or geopolitical tension—amplify it. An amplification factor F is applied to the most critical vulnerabilities to reflect their disproportionate impact on the system.

Importantly, the formulation includes the function max(1, $R_0$), which ensures that even if the negative factor $R_0$ is rated zero, it still contributes to the risk calculation, preventing total neutralization of its influence. This safeguards against underestimating latent or emerging risks.

The resulting expression, shown in Equation (7), calculates the net impact of external influences on supply chain security ($Z$) as a function of perceived risk $R(t)$, the nature of external conditions, and the amplification factor $F$. Each external factor variable ($R_0$, $R_1$, $R_3$, $R_5$) represents an aggregated ordinal score derived from a predefined set of qualitative indicators evaluated using the same scoring methodology applied to internal factors. These indicators capture observable operational conditions such as regulatory alignment, alliance cooperation, geopolitical constraints, resource availability, and strategic resilience. As a result, the variables retain explicit operational meaning and are grounded in measurable assessment inputs rather than abstract constructs. While the aggregation form is intentionally parsimonious, it does not assume independence or linear causality between external factors. Instead, synergistic and antagonistic effects are reflected through factor valuation, polarity, and the amplification term, rather than through explicit interaction terms.

These external factors are treated as contextual modifiers rather than independently optimized variables, reflecting their role in shaping—but not determining—the internal cybersecurity posture of the supply chain.

$$Z = (1 - R(t)) \cdot (R_5 + R_3) - R(t) \cdot F \cdot (R_1 + \max(1, R_0)) \quad (7)$$

This integration allows DEFCHAIN to dynamically incorporate geopolitical, regulatory, and strategic variables into cybersecurity assessments, reinforcing its capacity to reflect complex, real-world environments in a robust and adaptive way.

The cybersecurity model for armed forces supply chains provides a systematic approach to risk management and the adaptation of security measures in response to a dynamic threat environment. By combining factors and indicators, an iterative process, and external influences, the model goes beyond traditional static assessment methods and enables the dynamic adjustment of security strategies. It is designed to allow organizations to perform a quantified analysis of vulnerabilities, effectively detect and understand threats, and direct security measures based on data-driven decisions. The integration of external factors ensures a broader context for cybersecurity management, enabling greater preparedness for modern cyber challenges. Such a model enables the armed forces not only to enhance their resilience against cyber threats but also to improve adaptability and proactively manage security risks in complex supply chain systems.

### *4.8. Overall Dynamic Risk Assessment*

To determine the overall dynamic risk assessment, we developed a scale (see Tables 6 and 7) that enables classification of risk based on the cumulative value of security factors

and perceived threats. The system is based on four levels of risk, defined by score thresholds, where higher values indicate a better security posture and lower values suggest an increased risk of security incidents. The scale allows for straightforward interpretation of results, as the defined boundaries represent transitions between low, medium, high, and critical risk levels. To ensure comparability and consistency across different components and evaluations, all values used in this risk scale have been normalized to a common percentage-based scale. This enables the system to dynamically adjust its security measures according to current conditions and perceived threats, ensuring appropriate responses for effective risk management.

**Table 6.** Scale for overall dynamic risk assessment.

| Points | Risk Level | Colour Scale | Description |
|---|---|---|---|
| 200–330 | Low risk | Green | Security measures are appropriate and effective. No significant vulnerabilities or incidents have been detected. Compliance with security standards is high. The system is resilient to most threats. |
| 150–199 | Medium risk | Yellow | There are minor security deficiencies that should be addressed. Security incidents are possible, but no critical vulnerabilities are present. Regular monitoring and improvements are recommended. |
| 100–149 | High risk | Orange | Significant security deficiencies are present. There is a high likelihood of security incidents. Security measures are insufficient or improperly implemented. Immediate security improvements are required. |
| 0–99 | Critical risk | Red | Very high likelihood of security incidents or active attacks. Lack of basic security measures, high system vulnerability. Rapid and comprehensive security actions are urgently required; otherwise, there is a serious security threat. |

**Table 7.** General evaluation scale converted to percentages.

| Risk Level | Percentage | Colour Scale |
|---|---|---|
| Low risk | 80–100 | Green |
| Medium risk | 50–79 | Yellow |
| High risk | 20–49 | Orange |
| Critical risk | 0–19 | Red |

### *4.9. Validation of Model Consistency and Mathematical Correctness*

The DEFCHAIN model was validated through a comprehensive mathematical and combinatorial verification process covering the entire defined domain of static and dynamic inputs. The purpose of this validation was not empirical performance assessment, but confirmation of internal consistency, numerical stability, and correctness of all model transformations prior to analytical or operational use.

At the input level, the static part of the model is defined by 52 discrete indicators evaluated on a unified four-level ordinal scale, yielding a theoretical configuration space of $4^{52}$ possible static input combinations. Rather than treating this space as a monolithic set, validation was performed through a structured decomposition into four independent

component groups: supplier trust (S), in-transit security (T), organizational cybersecurity (O), and external factors (Z). This decomposition enables systematic enumeration and verification within each component while preserving full coverage of the overall indicator space.

Validation was conducted separately for each static component. Within each component, all theoretically admissible combinations of indicator values were enumerated and evaluated, allowing explicit verification of value ranges, linear normalization procedures, boundary conditions, and absence of numerical anomalies. Extreme configurations, including fully optimal and fully critical states, were explicitly included for each component, ensuring robustness of the static model under boundary conditions.

The results of this component-level enumeration and normalization yield 331 admissible static composite score values, which collectively preserve the ordering, boundary behaviour, and discriminatory structure implied by the full indicator-level configuration space. This reduction represents a deterministic aggregation of fully enumerated component outcomes rather than a sampling or approximation of the underlying indicator combinations.

The dynamic component of the model, based on logistic weighting as a function of perceived risk, was validated independently. Sensitivity parameters ($\lambda$), threshold values ($\theta$), and environmental risk levels (R) were discretized to represent qualitatively distinct response regimes. All defined combinations of these parameters were explicitly evaluated. Validation confirmed that the weighting function remains bounded within the unit interval, exhibits monotonic behaviour with respect to risk, and satisfies the theoretical properties of the logistic function, including correct positioning of the inflection point. No numerical instabilities or discontinuities were observed across the evaluated parameter space.

Integration of static and dynamic components was validated by verifying that dynamic values never exceed their static counterparts, that zero-valued static components remain zero after weighting, and that increasing risk consistently leads to non-increasing dynamic outputs. This confirms internal coherence between the static assessment layer and the dynamic adaptation mechanism.

Finally, a global combinatorial validation was performed by combining the 331 admissible static composite outcomes with the 1210 validated configurations of dynamic weights, yielding a total of 400,510 unique theoretical configurations of the composite score CS(t). All configurations were explicitly computed within the defined parameter ranges, demonstrating that the DEFCHAIN model operates correctly across its entire admissible configuration space and produces stable, bounded, and interpretable outputs for all combinations.

Overall, the validation results demonstrate that the DEFCHAIN model is mathematically sound, internally consistent, and robust across its full defined domain. The model's behaviour is predictable under both typical and extreme conditions, providing a reliable and reproducible foundation for the simulation-based analysis presented in this study and for future empirical applications.

To ensure full reproducibility, Figure 2 outlines the deterministic computational mapping of the DEFCHAIN model. The same computational logic is summarized in Algorithm 1 to provide an auditable and implementation-neutral description of the calculation sequence. The process starts with scoring 52 indicators for the S, T, O and Z dimensions. These are transformed into ordinal values using the ordinal scoring logic defined in Table 4 and the evidence rubric defined in Table 5. The dynamic weights are then computed via Equation (5), leading to the composite cybersecurity score CS(t) as defined in Equation (4) and updated over time through the adaptation logic in Equation (6). In the

event of missing indicator data, the model follows a conservative security principle by assigning a score of 0 (critical risk).

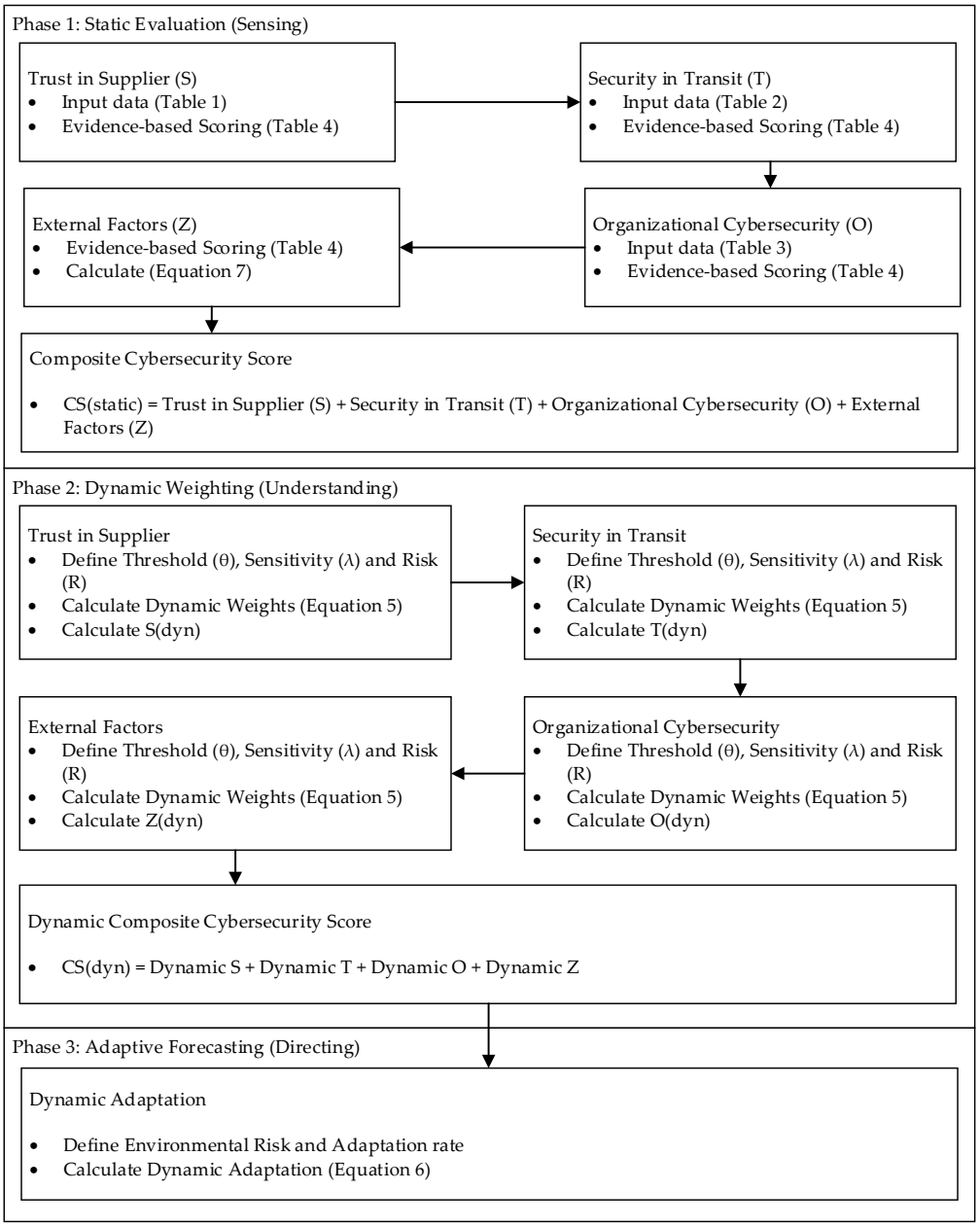


**Figure 2.** DEFCHAIN computational sequence and logic flow.

**Algorithm 1.** Deterministic computational sequence of the DEFCHAIN model, mapping indicator scores to the composite cybersecurity score CS(t).

Input:

– Indicator scores Ii ∈ {0, 1, 3, 5} for S, T, O, Z.
– Perceived risk level R(t) ∈ [0, 1].
– Model parameters λ, θ, k.

Steps:

1. Aggregate indicator scores into component values S, T, O and normalize them to [0, 100].
2. Compute dynamic weights wi(t) using the logistic weighting function (Equation (5)).

3. Compute the composite cybersecurity score CS(t) and update it over time using the adaptation equation (Equation (6)).

Missing data handling:

– If an indicator value Ii is unavailable or unverifiable, assign Ii = 0 (critical risk).

Output:

– Composite cybersecurity score CS(t) and associated risk level classification.

The reproducibility of the DEFCHAIN model is ensured through a deterministic three-step process:

1. Indicator Aggregation: Each of the 52 indicators is scored according to the logic in Table 4.
2. Component Normalization: Scores for S, T, and O are aggregated and normalized to a percentage scale (0–100%), while external factor Z is processed according to its defined impact scale.
3. Dynamic Computation: The final state CS(t) is calculated by applying the logistic weights from Equation (5) and solving the differential Equation (6). This ensures that, given the same initial indicator scores, the model consistently produces the trajectories shown in Figures 3–5 in the subsequent section.

### *4.10. Simulation Results and Model Behaviour*

To assess the behaviour of the DEFCHAIN model under controlled and reproducible conditions, a scenario-based deterministic simulation was conducted. The simulation framework was designed to analyze model behaviour across systematically constructed scenarios, enabling observation of temporal dynamics, parameter sensitivity, and regime-dependent responses. Rather than aiming to reproduce a specific real-world supply chain, the simulation serves to demonstrate how the model behaves under clearly defined combinations of static baseline conditions, environmental risk, response policies, and organizational adaptation capacity.

A total of 800 static scenarios were generated and evenly distributed across four predefined risk categories: low, medium, high, and critical. Across all combinations of static scenarios, environmental risk levels, response regimes, and adaptation rates, the simulation evaluated a total of 21,600 distinct scenario trajectories, each producing a complete 60-day time series of the composite security score. Each scenario represents a distinct configuration of cybersecurity indicators derived from the DEFCHAIN factor structure, encompassing supplier trust, in-transit security, organizational cybersecurity posture, and external contextual factors. Indicator values were assigned using the ordinal scoring methodology described earlier and aggregated into an initial composite security score representing the static baseline state of the system. This balanced distribution ensures uniform coverage of the static risk spectrum and enables direct comparison of model behaviour across different baseline conditions.

Environmental risk was modelled as an exogenous input parameter and held constant within each simulation run. Three discrete risk levels were examined: low environmental risk (R = 0.10), elevated but non-crisis risk (R = 0.40), and high to near-critical risk (R = 0.75). These values represent qualitatively distinct operational environments and allow clear interpretation of model behaviour under increasing external pressure without continuous fine-tuning of risk intensity.

Different organizational response postures were captured through paired combinations of response sensitivity and risk threshold parameters, grouped into three response regimes. The stable regime represents softly responsive systems with higher tolerance to

risk and gradual activation of security measures. The balanced regime reflects an operationally realistic configuration suitable as a default reference. The threshold-driven regime represents highly responsive systems in which relatively small increases in perceived risk trigger rapid and pronounced adaptation. For a given environmental risk level, the response function remained constant throughout the simulation horizon, ensuring that observed temporal changes were driven by adaptation dynamics rather than fluctuating threat inputs.

Parameter values used in the simulation were selected to represent qualitatively distinct operational regimes and response behaviours, rather than calibrated to a specific empirical system or dataset.

Organizational adaptation was modelled as a first-order dynamic process over a 60-day horizon, representing gradual adjustment of security measures under sustained environmental pressure. Three adaptation rates were examined, corresponding to slow, balanced, and rapid organizational responses. These rates reflect different levels of organizational agility and resource mobilization capacity and allow separation of adaptation speed from the effects of risk intensity and response policy.

For each static scenario, the simulation produced multiple temporal trajectories corresponding to different combinations of response regime and adaptation rate. This structure enables direct comparison of how sensitivity thresholds and organizational agility influence both the pace and extent of security adaptation. A balanced configuration of parameters ($\lambda = 2$; $\theta = 0.3$; $k = 0.08$; $R = 0.40$) was used as a baseline reference to support comparative interpretation and sensitivity analysis.

Taken together, the simulation design enables multidimensional analysis of model behaviour, allowing the effects of static baseline conditions, perceived environmental risk, response policy, and organizational adaptability to be examined both independently and in combination. The resulting outputs illustrate how the DEFCHAIN model differentiates between static risk exposure, environmental pressure, and organizational responsiveness, and how these elements interact over time to shape the evolution of the composite security score. The following figures present the observed temporal patterns, parameter effects, and aggregated outcomes across scenario classes.

Figure 3 presents the time evolution of the composite cybersecurity score CS(t) over a 60-day horizon under six different responsiveness configurations defined by pairs of sensitivity $\lambda$ and threshold $\theta$. All trajectories exhibit a smooth and monotonic increase in CS(t) over time, indicating stable dynamic behaviour of the model without oscillations or numerical instabilities.

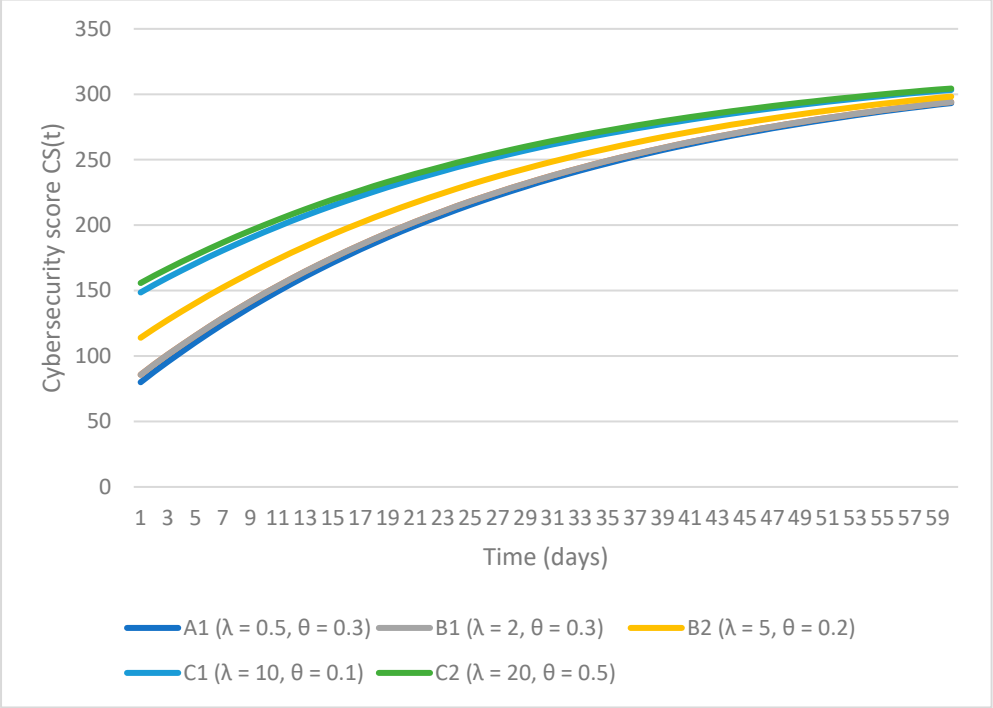


**Figure 3.** Time evolution of the cybersecurity score CS(t) under different responsiveness configurations ($\lambda$, $\theta$).

Differences between responsiveness configurations are most pronounced in the early phase of the simulation. Configurations with higher sensitivity and lower threshold values (C1 and C2) display higher initial response levels and faster early growth of the cybersecurity score compared to more softly responsive configurations (A1 and A2). In contrast, stable configurations with lower sensitivity parameters start from lower baseline values and exhibit more gradual convergence.

As time progresses, the trajectories increasingly converge, and differences between configurations diminish. By the end of the simulation horizon, all configurations approach a similar asymptotic range of cybersecurity scores, suggesting that responsiveness parameters primarily affect the pace of adaptation rather than the long-term attainable security level under fixed environmental risk conditions.

Overall, the figure illustrates that variations in ($\lambda$, $\theta$) influence short- to mid-term dynamics of security adaptation, while the long-term behaviour of the model remains bounded and consistent across responsiveness regimes.

Figure 4 illustrates the influence of the adaptation rate parameter k on the dynamic evolution of the composite cybersecurity score CS(t) over a 60-day simulation horizon. All trajectories originate from the same static baseline value, indicating identical initial conditions, and diverge over time solely as a consequence of different adaptation rates.

Clear differences are observed in the speed of increase in CS(t). The configuration with a high adaptation rate (k = 0.20) exhibits a rapid initial rise and approaches its asymptotic range within the first half of the simulation period. In contrast, the moderate adaptation rate (k = 0.08) results in a more gradual increase, while the slow adaptation configuration (k = 0.03) shows the slowest progression throughout the entire time horizon.

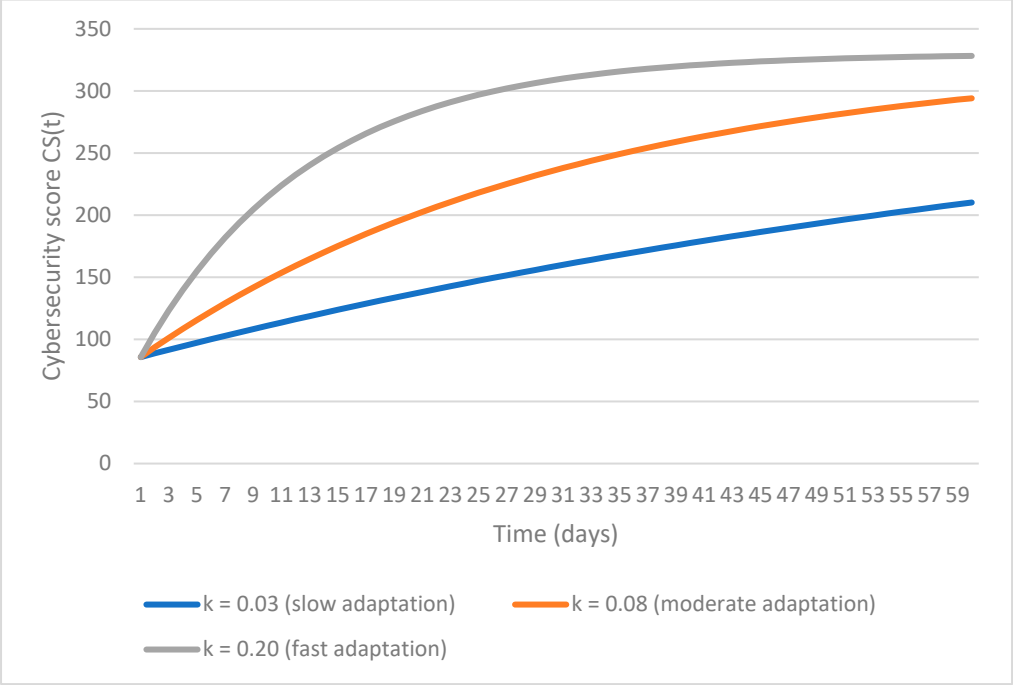


**Figure 4.** Influence of the adaptation rate parameter k on the dynamic evolution of CS(t).

Despite substantial differences in convergence speed, the trajectories preserve a consistent ordering over time, and no abrupt changes or instabilities are observed. The separation between curves remains pronounced across the full simulation window, highlighting the sustained effect of adaptation rate on the temporal profile of security improvement.

Overall, the figure demonstrates that variation in the adaptation rate parameter primarily affects the pace at which the cybersecurity score evolves, producing distinct temporal trajectories under otherwise identical conditions.

Figure 5 shows the impact of different values of the responsiveness parameter $\lambda$ on the time evolution of the composite cybersecurity score CS(t), while the threshold parameter is held constant at $\theta = 0.3$. All trajectories originate from the same static baseline and evolve smoothly over the 60-day simulation horizon, indicating stable model behaviour under varying sensitivity settings.

Differences between curves are visible primarily in the early and mid-stages of the simulation. Higher values of $\lambda$ result in consistently higher values of CS(t) throughout the time horizon, reflecting a stronger response intensity under identical threshold and environmental conditions. Lower values of $\lambda$ produce more gradual growth, with the corresponding trajectories remaining below those associated with higher sensitivity settings.

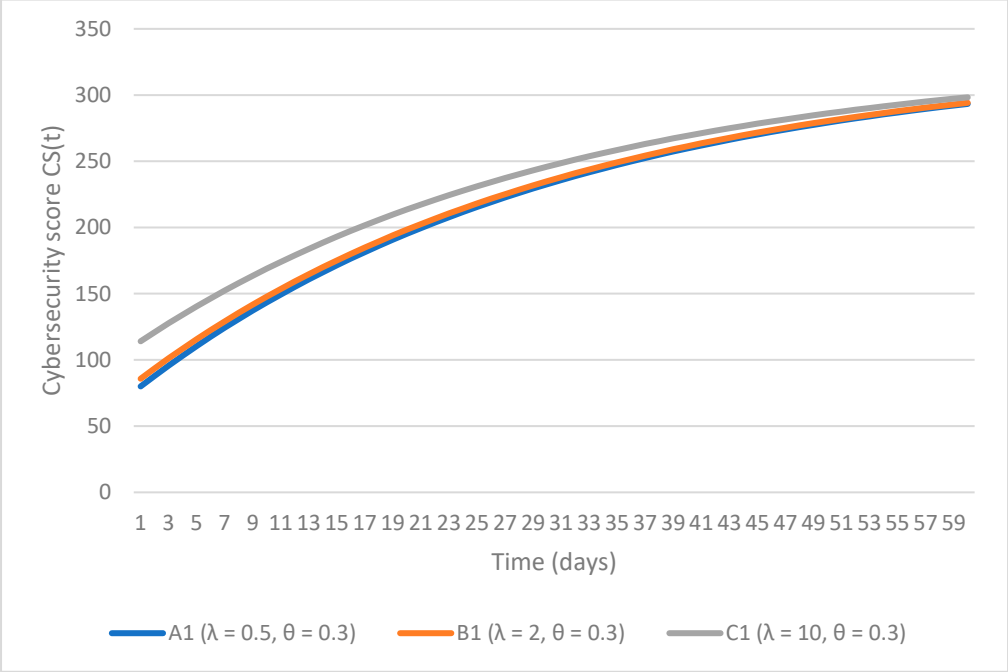


**Figure 5.** Impact of different $\lambda$ values on CS(t) with fixed threshold $\theta = 0.3$.

As time progresses, the trajectories exhibit gradual convergence, and the relative separation between curves diminishes. By the end of the simulation period, differences in CS(t) across $\lambda$ values are reduced, suggesting that the sensitivity parameter primarily influences the magnitude and pace of the response during earlier phases of adaptation rather than determining the long-term asymptotic level of the cybersecurity score.

Overall, the figure illustrates that variations in the responsiveness parameter $\lambda$, when evaluated under a fixed threshold, modulate the strength of the dynamic response without introducing instability or altering the bounded nature of the system.

Figure 6 presents the average composite cybersecurity score obtained from the DEFCHAIN simulation for each responsiveness configuration, together with the associated variability expressed by standard deviation. Bars represent mean values of the cybersecurity score, while error bars correspond to ± one standard deviation around the mean for each configuration.

The results show a systematic increase in average cybersecurity scores when moving from softly responsive configurations (A1, A2) toward more sensitive and threshold-driven configurations (C1, C2). This pattern is consistent across all evaluated parameter groupings, indicating that responsiveness settings influence the central tendency of the resulting security scores.

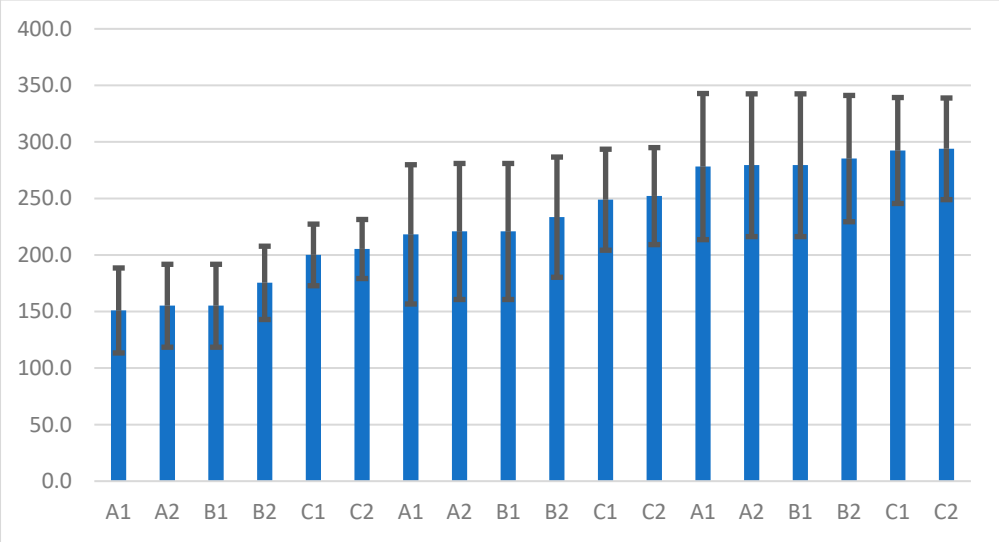


**Figure 6.** Average cybersecurity score with standard deviation bars. The blue bars denote the mean composite cybersecurity score for each responsiveness configuration, while the grey vertical error bars indicate the corresponding ± one standard deviation, reflecting variability across simulated scenario trajectories.

Each bar represents the mean composite cybersecurity score computed across all simulated static baseline scenarios for a given responsiveness configuration, while the standard deviation reflects dispersion across the corresponding set of scenario trajectories. The labels A1–C2 denote predefined combinations of the responsiveness parameter $\lambda$ and the risk threshold $\theta$, grouped into softly responsive (A), balanced (B), and threshold-driven (C) regimes, as defined in the simulation setup.

The magnitude of the standard deviation varies between configurations, reflecting differences in outcome dispersion across simulated scenarios. More responsive configurations exhibit larger standard deviations, indicating greater sensitivity to variations in static baseline conditions and dynamic adaptation paths. In contrast, less responsive configurations show smaller standard deviations, suggesting more stable but less adaptable security outcomes.

Overall, the figure summarizes the aggregated effects of responsiveness parameters on both the expected cybersecurity score and the variability of outcomes, providing a compact representation of central tendencies and dispersion across the simulated configuration space.

Figure 7 illustrates the relative sensitivity of the DEFCHAIN model to its key parameters: responsiveness ($\lambda$), threshold ($\theta$), adaptation rate (k), and environmental risk (R). The displayed values represent normalized sensitivity measures, enabling direct comparison of the relative influence of each parameter on the resulting composite cybersecurity score.

The results indicate marked differences in parameter sensitivity. The threshold parameter $\theta$ exhibits the highest sensitivity value, followed by environmental risk R and the adaptation rate k. In contrast, the responsiveness parameter $\lambda$ shows a substantially lower sensitivity relative to the other parameters.

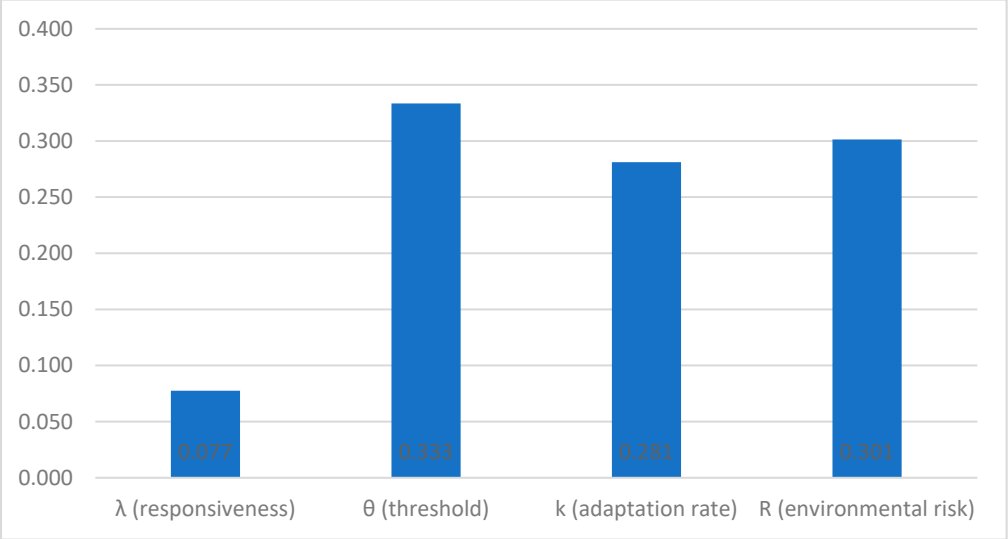


**Figure 7.** Sensitivity of the DEFCHAIN model to key parameters.

This ordering demonstrates that variations in decision thresholds and external risk conditions are associated with larger changes in model output than equivalent variations in response intensity. The comparatively lower sensitivity of $\lambda$ suggests a more moderating role in shaping model behaviour under the examined parameter ranges.

Overall, the figure provides a concise summary of the relative influence of core model parameters, highlighting which dimensions most strongly affect the resulting cybersecurity score within the evaluated configuration space.

It should be emphasized that the presented simulation results do not constitute an empirical validation of the DEFCHAIN model. Instead, the simulation serves as a structural and behavioural verification of model dynamics under controlled and reproducible conditions, complementing the analytical validation presented earlier by focusing on stability, parameter sensitivity, and internal consistency rather than predictive accuracy in real-world environments.

### *4.11. Behaviour of the Logistic Weighting Function in the DEFCHAIN Model*

The behaviour of the logistic weighting function used in the DEFCHAIN model is illustrated through a series of analytical visualizations that examine the effects of the responsiveness parameter $\lambda$, the risk threshold $\theta$, and their interaction with the perceived environmental risk R.

The first set of curves (Figure 8) shows the logistic weight w(R) for a fixed threshold value ($\theta = 0.05$) under varying values of the responsiveness parameter $\lambda$. For low values of $\lambda$, the weighting function exhibits a shallow slope, resulting in a gradual increase in w(R) across the entire risk interval. As $\lambda$ increases, the transition becomes progressively steeper and increasingly concentrated around the threshold value. At high $\lambda$ values, the function approaches a near step-like behaviour, where small changes in risk around $\theta$ produce disproportionately large changes in the weighting value. This confirms that $\lambda$ primarily controls the sharpness of the response rather than the location of the transition.

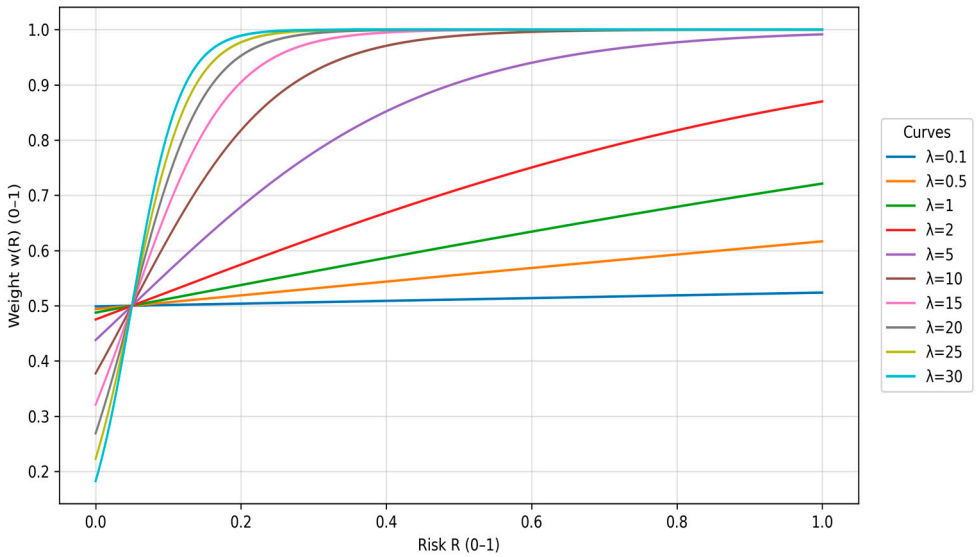


**Figure 8.** Effect of responsiveness parameter $\lambda$ on the logistic weight w(R) at fixed threshold ($\theta$ = 0.05).

The three-dimensional surface visualization further illustrates the combined influence of $\lambda$ and $\theta$ on the weighting function w(R) (Figure 9) for a fixed environmental risk level (R = 0.4). The surface shows smooth and bounded behaviour across the entire parameter space. Increasing $\lambda$ amplifies the sensitivity of the weight to deviations from the threshold, while increasing $\theta$ shifts the transition region toward higher risk values. The surface does not exhibit discontinuities or numerical instabilities, confirming the mathematical robustness of the weighting formulation.

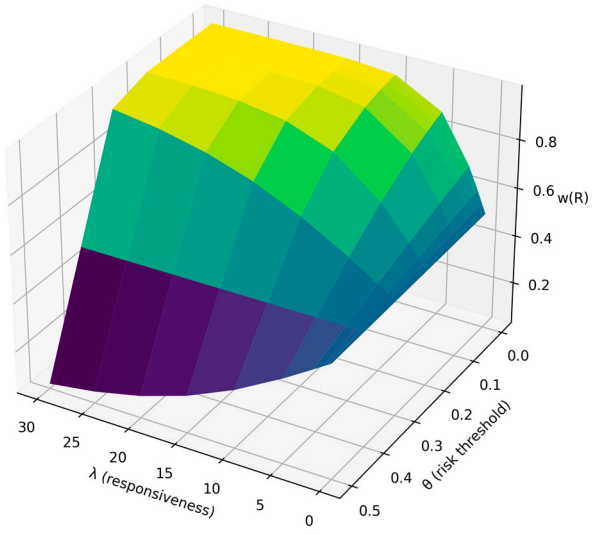


**Figure 9.** Joint influence of responsiveness ($\lambda$) and risk threshold ($\theta$) on the logistic weight w(R) at fixed environmental risk (R = 0.4). The surface color encodes the magnitude of the weighting function w(R), with darker (blue–purple) tones indicating lower values and lighter (green–yellow) tones indicating higher values of w(R).

The corresponding heat map (Figure 10) representation provides a compact overview of the same relationship. Regions of high weighting values emerge where the perceived risk exceeds the threshold under sufficiently high responsiveness settings. Conversely, for higher threshold values or lower responsiveness, the weighting remains moderate even

at elevated risk levels. The heat map highlights clear structural regimes in parameter space, demonstrating how different combinations of λ and θ map perceived risk into qualitatively distinct response intensities.

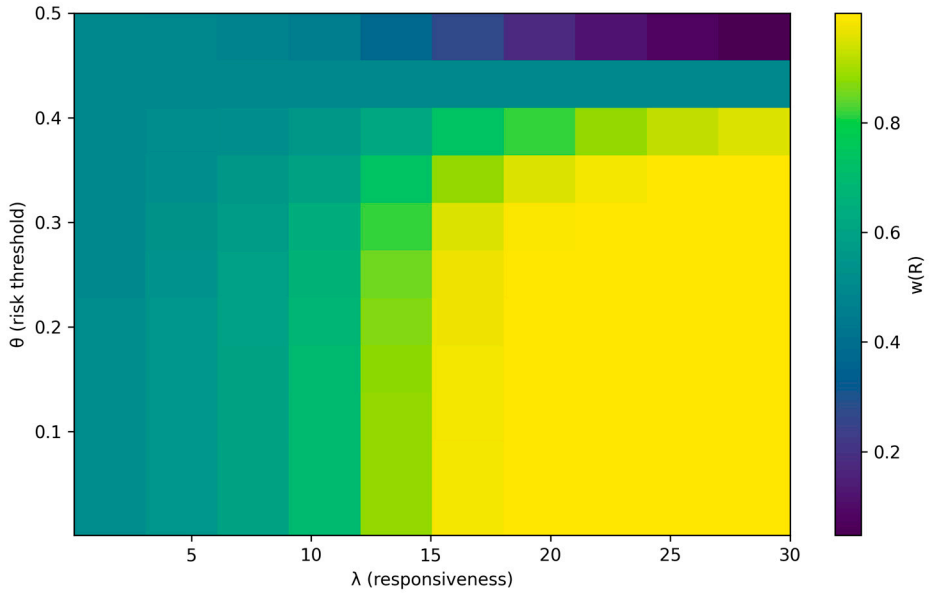


**Figure 10.** Heat map of the logistic weight w(R) as a function of responsiveness (λ) and risk threshold (θ) at R = 0.4.

The final set of curves (Figure 11) illustrates the effect of varying the threshold parameter θ while holding the responsiveness parameter constant (λ = 10). The results show a systematic horizontal shift in the logistic function along the risk axis. Lower values of θ cause the transition to occur at lower risk levels, while higher θ values delay the onset of strong weighting until higher risk is perceived. All curves intersect at w(R) = 0.5 when R = θ, confirming the analytical property of the logistic function and validating the correct implementation of the threshold mechanism.

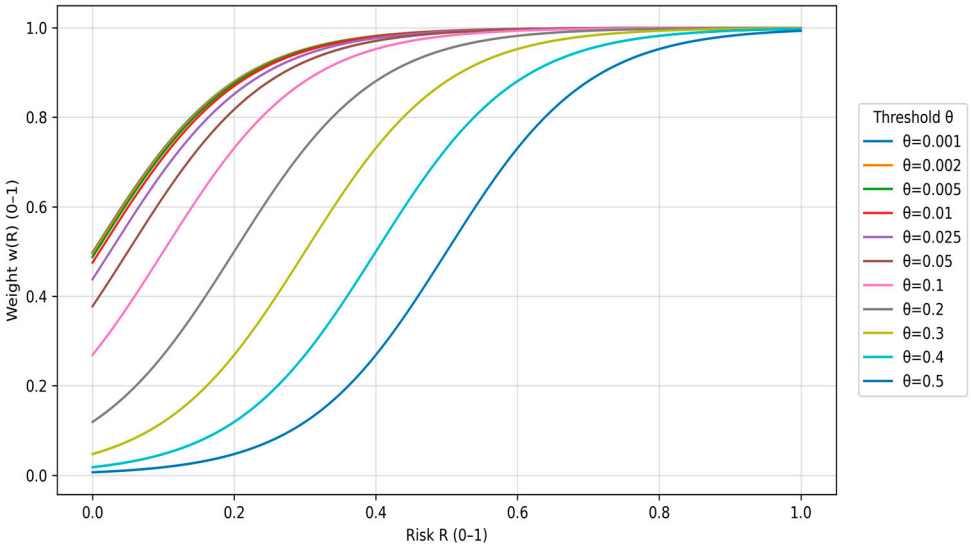


**Figure 11.** Logistic weight w(R) for different risk thresholds (θ) at fixed responsiveness (λ = 10).

Taken together, these results demonstrate that the DEFCHAIN weighting mechanism behaves in a predictable, continuous, and bounded manner across the full examined

parameter space. The visualizations confirm that $\lambda$ governs response intensity, $\theta$ determines the location of the transition, and their interaction defines the regime under which perceived environmental risk is translated into dynamic weighting within the model.

## 5. Discussion

This chapter provides a comprehensive interpretation of the research findings by analyzing the performance, applicability, and implications of the DEFCHAIN model in the context of cybersecurity in military supply chains. Building on the results of the model's development and comparative assessments, the discussion reflects on how the model addresses the key research questions and contributes to the advancement of risk-based cybersecurity management. It highlights the strengths of the proposed approach, such as its ability to integrate dynamic adaptation, predictive capability, and external influencing factors, while also acknowledging its limitations in terms of implementation complexity, empirical validation, and future adaptability. The discussion further explores the practical implications of the model, its scalability, and potential avenues for refinement and operational deployment within defence environments.

Literature review applied a rigorous, criteria-based methodology to evaluate the alignment of existing scholarly work with the DEFCHAIN model for cybersecurity in military supply chains. Despite a growing volume of research addressing cyber risks, resilience, and advanced technologies, the findings show that most studies exhibit only partial alignment—or none at all—with DEFCHAIN's integrated framework. While some contributions offer valuable insights into conceptual models, technical tools, or specific indicators, only a handful propose structured, quantifiable, and adaptive approaches comparable to DEFCHAIN. Notably, no study implements a model that simultaneously incorporates all three of DEFCHAIN's core components: risk factors and indicators, a dynamic process cycle, and external environmental dimensions. This gap confirms the originality of DEFCHAIN and underscores its value as a foundational model for future empirical research into cybersecurity resilience within military logistics environments.

The findings of this study confirm that a dynamic, mathematically structured approach—exemplified by the DEFCHAIN model—provides an analytically grounded mechanism for structured cybersecurity management in military supply chains compared to traditional static methods. By incorporating quantifiable indicators, adaptive processes, and external influencing factors, the model bridges a key research gap: it provides a tailored, operationally relevant tool for defence logistics, offering a practical way to evaluate and respond to cyber risks in real time.

One of the most significant outcomes is the demonstration that all three main cybersecurity dimensions—trust in suppliers, security in transit, and internal organizational resilience—can be systematically assessed using a unified, weighted scoring system. This system provides both snapshot evaluations and trend forecasting capabilities. The ability to calculate dynamic risk levels and simulate the impact of adaptive security responses over time represents a major advancement over checklist-based or compliance-only frameworks.

Notably, the model proves effective in distinguishing risk profiles between different suppliers and operational scenarios. Through the comparative analysis of multiple scenario-based configurations, the DEFCHAIN framework demonstrated its ability to differentiate between static vulnerability profiles and to capture how dynamic conditions—such as changing threat levels or fluctuating external factors—affect the overall cybersecurity posture. This dynamic adaptability is crucial in defence environments, where real-time changes in risk must be met with proportional and timely mitigation strategies.

An important added value lies in the inclusion of external factors—such as resource availability, geopolitical context, and organizational resilience—into the core risk model.

These are traditionally treated as contextual or qualitative elements, but here they are operationalized into the mathematical core of the model. This allows military decision-makers to consider broader strategic elements, such as shifting alliances or supply volatility, in the same decision-support framework as technical indicators.

Furthermore, the model's predictive capabilities are supported by the use of logistic functions and differential equations that govern the rate and intensity of security adjustments based on observed threats. This offers a realistic simulation of how organizations can adapt over time—both rapidly in crisis and gradually under stable conditions.

Nevertheless, while the model is conceptually and mathematically robust, its full operationalization depends on the availability of quality data and trained personnel. The simulations used to validate the model illustrate its theoretical potential, but empirical validation in live military environments remains necessary to confirm its full applicability and resilience under adversarial conditions.

The DEFCHAIN model does not assume complete or real-time availability of supplier data. Instead, it is explicitly designed to operate under conditions of information asymmetry and partial observability, which are characteristic of military and defence supply chains. In cases where indicator data are unavailable, unverifiable, or inconsistent—particularly among small and medium-sized suppliers—the model applies conservative scoring assumptions, treating limited transparency itself as an elevated risk rather than a neutral condition. This design choice reflects operational security principles in high-assurance environments, where uncertainty and restricted visibility are integral components of risk rather than exceptions and must be explicitly accounted for in decision-making. This conservative treatment of missing indicator data is consistent with the scoring methodology described earlier, where unverifiable conditions are explicitly modelled as elevated operational risk rather than as supplier non-compliance.

The DEFCHAIN model represents a significant advancement in cybersecurity assurance for military supply chains by providing a dynamic, mathematically grounded framework capable of adapting to evolving operational threats. Unlike traditional approaches that rely on static assessments or generalized compliance structures, DEFCHAIN integrates three core dimensions—trust in suppliers, security in transit, and organizational cybersecurity—within a unified analytical structure that explicitly accounts for contextual influences such as geopolitical dynamics, resource volatility, and systemic resilience. This triadic integration enables a level of granularity and responsiveness not typically present in existing models.

From a strategic perspective, DEFCHAIN extends beyond a purely diagnostic function by supporting anticipatory decision-making based on evolving risk conditions. The evaluation of illustrative scenario configurations demonstrates how variations in structural parameters, organizational preparedness, and external conditions translate into divergent cybersecurity profiles. These differences illustrate how inconsistencies in policy implementation, technical capability, and supplier transparency may result in markedly different system-level vulnerabilities, even within otherwise comparable operational environments.

More broadly, the model conceptualizes cybersecurity in supply chains not as a static condition, but as a fluctuating state requiring continuous reassessment and recalibration. The ability to simulate risk evolution over time, capture degradation effects, and incorporate external contextual pressures positions DEFCHAIN not only as an assessment tool, but as an analytical instrument for strategic foresight in complex defence-oriented supply chain environments.

However, this model—like any scientific construct—has boundaries. It assumes the availability of structured input data and institutional support for monitoring, which may not always be present in allied or partner systems. Furthermore, the model prioritizes a

defensive logic; it does not currently evaluate offensive cyber capabilities or deception tactics, which may influence threat perception and counter-response dynamics. Future adaptations could explore these dimensions.

Although DEFCHAIN was developed with a focus on military supply chains, its underlying structure and modular design allow for seamless adaptation to civilian contexts. Sectors such as healthcare, energy, pharmaceuticals, transportation, and critical infrastructure increasingly face similar cybersecurity threats stemming from supply chain interdependencies and digital vulnerabilities. By adjusting the operational parameters, indicators, and evaluation weights, the model can be tailored to reflect the unique threat landscapes, regulatory requirements, and operational constraints of civilian sectors. This flexibility enhances its utility as a cross-domain tool for proactive risk assessment, strategic planning, and resource allocation in both public and private sector environments.

In summary, DEFCHAIN makes a meaningful contribution by formalizing a dynamic framework for cyber resilience in complex defence-oriented supply chains. It offers a replicable, scalable approach that bridges theory and practice and can inform national and alliance-level strategies. While further empirical validation in live operational settings is required, the model lays the groundwork for a new standard in supply chain cyber assurance—one capable of withstanding the uncertainty and complexity of 21st-century security environments.

### *5.1. Interpretation of Simulation Results*

The simulation results provide several important insights into the behaviour and practical implications of the DEFCHAIN model. First, the observed monotonic and bounded evolution of the composite cybersecurity score across all simulated configurations confirms that the model behaves as a stable adaptive system. Regardless of responsiveness regime, environmental risk level, or adaptation speed, the model does not exhibit oscillatory or unstable behaviour. This property is particularly important in military and defence contexts, where assessment volatility can undermine trust in analytical decision-support tools and complicate command-level interpretation.

A key finding concerns the distinct roles of responsiveness parameters and adaptation dynamics. The results demonstrate that responsiveness settings, defined by the sensitivity parameter $\lambda$ and the risk threshold $\theta$, primarily influence the timing and intensity of the response, rather than the long-term attainable cybersecurity level under sustained environmental risk. Highly responsive, threshold-driven configurations produce faster initial improvements and higher early cybersecurity scores, but these advantages diminish over time as trajectories converge. This suggests that responsiveness parameters function as short- to mid-term tuning mechanisms, shaping how quickly an organization reacts to perceived risk, rather than determining the ultimate security posture.

In contrast, the adaptation rate parameter k consistently governs the pace of organizational learning and security improvement throughout the entire simulation horizon. Differences in k produce persistent separation between trajectories, indicating that organizational agility and capacity to implement security measures are decisive factors for sustained improvement. From an operational perspective, this implies that investments in rapid decision-making, resource mobilization, and implementation capability may yield more durable benefits than simply increasing response sensitivity.

The aggregated results further reveal an important trade-off between responsiveness and stability. More aggressive and threshold-driven configurations are associated with higher average cybersecurity scores (higher scores reflect model output under the defined scoring and weighting assumptions rather than empirical effectiveness) but also with increased variability across scenarios. This reflects greater sensitivity to baseline conditions and dynamic adaptation paths. Conversely, softly responsive configurations produce

more stable outcomes but adapt more slowly. This trade-off mirrors real-world defence planning challenges, where overly aggressive postures can lead to resource strain or overreaction, while overly conservative postures may delay necessary responses to emerging threats.

Sensitivity analysis reinforces the central role of decision thresholds and environmental risk in shaping model output. The dominance of the threshold parameter θ indicates that the decision of when to respond has a greater impact on system behaviour than the decision of how strongly to respond once triggered. This finding aligns with doctrinal practices in military risk management, where predefined alert levels, escalation criteria, and rules of engagement often carry more strategic weight than incremental adjustments in response intensity.

To further interpret the joint effect of the responsiveness parameter $\lambda$ and the risk threshold θ, Table 8 summarizes the characteristic interaction regimes implied by the logistic weighting function. Furthermore, Table 9 provides a feature-based baseline comparison, positioning DEFCHAIN against established frameworks like ISO/IEC 27001, ISO 28000, and NIST SP 800-161. This comparison highlights the shift from static compliance snapshots to dynamic, mathematically formulated risk trajectories. Unlike these conventional approaches, DEFCHAIN's primary novelty is its ability to model the interaction between risk perception and organizational response thresholds. The comparison underscores that DEFCHAIN addresses a different analytical objective, emphasizing quantitative and dynamic risk evaluation rather than purely qualitative process guidance.

**Table 8.** Interaction between $\lambda$ and θ in the logistic weighting function w(R).

| Dimension | DEFCHAIN | ISO/IEC 27001 [57] | NIST SP 800-161 [4] | Zero Trust Architecture [58] |
|---|---|---|---|---|
| Primary purpose | Cybersecurity risk evaluation in supply chains | Information security management system | Supply chain risk management guidance | Access control and network security paradigm |
| Domain focus | Defence and military supply chains (adaptable to civilian) | Organization-wide information security | ICT supply chain security | Enterprise networks and identities |
| Risk representation | Quantified, dynamic risk scores | Qualitative/control-based | Qualitative and process-oriented | Not explicitly risk-based |
| Temporal behaviour | Dynamic, time-dependent adaptation | Static compliance snapshot | Periodic reassessment | Continuous enforcement, not risk modelling |
| Treatment of external factors | Explicitly modelled and quantified | Contextual, not quantified | Contextual guidance | Implicit (trust assumptions) |
| Mathematical formulation | Explicit equations and parameters | None | None | None |
| Intended output | Composite cybersecurity score and trajectories | Certification status | Risk management recommendations | Enforcement policies |

**Table 9.** Feature-based comparison of DEFCHAIN against established cybersecurity and supply chain frameworks.

| Approach | Static Indicators | Dynamic Weighting | Process Loop [1] | External/Geopolitical Factors |
|---|---|---|---|---|
| ISO 28000 | Yes | No | No | No |
| NIST SP 800-161 | Yes | No | Partial | No |
| Maturity models | Yes | No | No | No |
| DEFCHAIN | Yes | Yes | Yes | Yes |

[1] Process loop refers to an explicitly defined, closed and model-internal feedback cycle.

The comparison highlights that DEFCHAIN addresses a different analytical objective than the referenced frameworks, emphasizing quantitative and dynamic risk evaluation rather than compliance, architectural enforcement, or process guidance.

### *5.2. Outcome-Level Benchmarking Against Established Cybersecurity Assessments*

To address the question of practical applicability, a limited outcome-level benchmarking was conducted against established cybersecurity audit and assessment frameworks, specifically ISO/IEC 27001 and NIST SP 800-161.

The objective was not numerical equivalence, but ordinal alignment between DEFCHAIN risk classifications and the qualitative outcomes produced by these frameworks.

Representative audit profiles were constructed based on commonly documented assessment outcomes (e.g., certified without major non-conformities; certified with major non-conformities; partially implemented supply chain controls). Each profile was translated into DEFCHAIN indicator scores using the rule-based ordinal scoring logic defined in Table 10. The resulting DEFCHAIN composite risk levels were then compared with the expected security posture implied by the benchmark frameworks.

The comparison shows consistent alignment between DEFCHAIN risk classes and audit-derived conclusions, supporting the external validity of the model at the outcome level.

**Table 10.** Outcome-level benchmarking of DEFCHAIN risk classifications against established cybersecurity assessment frameworks.

| Benchmark Framework | Assessment Outcome | Expected Security Posture | Indicative DEFCHAIN Indicator Pattern (S, T, O) | DEFCHAIN Classification |
|---|---|---|---|---|
| ISO/IEC 27001 | Certified, no major NC | Low–medium risk | Predominantly high scores (5) across S, T, and O | Low risk |
| ISO/IEC 27001 | Major non-conformities | High risk | Combination of low (1) and critical (0) scores across S, T, and O | High risk |
| NIST SP 800-161 | Controls partially implemented | Medium risk | Mixed pattern of medium (3) and low (1) scores across S, T, and O | Medium risk |
| NIST SP 800-161 | Controls largely absent | High–critical risk | Predominantly critical (0) and low (1) scores across S, T, and O | Critical risk |

The indicator patterns shown in Table 10 are illustrative and representative rather than computed values, intended to demonstrate ordinal consistency between benchmark assessment outcomes and DEFCHAIN risk classifications.

In addition to outcome-level benchmarking, the validation logic can be further strengthened through structured expert elicitation. A Delphi-style, multi-round assessment involving subject-matter experts in cybersecurity and defence logistics would enable calibration of indicator weights and sensitivity ranges for the dynamic parameters $\lambda$ and $\theta$. Expert judgments would be iteratively refined through controlled feedback and aggregated using median values and interquartile ranges to reduce individual bias. The resulting consensus-derived parameter bounds would then be incorporated into the model as calibrated inputs for scenario evaluation and sensitivity analysis, providing a non-classified yet empirically grounded complement to the benchmarking results.

### *5.3. Sensitivity, Threshold Policy, and Operational Interpretability*

The sensitivity analysis indicates that decision thresholds ($\theta$) and external risk conditions R(t) exert a significantly stronger influence on model outputs than the responsiveness parameter ($\lambda$). This finding has important operational implications for high-assurance supply chains. Within the DEFCHAIN framework, $\lambda$ primarily governs the intensity and smoothness of the model's response once risk escalation is recognized, whereas $\theta$ defines the policy boundary at which risk conditions trigger prioritization and escalation. In this sense, $\theta$ represents a strategic threshold policy rather than a purely technical tuning parameter.

Operationally, the prioritization of when to respond over how aggressively to respond aligns with established military command-and-control principles. A lower $\theta$ corresponds to a more risk-averse posture, in which early warning signals prompt rapid reprioritization of affected supply chain components, whereas a higher $\theta$ reflects a more risk-tolerant posture that delays escalation until threats become more explicit. The practical setting of $\theta$ should therefore be determined by mission criticality and the expected threat environment. For example, a mission-critical supply link operating in a contested environment would necessitate a significantly lower threshold than routine peacetime logistics.

DEFCHAIN further assumes that $\theta$ is not a static value but is subject to governance and command-level adjustment as operational contexts evolve. Threshold updates may be informed by changes in threat intelligence, shifts in mission phase, or broader strategic conditions, and should be enacted through predefined review processes rather than continuous automatic recalibration. The sensitivity results thus reinforce the interpretation of DEFCHAIN as a decision-support framework in which strategic policy choices regarding risk tolerance dominate system behaviour, while responsiveness parameters primarily shape execution once those policy boundaries are crossed.

The weighting parameters in DEFCHAIN are not intended to represent statistically derived estimates of real-world risk priorities. Rather, they function as policy-sensitive control parameters that encode different organizational response postures under uncertainty. To mitigate the risk of arbitrary weighting, the model relies on ordinal indicator scales, explicit scoring rules, and extensive sensitivity analysis, which demonstrates that qualitative risk ordering remains stable across plausible parameter ranges.

Outcome-level benchmarking against established assessment frameworks further provides external anchoring of risk classifications. Nevertheless, calibration of weighting parameters using empirical data, industry practice, or structured expert elicitation represents a clearly defined direction for future research, particularly as access to operational datasets becomes feasible.

### *5.4. Adversarial Dynamics and Model Scope*

Cybersecurity risk in military supply chains is inherently adversarial and shaped by adaptive attacker behaviour. DEFCHAIN does not explicitly model attacker strategies or

decision-making processes. Instead, it conceptualizes adversarial dynamics indirectly, through changes in environmental risk R(t), external contextual factors, and regime-dependent prioritization driven by threshold policies. In this sense, the model captures the effects of adversarial behaviour on risk posture and decision urgency, rather than simulating attacker–defender interactions themselves.

This design choice reflects the intended role of DEFCHAIN as a risk governance and prioritization framework rather than a cyber-conflict or threat-emulation model. Explicit modelling of attacker behaviour—such as game-theoretic interaction, red-team dynamics, or adaptive threat simulation—would require different assumptions, data, and validation strategies, and is therefore positioned as a complementary extension rather than a deficiency of the current approach.

### *5.5. Operationalization and Governance of External Factors*

The integration of external factors in DEFCHAIN is designed as a contextual modulation layer rather than a direct extension of component-level indicators. These factors capture geopolitical, regulatory, and strategic conditions assessed at the supplier-country or system-of-systems level, depending on the decision scope. Country-level factors include geopolitical stability, sanctions exposure, and alliance status, while system-level factors capture strategic conditions such as escalation dynamics or mission posture. Contract-specific factors may act as modifiers where legally relevant, but they are treated as contextual modifiers subordinate to broader environmental variables.

To ensure transparency and avoid ad hoc quantification, external factors are evaluated using a rule-based ordinal coding scheme anchored in observable signals. Representative data sources include government threat assessments, alliance posture reports, sanctions registers, and strategic warning products. Each factor is mapped to a bounded scale reflecting its directional effect—amplifying or mitigating—on the composite risk score. This approach reflects the relative intensity of contextual influence without implying precise numerical magnitude, thereby avoiding false precision in domains where empirical measurement is inherently constrained.

External factor values are updated at policy-relevant intervals (e.g., changes in threat intelligence or mission phase) rather than continuously, governed through command- or policy-level review processes. This design positions external modulation as a stable strategic driver of risk prioritization. While the validity of this quantification is currently rooted in internal consistency and sensitivity analysis, future work will focus on empirical calibration through expert elicitation and operational studies.

### *5.6. Interpretation of Dynamic Behaviour*

The simulation results demonstrate that the composite cybersecurity score CS(t) evolves in a monotonic and stable manner across all examined configurations. Regardless of the selected responsiveness regime, adaptation rate, or environmental risk level, the trajectories exhibit smooth convergence without oscillations, discontinuities, or chaotic behaviour. This property is significant, as it confirms that the DEFCHAIN model translates risk perception and organizational response into controlled and predictable system dynamics.

The monotonic increase in CS(t) reflects a fundamental design principle of the model: under sustained environmental pressure, security posture improves through incremental adaptation rather than abrupt shifts. From an operational perspective, this behaviour is desirable because it avoids artificial volatility in the assessment of cybersecurity readiness. Sudden fluctuations in security scores could undermine trust in the model outputs and complicate decision-making, particularly in high-assurance environments where stability and predictability are essential.

The results further indicate that the responsiveness parameter $\lambda$ and the adaptation rate k primarily influence the speed of convergence rather than the asymptotic level of the cybersecurity score. Higher values of $\lambda$ lead to stronger early responses to perceived risk, while higher values of k accelerate the rate at which the system approaches its long-term range. However, neither parameter alters the bounded nature of the model or produces unrestrained growth. This separation between response intensity and long-term limits ensures that aggressive configurations do not result in unrealistic or unstable outcomes.

Such behaviour is particularly relevant for military and defence-related systems, where rapid overreaction can be as problematic as delayed response. The DEFCHAIN model supports differentiated response postures by allowing organizations to adjust how quickly they react to risk without compromising overall system stability. In this sense, responsiveness and adaptation parameters function as tuning mechanisms rather than sources of structural instability.

Overall, the observed dynamic behaviour confirms that DEFCHAIN operates as a controlled adaptive system. It does not exhibit abrupt transitions or chaotic escalation but instead responds proportionally and continuously to environmental pressure. This property reinforces the suitability of the model for strategic and operational decision support, where reliable interpretation of temporal trends is more valuable than short-lived sensitivity to transient fluctuations.

### *5.7. Role of Responsiveness and Threshold Parameters*

The sensitivity analysis highlights a clear asymmetry between the roles of the responsiveness parameter $\lambda$ and the risk threshold parameter $\theta$ in shaping the behaviour of the DEFCHAIN model. While both parameters influence the dynamic weighting mechanism, the results indicate that variations in $\theta$ produce substantially larger changes in the composite cybersecurity score than comparable variations in $\lambda$. This finding underscores the central role of threshold selection in determining how perceived risk is translated into organizational response.

The dominance of the threshold parameter reflects its function as a decision boundary within the model. The value of $\theta$ defines the point at which perceived environmental risk transitions from being tolerated to triggering a stronger adaptive response. In contrast, the responsiveness parameter $\lambda$ primarily modulates how sharply this transition occurs once the threshold has been crossed. As a result, $\lambda$ influences the intensity of the response, whereas $\theta$ determines whether and when a response is initiated.

This distinction aligns closely with real-world decision-making processes in military and defence organizations. Doctrinal frameworks, policies, and rules of engagement (ROE) typically specify clear thresholds for action—such as alert levels, readiness postures, or escalation criteria—before operational responses are authorized. These thresholds are often more consequential than the precise magnitude of the response itself, as premature or delayed activation can entail high strategic and operational costs.

The simulation results further suggest that high responsiveness in the absence of a well-defined threshold may lead to disproportionate reactions to moderate risk levels. Without an appropriate $\theta$, even small fluctuations in perceived risk can trigger strong responses, increasing the likelihood of resource exhaustion, operational fatigue, or unnecessary escalation. Conversely, a clearly defined threshold allows organizations to maintain stability under normal conditions while still enabling rapid and decisive action once risk exceeds an acceptable level.

Overall, the observed sensitivity patterns confirm that effective risk management within the DEFCHAIN framework depends more on when to respond than on how aggressively to respond. The threshold parameter $\theta$ serves as the primary strategic control lever, while the responsiveness parameter $\lambda$ plays a secondary, tuning role. This hierarchy

reflects practical considerations in high-assurance environments, where disciplined threshold setting is essential to balance readiness, proportionality, and long-term sustainability of defensive postures.

### *5.8. Limitations and Scope of Applicability*

While the results demonstrate the internal consistency, stability, and analytical usefulness of the DEFCHAIN model, several limitations must be acknowledged regarding the scope and interpretation of the presented simulations. First, the simulation results do not constitute an empirical validation of the model against real-world incident data. The scenarios used in the analysis are synthetic and intentionally constructed to explore the behaviour of the model across a broad and controlled parameter space. As such, the simulations are designed to demonstrate model properties rather than predictive accuracy. Due to the restricted nature of military incident reports, the model's operational utility is demonstrated through a documented case vignette in Appendix A. This vignette utilizes a profile constructed from non-classified security requirements and realistic supplier data, allowing for a fully auditable demonstration of how static vulnerabilities translate into dynamic risk trajectories under controlled stress-test conditions.

Second, the environmental risk parameter R is held constant within each simulation run. This assumption allows isolation of the effects of responsiveness, threshold, and adaptation parameters, but it does not capture rapidly fluctuating or adversarial risk dynamics that may occur in real operational environments. Consequently, the presented results should be interpreted as responses to sustained risk conditions rather than short-term shock events or highly volatile threat landscapes.

Third, the static scenarios represent aggregated baseline conditions derived from ordinal indicator scoring rather than direct measurements of operational performance. While this abstraction is appropriate for strategic-level analysis and comparative assessment, it may not fully reflect the granularity or temporal variability of real-world supply chain data. The model, therefore, emphasizes structural understanding and relative positioning rather than precise point estimates.

The DEFCHAIN framework is not intended to function as a real-time incident response system or an autonomous decision-making engine. Without appropriate calibration and integration with operational data sources, direct application to real-time tactical decision-making could lead to misinterpretation or overreaction. Instead, the model is best suited for strategic planning, risk posture assessment, scenario analysis, and policy evaluation, where interpretability and controlled adaptation are prioritized over immediate predictive output.

Taken together, these limitations highlight that DEFCHAIN should be understood as an analytical and decision-support framework rather than a predictive oracle. Its primary value lies in structuring complex cybersecurity risk information, exploring the implications of different response postures, and supporting informed judgment in high-assurance environments. Future work may address empirical calibration, dynamic risk inputs, and integration with operational monitoring systems to extend the applicability of the model beyond the analytical domain explored in this study.

### *5.9. Implications for Military and High-Assurance Supply Chains*

The results demonstrate that the DEFCHAIN model is well-suited for application in military and other high-assurance supply chains, where cybersecurity is inseparable from operational readiness, resilience, and command responsibility. Unlike generic risk scoring approaches, DEFCHAIN explicitly integrates static baseline conditions with dynamic adaptation driven by perceived environmental risk, enabling a structured and context-aware assessment of supply chain cybersecurity posture.

One of the key implications of the model is its ability to support early warning and gradual escalation. The logistic weighting mechanism allows small but persistent increases in perceived risk to be reflected in the dynamic cybersecurity score without triggering abrupt or disproportionate responses. This property is particularly relevant in military environments, where early indicators of degradation—such as reduced supplier trust, increased exposure during transit, or emerging external pressures—must be detected and interpreted before they escalate into operationally disruptive events.

The model further enables differentiated responses across varying operational contexts. By adjusting threshold and responsiveness parameters, DEFCHAIN can represent different doctrinal postures, mission profiles, or threat environments. This allows the same framework to be applied across peacetime operations, heightened alert conditions, and crisis scenarios without altering the underlying structure of the model. Such flexibility is essential in military supply chains, where uniform responses are rarely appropriate, and proportionality is a core principle of risk management.

From a command and control perspective, DEFCHAIN supports informed decision-making by preserving transparency in how risk inputs are translated into dynamic outcomes. Each component of the composite score remains traceable to underlying indicators, thresholds, and response parameters. This transparency distinguishes the model from black-box approaches that produce numerical outputs without providing insight into the mechanisms driving those results. Commanders and decision-makers can therefore interpret not only the current security posture but also the reasons for its evolution over time.

Importantly, the interpretability of DEFCHAIN enhances trust in the model outputs. In high-assurance environments, acceptance of analytical tools depends not only on their numerical accuracy but also on their explanatory ability and alignment with doctrinal reasoning. By making the roles of risk perception, decision thresholds, and adaptation dynamics explicit, DEFCHAIN facilitates shared understanding between technical analysts and operational leaders.

Overall, the implications of the results suggest that DEFCHAIN functions as a decision-support framework rather than a prescriptive automation tool. It enables commanders to understand trends, anticipate vulnerabilities, and evaluate the consequences of different response postures, thereby supporting proactive and proportionate management of cybersecurity risk in military and high-assurance supply chains.

### *5.10. Literature Recommendation for Further Research*

Our comprehensive literature reviews critically informed the conceptualization and development of our DEFCHAIN model. We specifically sought out studies that proposed the construction of models akin to what DEFCHAIN offers, focusing on future research directions that directly align with our model's core components: its development, indicator utilization, dynamic processes, and the influence of external factors. A substantial segment of the reviewed literature directly proposed the expansion of conceptual models that integrate structured indicators and security-related factors, thereby laying the groundwork that resonates with DEFCHAIN's foundational design. Notably, Yeboah-Ofori and Islam [12] and Pandey et al. [11] suggested frameworks that align with our approach to building a comprehensive model for cybersecurity in supply chains. Further, the imperative to explore advanced technologies such as SIEM, blockchain, and artificial intelligence, as championed by Herr et al. [31] and Hammi et al. [34], provided explicit suggestions for the technological backbone essential to a model like DEFCHAIN. These authors advocated for the very types of integrations that form the architectural core of our proposed solution. Several researchers also called for the adaptation of such models across various sectors, regions, or regulatory contexts. This emphasis, seen in the works of Reinsch [45]

and Wallis and Dorey [53], directly supported our ambition to design DEFCHAIN with inherent external adaptability, responding to a recognized need in the literature for models capable of broader application. Moreover, a recurring theme in the literature, as highlighted by Creazza et al. [18] and Lewis et al. [19], was the urgent need for developing robust qualitative and quantitative indicators. These proposals directly informed the design of DEFCHAIN's evaluation mechanisms, as we sought to build a model with strong, measurable insights. Finally, contributions from sources like CISA [3], addressing systemic and ethical considerations, provided critical insights for the responsible and secure implementation of a model like DEFCHAIN. These recommendations guided our efforts to ensure DEFCHAIN's broader utility within real-world environments. This systematic review thus revealed a compelling consensus in the literature, with numerous authors proposing the very elements and functionalities that define our DEFCHAIN model, validating its design and demonstrating a clear need for such a comprehensive solution.

### *5.11. Significance of Findings for the Field and Identified Research Gaps*

The DEFCHAIN model presents a new operational paradigm for evaluating cybersecurity in supply chains—one that combines quantified risk indicators, dynamic weighting, and real-time adaptability to changing threat conditions. Its application extends beyond the defence sector, offering a structured foundation for enhancing cyber resilience in critical civilian systems such as healthcare logistics, financial infrastructure, and energy distribution. By operationalizing cyber risk evaluation through modular and process-driven logic, the model supports decision-makers in prioritizing protection efforts based on real-time situational awareness rather than retrospective auditing or static controls.

Importantly, the findings suggest that a transition from checklist-based compliance to dynamically adaptive risk management is both necessary and achievable. The model enables organizations to calibrate their protective measures continuously, in response to changing threat landscapes and operational constraints. This lays the groundwork for more agile and resilient supply chain architectures, capable of maintaining continuity even under cyber pressure.

However, the study also identifies key areas for future research. First, empirical testing of the DEFCHAIN model across different sectors and geopolitical contexts remains limited and is essential for confirming its generalizability. Second, real-world deployments could further refine indicator weights, dynamic thresholds, and sector-specific adaptations. Third, integration with automated threat intelligence systems and AI-enabled decision support tools represents an opportunity to enhance the model's predictive capabilities.

In sum, DEFCHAIN not only responds to an urgent need for more effective cybersecurity in supply chains but also opens new pathways for cross-sectoral application and methodological innovation. Its structured design and dynamic adaptability create a foundation upon which future research can build more intelligent, context-aware, and interoperable cyber risk management systems.

### *5.12. Strengths and Weaknesses of the Model*

The DEFCHAIN model offers several key strengths. Its primary advantage lies in the integration of quantifiable indicators with a dynamic risk assessment process, enabling real-time adaptation to evolving threats. This sets it apart from traditional static assessment models. The model also incorporates external geopolitical and regulatory factors, expanding the analytical scope beyond internal organizational measures. Its modular architecture allows it to be tailored for both military and civilian environments, enhancing

cross-sectoral applicability. The structured scoring system facilitates decision-making by transforming complex security dynamics into actionable insights.

However, the model also presents some limitations. Empirical validation is limited to simulation scenarios and case study approximations, which may not capture the full spectrum of real-world complexity. Further testing in operational environments is required to validate its predictive accuracy and usability under time pressure. In addition, indicator weights and thresholds were defined analytically, not yet calibrated through large-scale data or machine learning optimization, which could enhance precision. While the model supports dynamic adaptation, it still relies on predefined processes and scoring schemes, which may reduce flexibility in completely novel or unanticipated threat environments.

These strengths and weaknesses reflect the model's current maturity: it offers a structured, innovative, and operationally relevant framework, but further research and real-world deployment are necessary to refine its robustness, scalability, and automation potential.

To address the inherent constraints of empirical data access in the defence sector, the model was subjected to a multi-layered validation framework. Table 11 summarizes the scope and strength of these validation efforts, demonstrating the model's robustness relative to its strategic positioning.

**Table 11.** Summary of the DEFCHAIN model validation framework.

| Validation Type | Scope | Strength |
| --- | --- | --- |
| Mathematical Consistency | All 400,510 theoretical states | Ensures no numerical instabilities or logic gaps in the static-dynamic transition. |
| Behavioural Verification | 21,600 distinct trajectories | Confirms stable, monotonic adaptation under various risk stress-tests. |
| Ordinal Benchmarking | Comparison with ISO 27001/NIST | Confirms the model aligns with established industrial security standards. |

### *5.13. Theoretical Contribution of the DEFCHAIN Model*

The DEFCHAIN model represents a theoretically grounded and structured contribution to cybersecurity risk evaluation in supply chains, particularly within the defence domain. Unlike conventional models that emphasize compliance checklists or sector-neutral frameworks, DEFCHAIN introduces a domain-specific, process-driven, and quantitatively measurable structure designed to address the unique complexity of military logistics and operational environments.

First, the model fills a gap in the theoretical literature by providing a framework specifically tailored for defence supply chains, which differ significantly from commercial ones in terms of threat exposure, regulatory demands, and operational constraints. Whereas most existing models abstract away from the specifics of the military context, DEFCHAIN grounds its structure in defence-related requirements such as classified information handling, supplier vetting, and mission-critical resilience. Second, DEFCHAIN incorporates a dynamic assessment process—sensing, understanding, and directing—that captures the evolving nature of cybersecurity threats. This dynamic feedback loop goes beyond the static assessments typically found in the literature and offers a theoretical model for continuous adaptation in complex and contested environments. Third, the model integrates both internal and external dimensions of cyber risk, combining indicators related to suppliers, in-transit protection, and organizational security with external factors such as geopolitical pressure, legal frameworks, and strategic resilience. This comprehensive approach enriches existing theories by demonstrating how external conditions shape cybersecurity risk profiles in supply chains. Fourth, DEFCHAIN contributes to the

conceptualization of cyber resilience as an adaptive capability rather than a reactive response. Its ability to reconfigure in real time, based on quantifiable risk signals, extends theoretical perspectives on resilience by aligning it with predictive and pre-emptive system behaviour. Finally, the model's modular architecture and applicability across both military and civilian sectors bridge two traditionally separate theoretical domains. It lays the foundation for a cross-sectoral theory of cybersecurity, where defence-grade resilience strategies inform critical infrastructure protection in areas such as healthcare, energy, and public administration.

In sum, DEFCHAIN offers not only a practical tool for defence logistics but also a conceptual platform for advancing cybersecurity risk management theory in complex supply chain ecosystems.

### *5.14. Answers to Research Questions*

The first research question, which addresses the influential factors and indicators of cybersecurity in supply chains and their quantification for improved risk assessment and more effective security management, emphasizes the division of these elements into three main categories. The first category covers trust in suppliers, where key elements include certifications and compliance with standards, financial stability, contractual security, the inclusion of security requirements in contracts, risk management plans, and transparency in cooperation with military structures. The second category focuses on security in transit, which involves encryption of communications, data integrity verification, authentication and access control in logistics movements, physical protection of transport routes, as well as anomaly detection and protection against attacks. The third category addresses organizational cybersecurity, which is based on strategic security planning, risk management, incident response, forensic analysis, regular security testing, and staff training and awareness. The quantification of indicators is carried out using a four-level scale that assesses risks with points from 0 (critical risk) to 5 (low risk). This rating is then visualized with a colour scale, enabling quick analysis of the security status and facilitating decision-making.

The second research question, which examines the role of systematic risk assessment and cybersecurity models in the timely identification of threats, forecasting the future security state, and dynamically adjusting protective measures, emphasizes the importance of using advanced risk assessment methods. The model enables early detection of threats through penetration testing, anomaly monitoring, and artificial intelligence to predict attacks. Predicting the future state of cybersecurity is based on dynamic weights that adjust according to perceived security challenges, with the model automatically adjusting priority measures based on current conditions, such as increased risks during transit. Dynamic adjustment of security measures is carried out using a mathematical model that incorporates a logistic function for weight adjustment based on perceived risks, a sensitivity factor that determines the speed of adjustments, and consideration of external factors such as geopolitical conditions and resource availability. This approach ensures continuous improvement of security, as new data is continuously incorporated into risk assessments, enabling proactive management of cybersecurity threats in the supply chains of armed forces.

In conclusion, it can be stated that the comprehensive model for assessing cybersecurity in supply chains enables a better understanding of security vulnerabilities, more effective risk management, and timely adjustment of security measures in response to current threats. Through systematic evaluation and dynamic adjustments, the model contributes to increased resilience of the supply chains of armed forces and reduces operational risks in the modern cybersecurity environment.

*5.15. Limitations of the Study*

This study has several limitations that should be considered when interpreting its findings and practical applicability. Most notably, the proposed DEFCHAIN model has not yet been empirically validated using real-world military supply chain data. Direct access to operational or classified datasets from armed forces environments was not possible due to security, confidentiality, and data availability constraints. As a result, model validation is based on structural consistency checks, sensitivity analysis, scenario-based simulations, and outcome-level benchmarking, rather than on empirical field deployment.

This validation strategy establishes internal coherence, behavioural plausibility, and external anchoring of the model, but it does not substitute for empirical testing under operational conditions. Consequently, while DEFCHAIN is suitable as a decision-support and analytical framework, its effectiveness as a deployed assessment tool in real military environments remains to be demonstrated.

A further limitation arises from the inherent complexity and heterogeneity of military supply chains. Although the model incorporates a broad set of internal and external factors, it cannot fully capture the specific operational nuances of individual units, missions, or coalition contexts. In addition, cybersecurity threats and regulatory requirements continue to evolve, meaning that the model reflects current threat landscapes and governance frameworks rather than providing long-term predictive capability.

Finally, the mathematical formulation of the model relies on quantified indicators and weighting parameters that, while rule-based and transparent, inevitably involve analytical judgement. The practical utility of the model also depends on the availability of adequate human, technical, and organizational resources; where such resources are constrained, assessment fidelity may be reduced.

Future research should therefore prioritize empirical validation through pilot deployments, expert-elicitation studies, or controlled operational exercises, as well as continuous refinement of indicators and parameters in response to evolving threat and regulatory environments.

Although the DEFCHAIN architecture is modular and parameterized, this study does not provide empirical cross-domain validation. Differences in risk dynamics, regulatory environments, and operational priorities across civilian industries may require substantial adaptation. Civilian application of the model, therefore, remains a design hypothesis to be evaluated through future cross-domain case studies and empirical pilot applications.

Finally, DEFCHAIN does not explicitly model adversarial attacker behaviour. While the model incorporates dynamic risk signals, external threat conditions, and escalation mechanisms that reflect the impact of hostile actions, it does not simulate attacker strategies, adaptive behaviour, or interaction dynamics. As such, DEFCHAIN is not intended to replace threat modelling, red-teaming, or cyber conflict simulation, but to complement these approaches by providing structured risk evaluation and decision support. Future research could integrate DEFCHAIN with adversarial modelling techniques to enhance analytical depth in high-conflict scenarios.

## 6. Conclusions

Ensuring cybersecurity in supply chains is becoming increasingly complex due to the rapid evolution of digital infrastructures and the growing sophistication of cyber threats. This study has shown that many existing approaches address cybersecurity risks in a fragmented manner, often focusing on isolated controls, compliance requirements, or architectural elements, without providing an integrated and dynamic perspective. In response, the DEFCHAIN model was introduced as a structured, analytically grounded framework for evaluating cybersecurity risk in supply chains under evolving conditions.

https://doi.org/10.3390/systems14020132

A central contribution of DEFCHAIN lies in its ability to represent cybersecurity as a dynamic and adaptive process. Through scenario-based simulation, the model demonstrates stable, bounded, and interpretable behaviour across a wide configuration space, while explicitly differentiating between static baseline exposure, external environmental pressure, responsiveness policies, and organizational adaptation capacity. The results indicate that decision thresholds and environmental risk exert a stronger influence on system behaviour than response intensity alone, underscoring the strategic importance of well-defined escalation criteria in supply chain cybersecurity management.

The model's modular structure and parameterized design enable its application across diverse organizational contexts without requiring reliance on sector-specific threat data. Although originally motivated by defence logistics, DEFCHAIN is equally applicable to civilian domains characterized by high interdependence and criticality, including energy, healthcare, and financial supply chains. By supporting continuous monitoring, scenario exploration, and comparative assessment of response strategies, the model facilitates a shift from static, compliance-oriented approaches to proactive and policy-informed risk management.

The present study focuses on structural and behavioural validation rather than empirical prediction. As such, the value of the proposed framework lies in its analytical clarity, interpretability, and capacity to support informed decision-making under uncertainty. Future research may extend DEFCHAIN through structured expert elicitation (e.g., the Delphi method) to empirically calibrate indicator weights and decision thresholds, alongside the integration of automated threat intelligence and machine learning techniques, and enhanced modelling of interdependencies between supply chain actors. Additional work on standard harmonization, data provenance, and secure information exchange could further strengthen its applicability in complex, multi-organizational environments.

**Author Contributions:** Conceptualization, M.P. and B.R.; methodology, M.P. and B.R.; validation, M.P. and B.R.; investigation, M.P. and B.R.; data curation, M.P. and B.R.; writing—original draft preparation, M.P.; writing—review and editing, M.P. and B.R.; supervision, B.R. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## Abbreviations

The following abbreviations are used in this manuscript:

| | |
|---|---|
| AI | Artificial Intelligence |
| ANOVA | Analysis of Variance |
| C4I | Command, Control, Communications, Computers, and Intelligence |
| CCfAR | Cybersecurity Centre for Advanced Research |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CRA | Cyber Resilience Act |
| C-SCRM | Cyber Supply Chain Risk Management |
| DEFCHAIN | Defensive Evaluation Framework for Cybersecurity in Supply Chains |
| EU | European Union |
| FMCG | Fast-Moving Consumer Goods |
| GDPR | General Data Protection Regulation |
| ICT | Information and Communication Technology |
| IDS/IPS | Intrusion Detection/Prevention Systems |
| IEC | International Electrotechnical Commission |

| | |
|---|---|
| IIoT | Industrial Internet of Things |
| IoT | Internet of Things |
| ISO | International Organization for Standardization |
| IT | Information Technology |
| NIS | Network and Information Security |
| NIST | National Institute of Standards and Technology |
| OODA | Observe–Orient–Decide–Act |
| OT | Operational Technology |
| PDCA | Plan, Do, Check, Act |
| SCM | Supply Chain Management |
| SEISMIC | Security Evaluation and Integration of Software and Managed Infrastructure Components |
| SIEM | Security Information and Event Management |
| SMEs | Subject Matter Experts |
| SSDF | Secure Software Development Framework |
| U.S. CMMC | United States Cybersecurity Maturity Model Certification |
| UAE | United Arab Emirates |
| UK | United Kingdom |

## Appendix A. Documented Case Vignette–Strategic Supplier Evaluation

This case vignette demonstrates the operational application of the DEFCHAIN model using a representative profile of a high-tier defence supplier. The indicators and baseline scores are derived from non-classified procurement requirements and open-source security standards (e.g., NIST 800-171 basics). The vignette reflects a class of supply chain cybersecurity incidents widely documented in open-source incident reporting, including trusted third-party software compromises and strategic supplier security failures, rather than a purely hypothetical construct. This vignette serves to operationally demonstrate the transition from static vulnerability assessment to dynamic risk evaluation. For the purposes of this vignette, all indicators were fully scored. In operational scenarios with incomplete data, the DEFCHAIN model handles missing indicators by assigning a conservative score of 0 (critical risk) to ensure a high-assurance security posture.

*Perceived Risk Assignment*

In the DEFCHAIN model, perceived risk values are not derived from static indicator scores. Instead, they represent external inputs obtained through the sensing phase, such as threat intelligence, situational awareness, or environmental assessment. In this illustrative example, perceived risk levels are explicitly assigned to demonstrate the computational flow of the model, without implying any functional dependency between static scores and risk perception.

For Company A, the perceived risk levels are set as follows:

- Supplier-related risk: RS = 0.20 (low perceived risk),
- Transit-related risk: RT = 0.20 (low perceived risk),
- Organizational risk: RO = 0.20 (low perceived risk),
- External factors risk: RZ = 0.20 (low perceived risk).

These values are selected to represent a stable operational environment and serve solely illustrative purposes.

### *Appendix A.1. Phase 1: Sensing–Static Indicator Scoring*

*Trust in Suppliers (S)*

Company A is evaluated using eleven supplier-related indicators, scored on the four-level ordinal scale (0–1–3–5). The resulting static score is: S(static) = 47 points, corresponding to 85/100.

For the supplier trust component, the following responsiveness parameters are applied:

- Sensitivity parameter: $\lambda(S) = 20$,
- Threshold parameter: $\theta(S) = 0.05$.

Using the logistic weighting function defined in Equation (5), the dynamic weight is obtained as: $w(S) = L(R(S)) \approx 0.98$.

The resulting dynamic trust score is therefore: $S(dyn) = w(S) \cdot S(static) \approx 0.98 \cdot 85 = 84$.

*Security in Transit (T)*

The in-transit security component is evaluated using eleven indicators. For Company A, the static score is: T(static)= 45 points, corresponding to 82/100.

Applied parameters:

- Sensitivity parameter: $\lambda(T) = 15$,
- Threshold parameter: $\theta(T) = 0.005$.

The resulting logistic weight is: $w(T) = L(R(T)) \approx 0.95$.

Thus, the dynamic transit security score is: $T(dyn) = w(T) \cdot T(static) \approx 0.95 \cdot 82 = 78$.

*Organizational Cybersecurity (O)*

Organizational cybersecurity is assessed across four process phases (planning, implementation, verification, improvement) and twenty indicators. For Company A, the static organizational cybersecurity score is: O(static) = 92 points, corresponding to 77/100.

Applied parameters:

- Sensitivity parameter: $\lambda(O) = 20$,
- Threshold parameter: $\theta(O) = 0.005$.

The corresponding dynamic weight is: $w(O) = L(R(O)) \approx 0.98$.

The resulting dynamic organizational cybersecurity score is: $O(dyn) = w(O) \cdot O(static) \approx 0.98 \cdot 77 = 75$.

*External Factors (Z)*

Finally, external contextual factors are incorporated using Equation (7). For illustrative purposes, Company A is evaluated with predominantly favourable external conditions:

- Positive factors (R5, R3): strong regulatory alignment and allied cooperation,
- Negative factors (R1, R0): moderate geopolitical and legal constraints,
- Amplification factor: F = 2.

The static external factors cybersecurity score is: Z(static) = 17 points.

Applied parameters:

- Sensitivity parameter: $\lambda(Z) = 20$,
- Threshold parameter: $\theta(Z) = 0.005$.
- The corresponding dynamic weight is: $w(Z) = L(R(Z)) \approx 0.98$.

The resulting dynamic external factors score is: $Z(dyn) = w(Z) \cdot Z(static) \approx 0.98 \cdot 17 = 16.6$.

The resulting external influence term modifies the perceived risk and contributes to the final adjusted cybersecurity assessment, demonstrating how DEFCHAIN integrates geopolitical, regulatory, and strategic context into the overall evaluation.

*Composite Cybersecurity Score*

The static composite cybersecurity score for Company A is calculated by aggregating the static component scores according to the aggregation function defined in Equation: $CS(static) = f(S(static), T(static), O(static), Z(static))$.

Substituting the values:

$CS(static) = S(static) + T(static) + O(static) + Z(static) = 85 + 82 + 77 + 17 = 261$.

This value represents the baseline cybersecurity posture prior to dynamic adaptation.

The value CS(static) = 261 refers to the aggregate score obtained by summing the already normalized S(static), T(static), and O(static) component values together with the external factor contribution Z(static).

In the static formulation, the external factor component Z is included as a simple additive raw contribution to reflect baseline contextual conditions and is not normalized in the same manner as the internal components S, T, and O.

*Appendix A.2. Phase 2: Understanding–Dynamic Risk Weighting*

*Dynamic Composite Cybersecurity Score*

The dynamic composite cybersecurity score is obtained by aggregating the dynamically adjusted component values according to the same aggregation logic used for the static baseline.

Substituting the calculated values yields: CS(dyn) = S(dyn) + T(dyn) + O(dyn) + Z(dyn) = 84 + 78 + 75 + 16.6 = 253.6.

*Appendix A.3. Phase 3: Directing–Adaptive Forecasting*

*Dynamic Adaptation*

To illustrate the dynamic behaviour of the DEFCHAIN model, a balanced response regime is considered with the following parameters:

- Environmental risk: R(t) = 0.40,
- Adaptation rate: k = 0.08.

Using the dynamic adaptation formulation presented in Equation (6), the composite cybersecurity score evolves over time as the system adapts to sustained environmental pressure. The resulting time-dependent cybersecurity score increases monotonically and converges toward a stable asymptotic range, as shown in the simulation results section.

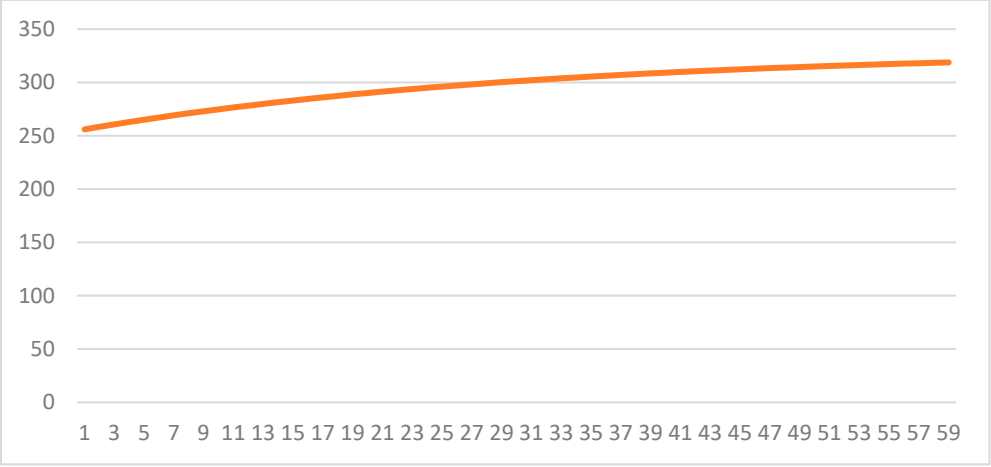


**Figure A1.** Dynamic adaptation of the composite cybersecurity score over the simulation horizon.

This demonstrates how DEFCHAIN transitions from a static assessment to a dynamic evaluation, capturing both initial cybersecurity posture and the effects of organizational responsiveness and adaptation over time.

*Interpretative Note*

This worked example illustrates the internal logic of the DEFCHAIN model and demonstrates how a static cybersecurity assessment is transformed into a dynamic, context-aware evaluation. The example is illustrative in nature and is intended to clarify the computational flow of the model rather than to provide empirical validation.

The results show that static cybersecurity scores alone may overestimate effective security posture when perceived risk and organizational responsiveness are taken into account. Even under favourable conditions, dynamic weighting systematically adjusts component scores, reflecting the fact that cybersecurity is a conditional and situational state rather than a fixed attribute.

The example further highlights the functional separation between static indicators and perceived risk. Perceived risk is treated as an external input derived from situational awareness and threat intelligence, avoiding circular dependencies and enabling the integration of real-time environmental information without recalibrating the indicator framework.

By incorporating responsiveness parameters and external contextual factors, DEFCHAIN supports scenario analysis and sensitivity exploration, allowing decision-makers to examine how different risk perceptions and response regimes influence overall cybersecurity outcomes. The dynamic adaptation segment illustrates how cybersecurity posture evolves over time under sustained environmental pressure, emphasizing trajectory and stability rather than point-in-time assessment.

Overall, this example demonstrates the applicability of DEFCHAIN as a structured decision-support framework for evaluating cybersecurity in complex and dynamic supply chain environments.

This worked example functions as a documented case vignette, providing a granular mapping of security indicators to risk levels. It demonstrates that the DEFCHAIN architecture is capable of integrating diverse data points into a coherent operational picture, suitable for strategic procurement and supplier risk management.

## References

1. Rahayu, S.B.; Jusoh, N.; Halip, M.H.M.; Taib, S.M.; Lee, M.G. A conceptual model of military blockchain for repair parts supply chain management. In Proceedings of the 2021 International Conference on Computer & Information Sciences (ICCOINS), Virtual, 13–15 July 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 146–150. https://doi.org/10.1109/ICCOINS49721.2021.9497227.
2. Zhang, H.; Nakamura, T.; Sakurai, K. Security and Trust Issues on Digital Supply Chain. In Proceedings of the 2019 IEEE International Conference on Dependable, Autonomic and Secure Computing, Pervasive Intelligence and Computing, Cloud and Big Data Computing, and Cyber Science and Technology Congress, Fukuoka, Japan, 5–8 August 2019; IEEE: Piscataway, NJ, USA, 2019. https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00069
3. Lamba, A.; Singh, S.; Singh, B.; Dutta, N.; Muni, S.S.R. Analyzing and fixing cyber security threats for supply chain management. *Int. J. Technol. Res. Eng.* **2017**, *4*, 5678—5681.
4. Reuben, J.A.; Ware, N. Approach to handling cyber security risks in supply chain of defence sector. *Ind. Eng. J.* **2019**, *12*, 1–12.
5. Herr, T.; Lee, J.; Loomis, W.; Scott, S. Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain. 2020. Available online:https://www.atlanticcouncil.org/in-depth-research-reports/report/breaking-trust-shades-of-crisis-across-an-insecure-software-supply-chain/ (accessed on 1 May 2025).
6. Cybersecurity and Infrastructure Security Agency (CISA). *Defending Against Software Supply Chain Attacks*; Cybersecurity and Infrastructure Security Agency (CISA): Cagliari, Italy, 2021.
7. Boyens, J.; Paulsen, C.; Moorthy, R.; Bartol, N. *NIST SP 800-161 Rev*; Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2022. https://doi.org/10.6028/NIST.SP.800-161r1.
8. Bartol, N. *Utilities Telecom Council Cyber Supply Chain Risk Management For Utilities–Roadmap for Implementation*; Utilities Telecom Council: Washington, DC, USA, 2015.
9. Kaur, H.; Gupta, M.; Singh, S.P. Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. *Int. J. Prod. Econ.* **2024**, *275*, 109338. https://doi.org/10.1016/j.ijpe.2024.109338.
10. Hou, Y.; Such, J.; Rashid, A. *Understanding Security Requirements for Industrial Control System Supply Chains*; Security Lancaster Institute, Lancaster University: Lancaster, UK, 2024.
11. Davis, A. Building cyber-resilience into supply chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 19–27.
12. Boyes, H. Cybersecurity and cyber-resilient supply chains. *Technol. Innov. Manag. Rev.* **2015**, *5*, 28–34.

13. do Amaral, T.M.S.; Gondim, J.J.C. Integrating Zero Trust in the cyber supply chain security. In Proceedings of the 6th Workshop on Communication Networks and Power Systems (WCNPS), Brasilia, Brazil, 18–19 November 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6.
14. Pandey, S.; Singh, R.K.; Gunasekaran, A.; Kaushik, A. Cyber security risks in globalized supply chains: Conceptual framework. *J. Glob. Oper. Strateg. Sourc.* **2020**, *13*, 103–128. https://doi.org/10.1108/JGOSS-05-2019-0042.
15. Yeboah-Ofori, A.; Islam, S. Cyber security threat modeling for supply chain organizational environments. *Future Internet* **2019**, *11*, *63*. https://doi.org/10.3390/fi11030063.
16. Yeboah-Ofori, A.; Islam, S.; Yeboah-Boateng, E. Cyber threat intelligence for improving cyber supply chain security. In Proceedings of the International Conference on Cyber Security and Internet of Things (ICSIoT), Accra, Ghana, 29–31 May 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 28–33. https://doi.org/10.1109/ICSIoT47925.2019.00012.
17. Cantrell, B. Regulations are Forcing Organizations to Address Software Supply Chain Security. 2024. Available online: https://www.scmr.com/article/regulations-are-forcing-organizations-to-address-software-supply-chain-security (accessed on 1 May 2025).
18. Prevalent The Third-Party Risk Management Compliance Handbook—Part II: Industry Standards & Guidelines. 2021. Available online: https://info.mitratech.com/hubfs/Other/M-and-A/Prevalent/documents/resources/Prevalent-TPRM-Compliance-Handbook-PartII-0721.pdf (accessed on 1 Jun 2025)
19. Centre for Cyber Security DA for DGovernment. *Cyber Security in Supplier Relationships: Protect Your Organization When Outsourcing IT Operations in the Entire Process—from Start to Finish*, 2nd ed.; Centre for Cyber Security DA for DGovernment, Copenhagen, Denmark, 2023.
20. Cabinet Office. *Supplier Assurance Framework: Good Practice Guide*; Cabinet Office: London, UK, 2018.
21. Creazza, A.; Colicchia, C.; Spiezia, S.; Dallari, F. Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era. *Supply Chain Manag. Int. J.* **2022**, *27*, 30–53. https://doi.org/10.1108/SCM-02-2020-0073.
22. Lewis, R.; Louvieris, P.; Abbott, P.; Clewley, N.; Jones, K. Cybersecurity information sharing: A framework for information security management in UK SME supply chains. In Proceedings of the Twenty Second European Conference on Information Systems, Tel Aviv, Israel, 9–11 June 2014; IEEE: Piscataway, NJ, USA, 2014.
23. Del Giorgio Solfa, F. Impacts of Cyber Security and Supply Chain Risk on Digital Operations. *Int. J. Technol. Innov. Manag.* **2022**, *2*, 18–32. https://doi.org/10.54489/ijtim.v2i2.98.
24. Latif, M.N.A.; Aziz, N.A.A.; Hussin, N.S.N.; Aziz, Z.A. Cyber security in supply chain management: A systematic review. *LogForum* **2020**, *17*, 49–57. https://doi.org/10.17270/J.LOG.2021555 and https://www.logforum.net/volume17/issue1/abstract-4.html.
25. Yeboah-Ofori, A.; Addo-Quaye, R.; Oseni, W.; Amorin, P.; Agangmikre, C. Cyber supply chain security: A cost-benefit analysis using net present value. In Proceedings of the 2021 International Conference on Cyber Security and Internet of Things (ICSIoT), Virtual, 15–17 December 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 15–17. https://doi.org/10.1109/ICSIoT55070.2021.00018.
26. Bradshaw, S. *Combatting Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity*; Centre for International Governance Innovation: Waterloo, ON, USA, 2017; pp. 105–120.
27. Urciuoli, L. Cyber-resilience: A strategic approach for supply chain management. *Technol. Innov. Manag. Rev.* **2015**, *5*, 13–18.
28. Pellathy, D.; Burnette, M. *Managing Cyber Risks in Global Supply Chains: The Four Fundamentals*; The University of Tennessee: Knoxville Knoxville, TN, USA, 2020.
29. Levite, A.E. *ICT Supply Chain Integrity: Principles for Governmental and Corporate Policies*; Carnegie Endowment for International Peace: Washington, DC, USA, 2019.
30. Boiko, A.; Shendryk, V.; Boiko, O. Information systems for supply chain management: Uncertainties, risks and cyber security. *Procedia Comput. Sci.* **2019**, *149*, 65–70. https://doi.org/10.1016/j.procs.2019.01.108.
31. Odimarha, A.C.; Ayodeji, S.A.; Abaku, E.A. Securing the Digital Supply Chain: Cybersecurity Best Practices for Logistics and Shipping Companies. *World J. Adv. Sci. Technol.* **2024**, *5*, 26–33. https://doi.org/10.53346/wjast.2024.5.1.0030.
32. Sarumi, J.A.; Okunoye, A. A review of potential threats in supply chain cyber security. *J. Behav. Inform. Digit. Humanit. Dev. Res.* **2021**, *7*, 73–86. https://doi.org/10.22624/AIMS/BHI/V7N1P6.
33. Herr, T.; Loomis, W.; Schroeder, E.; Scott, S.; Handler, S.; Zuo, T. *Broken Trust: Lessons from Sunburst*; Atlantic Council: Washington, DC, USA, 2021.
34. Martínez, J.; Durán, J.M. Software supply chain attacks, a threat to global cybersecurity: SolarWinds' case study. *Int. J. Saf. Secur. Eng.* **2021**, *11*, 537–545. https://doi.org/10.18280/ijsse.110505.

35. Department of the Environment, Climate, Communications. *Electronic Communications Security Measures 009—Supply Chain Security v1*; Department of the Environment, Climate, Communications, Dublin, Ireland, 2021.
36. Hammi, B.; Zeadally, S.; Nebhen, J. Security threats, countermeasures, and challenges of digital supply chains. *ACM Comput. Surv.* **2023**, *55*, 316. https://doi.org/10.1145/3588999.
37. Adenekan, O.A.; Ezeigweneme, C.; Chukwurah, E.G. Strategies for protecting IT supply chains against cybersecurity threats. *Int. J. Manag. Entrep. Res.* **2024**, *6*, 1598–1606. https://doi.org/10.51594/ijmer.v6i5.1125.
38. Gupta, N.; Tiwari, A.; Bukkapatnam, S.T.S.; Karri, R. Additive Manufacturing Cyber-Physical System: Supply Chain Cybersecurity and Risks. *IEEE Access* **2020**, *8*, 47322–47336. https://doi.org/10.1109/ACCESS.2020.2978815.
39. Sobb, T.; Turnbull, B.; Moustafa, N. Supply Chain 4. 0: A Survey of Cyber Security Challenges, Solutions and Future Directions. *Electronics* **2020**, *9*, 1864. https://doi.org/10.3390/electronics9111864.
40. Leligou, H.C.; Lakka, A.; Karkazis, P.A.; Costa, J.P.; Tordera, E.M.; Santos, H.M.D.; Romero, A.A. Cybersecurity in supply chain systems: The farm-to-fork use case. *Electronics* **2024**, *13*, 215. https://doi.org/10.3390/electronics13010215.
41. MITRE Corporation. *System of Trust: A Framework for Supply Chain Security*; MITRE Corporation: Bedford, MA, USA, 2021.
42. Masip-Bruin, X.; Marín-Tordera, E.; Ruiz, J.; Jukan, A.; Trakadas, P.; Cernivec, A.; Lioy, A.; López, D.; Santos, H.; Gonos, A.; et al. Cybersecurity in ICT supply chains: Key challenges and a relevant architecture. *Sensors* **2021**, *21*, 6057. https://doi.org/10.3390/s21186057.
43. Hammock, C.J. Enabling the Development and Deployment of NATO Cyber Operations: An Analysis of Modern Cyber Warfare Operations and Thresholds of Global Conflict. *J. Inf. Warf.* **2017**, *16*, 79–94.
44. Kramer, F.D.; Teplinsky, M.J. *Cybersecurity and Tailored Deterrence*; Atlantic Council of the United States: Washington, DC, USA, 2013.
45. Falk, C.D. Cyber Supply Chain Security and the Swedish Security Protected Procurement with Security Protective Agreement. Master's Thesis, Department of Computer and Systems Sciences, Stockholm University, Stockholm, Sweden, 2022.
46. Reinsch, W.A.; Benson, E.; Arasasingham, A. Securing Semiconductor Supply Chains: An Affirmative Agenda for International Cooperation. 2022. Available online: https://www.hinrichfoundation.com/research/how-to-use-it/securing-semiconductor-supply-chains (accessed on 1 May 2025).
47. Carter, S.D. Hackers putting global supply chain at risk. *Natl. Def.* **2020**, *105*, 15–16.
48. Rosenzweig, P.; Waldron, K. *Broadening the Lens on Supply Chain Security in the Cyber Domain*; R Street Institute: Washington, DC, USA, 2019.
49. Sanchez, R.R.; Ebner, S.W. New Cyber Rules to Safeguard Supply Chain. *Natl. Def.* **2017**, *101*, 15–17.
50. Coufalíková, A.; Klaban, I.; Šlajs, T. Complex strategy against supply chain attacks. In Proceedings of the 2021 International Conference on Military Technologies (ICMT), Brno, Czech Republic, 8–11 June 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 1–6. https://doi.org/10.1109/ICMT52455.2021.9502768.
51. Burnson, P. New Deloitte Study Identifies Cyber Vulnerabilities in Manufacturing Supply Chains. 2017. Available online: https://www.scmr.com/article/new_deloitte_study_identifies_cyber_vulnerabilities_in_manufacturing_supply (accessed on 1 May 2025).
52. Warrick, T.; Durkovich, C.; Massa, M. DHS's Public-Private Partnerships Are Unique and Should Be Modernized to Effectively Counter the Threats of the 2020s. In *Future of DHS Project: Key Findings and Recommendations*; Atlantic Council: Washington, DC, USA, 2020.
53. Bartol, N. Cyber supply chain security practices DNA—Filling in the puzzle using a diverse set of disciplines. *Technovation* **2014**, *34*, 354–361. https://doi.org/10.1016/j.technovation.2014.01.005.
54. Wallis, T.; Dorey, P. Implementing Partnerships in Energy Supply Chain Cybersecurity Resilience. *Energies* **2023**, *16*, 1868. https://doi.org/10.3390/en16041868.
55. Wallis, T.; Johnson, C.; Khamis, M. Interorganizational cooperation in supply chain cybersecurity: A cross-industry study of the effectiveness of the UK implementation of the NIS directive. *Inf. Secur. Int. J.* **2021**, *48*, 36–68. https://doi.org/10.11610/isij.4812.
56. United Kingdom Ministry of Defence. Joint Concept Note 1/20: Multi-Domain Integration. UK Ministry of Defence: London, UK, 2 December 2020. Available online: https://assets.publishing.service.gov.uk/media/6579c11a254aaa000d050c6e/20201112-ARCHIVE_JCN_1_20_MDI_Official.pdf (accessed on 1 April 2025)

57. *ISO/IEC 27001:2022*; Information Security, Cybersecurity and Privacy Protection. International Organization for Standardization: Geneva, Switzerland, 2022.
58. Rose, S.; Borchert, O.; Mitchell, S.; Connelly, S. *NIST SP 800-207*; Zero Trust Architecture. National Institute of Standards and Technology: Gaithersburg, MD, USA, 2020. https://doi.org/10.6028/NIST.SP.800-207.