Sinergi International Journal of Logistics
E-ISSN: 2988-6244
Volume. 2, Issue 3, August 2024
Page No: 174-186

Cybersecurity in Digital Supply Chains: A Narrative Review of Threats and Strategic Frameworks for Sustainable Logistics

Ahmad Faisal[1], Hedi Cupiadi[2], Sopannadi[3]
[1]Universitas Dirgantara Marsekal Suryadarma, Indonesia
[2]Universitas Garut, Indonesia
[3]Politeknik Elektronika Negeri Surabaya, Indonesia
Correspondent: ahmad@unsurya.ac.id[1]

Received : May 30, 2024
Accepted : August 2, 2024
Published : August 30, 2024

Citation: Faisal, A., Cupiadi, H. Sopannadi (2024). Cybersecurity in Digital Supply Chains: A Narrative Review of Threats and Strategic Frameworks for Sustainable Logistics. Sinergi International Journal of Logistics, 2(3), 174-186.

ABSTRACT : As global supply chains increasingly digitize their operations, cybersecurity in logistics information systems has become a critical concern. This study aims to synthesize current knowledge on cybersecurity threats, technological advancements, and strategic responses within the logistics sector. A structured narrative review was conducted using IEEE Xplore, Scopus, and Web of Science to identify relevant literature published between 2013 and 2024. The search utilized targeted Boolean combinations incorporating technical and operational keywords to ensure a holistic review. The findings highlight the prevalence of cyber threats such as ransomware, phishing, and DDoS attacks, which significantly affect operational continuity and data integrity. In response, emerging technologies such as blockchain and artificial intelligence are increasingly adopted to enhance detection, transparency, and risk mitigation. Despite these advancements, systemic challenges persist, including the reliance on legacy systems, regulatory fragmentation, and insufficient coordination between public and private sectors. This review emphasizes the need for integrated cybersecurity frameworks that align technical solutions with strategic policy reforms. Effective implementation requires not only technological innovation but also cross-sectoral collaboration, updated regulatory structures, and workforce development. Future research should explore empirical effectiveness, especially in diverse regional contexts, and investigate intersections between cybersecurity, sustainability, and governance. These insights offer a pathway toward resilient and secure logistics systems in a digitalized global economy.

Keywords: cybersecurity in logistics; supply chain security; blockchain in logistics; cyber threats and risk mitigation; logistics digital transformation; IoT security; regulatory frameworks

INTRODUCTION

In an increasingly interconnected and digitized global economy, the logistics sector has undergone profound transformation. Technologies such as the Internet of Things (IoT), blockchain, and advanced data analytics have redefined operational practices, enhancing supply chain transparency, efficiency, and responsiveness (Ansari & Ujjan, 2024; Schislyaeva et al., 2023). This wave of digital transformation, however, has simultaneously introduced unprecedented vulnerabilities, making logistics information systems prime targets for cyberattacks. As logistics operations become more

reliant on real-time digital coordination and data exchange, the safeguarding of these systems has become a critical strategic priority. The urgency to develop robust cybersecurity measures is further amplified by the sector's essential role in global trade and economic continuity (Anugrah & Patil, 2023; Meilenda & Syarif, 2024; Sugiarto & Suprayitno, 2023).

Recent literature underscores the dual nature of technological integration in logistics. On one hand, digital tools optimize inventory tracking, automate warehousing, and streamline transportation management. On the other hand, the expansion of the digital surface area exposes critical logistics infrastructure to cyber threats. Cybersecurity concerns now extend beyond traditional IT departments, encompassing operational technologies and enterprise-wide systems. Bronk (2020) emphasized that logistics organizations are now dealing with complex cyber environments, where legacy systems coexist with newer digital platforms, creating complex attack surfaces. In this context, cybersecurity in logistics is not just an IT issue but a multidimensional challenge that intersects with business continuity, reputational risk, and geopolitical resilience (Butar & Ahmed, 2023; Darmiono, 2023; Marnova & Tung, 2023).

Empirical evidence supports the notion that logistics systems are increasingly susceptible to cyber intrusions. Bronk (2020) reported a notable surge in cyberattacks targeting logistics firms, particularly those that rapidly digitized their operational frameworks during global disruptions. Similarly, Canepa et al. (2021) highlighted vulnerabilities in maritime infrastructure, a key node in global logistics, through controlled simulations using cyber ranges. These simulations demonstrated that inadequate cybersecurity protocols could lead to significant operational disruptions and financial loss. Furthermore, the report on "ICT Solutions and Digitalisation in Ports and Shipping" (2021) reveals that digital ports, despite their efficiency gains, are exposed to systematic cyber threats if the pace of digital integration is not matched with proportional investment in security frameworks. These findings illustrate that the speed of digital adoption, when unmatched by cybersecurity preparedness, increases systemic risk within the logistics domain (Al Firdausi & Suprayitno, 2023; Sutejo et al., 2023; Wibowo et al., 2023).

The vulnerability of logistics systems to cyber threats is further amplified by their extensive interdependencies. The sector operates as a complex web of service providers, technology platforms, transportation networks, and regulatory entities. This complexity increases the attack vectors available to malicious actors. Bronk (2020) observed that even minor breaches in third-party logistics platforms could cascade across the supply chain, affecting multiple stakeholders simultaneously. The integration of IoT devices, while enhancing visibility, also introduces new points of entry for cyber attackers, especially when these devices lack proper authentication mechanisms. Moreover, data breaches in logistics do not only compromise operational efficiency but may also endanger sensitive information such as customer databases, cargo manifests, and national security-related data.

Despite growing awareness, the implementation of effective cybersecurity frameworks in logistics remains a significant challenge. One primary difficulty lies in the coexistence of legacy systems with modern digital solutions. These older systems often lack compatibility with newer security protocols and are difficult to patch or upgrade without disrupting operations (Ansari & Ujjan,

2024). Additionally, the logistics sector is characterized by a high degree of decentralization, with multiple actors—such as freight forwarders, customs agents, carriers, and warehousing firms—each operating under different technological standards. This fragmentation hampers the uniform implementation of security policies and increases the risk of inconsistent defenses across the supply chain (Schislyaeva et al., 2023).

The sector also suffers from a shortage of cybersecurity professionals who possess domain-specific knowledge. While generic cybersecurity skills are in demand across industries, the logistics sector requires experts who understand both digital security and the operational intricacies of supply chains. Bronk (2020) noted that the talent gap in cybersecurity is particularly acute in emerging markets, where investment in digital infrastructure is not always matched by investment in cybersecurity capacity-building. Furthermore, budgetary constraints and competing operational priorities often limit the resources available for cybersecurity upgrades, especially for small and medium-sized logistics enterprises.

The current body of literature on cybersecurity in logistics reveals several gaps that justify the need for a comprehensive review. While there is a robust body of work focusing on technical measures such as encryption, intrusion detection systems, and firewalls, much of this research remains siloed from the operational realities of logistics management (Ansari & Ujjan, 2024). Few studies holistically integrate the technological, managerial, and policy dimensions of cybersecurity in logistics. Moreover, there is a notable lack of empirical studies that assess the real-world effectiveness of proposed cybersecurity solutions in logistics contexts. Bronk (2020) argues that without such integration, research findings may have limited applicability in guiding practical interventions. Another underexplored area is the role of regulatory and geopolitical factors in shaping cybersecurity policies for transnational logistics operations.

This review aims to achieve two primary objectives. First, it seeks to synthesize and critically evaluate the various approaches that have been developed to mitigate cybersecurity risks in the logistics sector. This includes an analysis of both technical tools and strategic frameworks. Second, the review aims to identify existing knowledge gaps and propose directions for future research, particularly those that enhance the contextual relevance of cybersecurity practices in logistics (Ansari & Ujjan, 2024; Bronk, 2020). By incorporating multidisciplinary perspectives—from information technology to operations management and policy studies—this review contributes to the development of a more comprehensive and adaptive understanding of cybersecurity in logistics systems.

The scope of this review is intentionally focused on logistics operations within the broader framework of industrial digitalization. Given the heterogeneity in technological maturity and regulatory frameworks across regions, this study limits its geographic scope to logistics systems in highly industrialized and digitally advanced economies. These contexts are particularly relevant due to their early adoption of digital logistics solutions and corresponding exposure to sophisticated cyber threats. Additionally, the review will prioritize literature that explores cybersecurity issues within integrated supply chain environments, such as manufacturing-logistics interfaces and smart

port ecosystems. This narrowed focus allows for an in-depth examination of cybersecurity dynamics where digital infrastructure and operational complexity are most pronounced.

In summary, the convergence of digital technologies and logistics operations presents both opportunities and vulnerabilities. While the literature acknowledges the growing cybersecurity risks facing the logistics sector, it also reveals significant conceptual and empirical gaps. Through a critical review of existing research, this study endeavors to provide a clearer understanding of the cybersecurity challenges unique to logistics systems and to identify pathways for more integrated and actionable solutions. The urgency of this endeavor cannot be overstated, as the resilience of global supply chains increasingly hinges on the robustness of their digital defenses.

METHOD

This narrative review employs a structured methodology to identify, select, and synthesize academic literature concerning cybersecurity in logistics information systems. The primary aim of the methodological approach is to ensure that the review captures the breadth and depth of current scholarly discourse and empirical evidence on cybersecurity threats, strategies, and implementations within logistics contexts. Given the multidisciplinary nature of the topic, encompassing computer science, supply chain management, digital infrastructure, and organizational behavior, the methodology was designed to include both technical and managerial perspectives.

The literature search was conducted primarily through IEEE Xplore, Scopus, and Web of Science. IEEE Xplore was selected as the core database because of its comprehensive indexing of peer-reviewed technical articles and conference proceedings, especially in the areas of cybersecurity, Internet of Things (IoT), blockchain, and digital transformation—domains directly linked to the evolution of logistics systems (Ansari & Ujjan, 2024). IEEE Xplore provides direct access to cutting-edge research on cyber defense mechanisms, network infrastructure vulnerabilities, and real-world applications of secure digital technologies. In parallel, Scopus and Web of Science were included due to their interdisciplinary reach and their ability to capture articles at the intersection of information systems, supply chain logistics, engineering, and management sciences. The inclusion of multiple databases was crucial to ensure coverage across the technological-operational spectrum of cybersecurity in logistics.

To retrieve the most relevant literature, an advanced Boolean search strategy was developed. Keywords and Boolean operators were selected to reflect both the technical terminology used in cybersecurity literature and the domain-specific language of logistics and supply chain research. The core search strings included: ("cybersecurity" OR "cyber security" OR "information security") AND ("logistics" OR "supply chain" OR "transportation") AND ("information system" OR "digitalization" OR "ICT"). This initial query was refined iteratively to include complementary concepts such as "threat", "risk", "vulnerability", "digital infrastructure", and "smart logistics". This

approach ensured that the search captured both narrow and broad studies, facilitating a comprehensive review of how cybersecurity challenges intersect with logistical operations.

The search was limited to articles published between 2013 and 2024, a period that encapsulates the rise of Industry 4.0, the mainstreaming of IoT technologies, and a heightened focus on supply chain cybersecurity in response to global events such as the COVID-19 pandemic and growing geopolitical cyber threats. Only peer-reviewed journal articles, conference papers, and book chapters were included in the analysis to maintain academic rigor. Publications not written in English, duplicate entries, and non-scholarly sources such as news articles, editorials, and promotional reports were excluded from the review.

The inclusion criteria required that studies specifically address cybersecurity issues within logistics contexts or present cybersecurity frameworks that are directly applicable to logistics and supply chain systems. Studies were considered relevant if they: (1) proposed or evaluated cybersecurity models or protocols for logistics; (2) analyzed cyber threats or vulnerabilities within logistics systems; (3) presented empirical data or case studies from logistics organizations; or (4) explored the integration of digital technologies such as IoT, blockchain, or artificial intelligence with implications for cybersecurity. Conversely, studies were excluded if they focused solely on cybersecurity in unrelated sectors, such as finance, education, or healthcare, unless they provided transferable insights into network security or data protection that could be contextualized for logistics applications.

The selection process followed a multi-phase procedure. In the initial phase, titles and abstracts of all search results were screened to assess basic relevance to the research topic. Studies that clearly met the inclusion criteria were flagged for full-text review. In the second phase, the full texts were read in detail and evaluated against a standardized protocol that assessed their methodological rigor, clarity of cybersecurity framework, relevance to logistics operations, and contribution to existing knowledge. Studies were prioritized if they provided original empirical evidence, demonstrated innovative cybersecurity applications, or presented conceptual frameworks that could be operationalized within logistics environments.

Following the selection of eligible studies, data extraction was carried out using a narrative synthesis approach. Key information was drawn from each study, including publication year, methodological approach, cybersecurity domain (e.g., threat detection, access control, risk management), logistics sub-sector (e.g., transportation, warehousing, maritime logistics), technological focus (e.g., IoT, blockchain, cloud computing), and geographical context. This information was subsequently used to categorize the literature thematically, allowing for the identification of prevailing trends, recurring challenges, and promising solutions across different logistics domains.

Throughout the selection and synthesis process, efforts were made to ensure objectivity and minimize bias. All search and selection steps were independently verified by a second reviewer with expertise in digital systems and supply chain operations. Disagreements over inclusion or

interpretation of results were resolved through discussion and consensus, and a detailed audit trail of all decisions was maintained for transparency.

In summary, the methodological approach adopted in this review integrates technical precision with contextual relevance. By leveraging reputable academic databases and a robust search strategy, the review ensures comprehensive coverage of the cybersecurity landscape within logistics systems. The inclusion and exclusion criteria were carefully defined to balance focus with breadth, and the literature selection process was governed by methodological transparency and scholarly rigor. This methodological foundation supports a thorough and balanced examination of cybersecurity in logistics, laying the groundwork for the thematic analysis and critical discussion presented in the subsequent sections.

RESULT AND DISCUSSION

The findings from the reviewed literature provide a comprehensive understanding of the multifaceted nature of cybersecurity within logistics information systems. The analysis of the sources reveals a thematic structure that encompasses three key areas: the types and impacts of cyber threats, emerging technological trends in cybersecurity applications, and strategic responses including policy frameworks and institutional practices. These themes collectively contribute to a nuanced appreciation of the cybersecurity landscape in the logistics sector, highlighting its operational vulnerabilities and the strategic imperatives for resilience in an era of rapid digitalization.

A. Cyber Threats

Contemporary literature consistently underscores the prevalence and diversity of cyber threats targeting logistics information systems. Among the most frequently cited forms of cyberattacks are ransomware, phishing, and Distributed Denial-of-Service (DDoS) attacks. These threats often exploit systemic vulnerabilities across interconnected logistics infrastructures, especially at critical nodes of the supply chain where multiple data systems converge (Bronk, 2020). Such attack vectors are further amplified by the increasing use of integrated platforms, cloud-based services, and IoT-enabled devices that often lack adequate cybersecurity protocols.

Malware-based threats present a particularly serious challenge, with capabilities to infiltrate control systems and paralyze operational processes. Bronk (2020) notes several incidents where malware compromised entire distribution networks, leading to transportation shutdowns, disrupted warehousing operations, and significant logistical delays. These incidents demonstrate the operational fragility induced by insufficient cyber preparedness.

The consequences of such attacks are acutely felt in two primary domains: operational efficiency and data security. Weaver et al. (2022) documented that system downtime, delayed deliveries, and reputational damage resulting from cyber incidents have led to substantial financial losses for logistics firms. In addition to direct disruptions, the compromise of sensitive data—including customer information, shipment records, and supply chain intelligence—erodes stakeholder trust

and heightens the risk of long-term systemic failure. The financial and reputational costs incurred from such incidents underscore the urgent need for proactive and layered cybersecurity defenses in logistics operations.

B. Technology Trends

To address the evolving cyber threat landscape, a range of advanced technologies have been deployed in the logistics sector. Notably, blockchain, artificial intelligence (AI), and the Internet of Things (IoT) have emerged as leading technological interventions aimed at strengthening cybersecurity postures. Ansari and Ujjan (2024) highlight the strategic implementation of blockchain technology to enhance data integrity and ensure transparency across distributed supply chain transactions. Because blockchain records are immutable and decentralized, they offer robust protection against unauthorized data manipulation, especially in documentation and tracking systems.

Demertzis et al. (2022) emphasize blockchain's potential in mitigating insider threats and data tampering by enabling traceable audit trails and automated smart contracts. These features not only enhance trust across the supply chain but also provide for real-time validation of transactional integrity.

Artificial intelligence and machine learning technologies have also been adopted to improve threat detection capabilities. AI-driven systems, as described by Schislyaeva et al. (2023), can identify anomalous network behaviors indicative of cyber intrusion, often before the attack manifests fully. Through predictive analytics and behavioral pattern recognition, these technologies offer logistics firms the ability to preemptively respond to threats, significantly reducing incident response times.

Empirical assessments reveal that the integration of AI into cybersecurity operations has led to measurable improvements in both detection accuracy and risk mitigation efficiency. Schislyaeva et al. (2023) report that AI-enabled intrusion detection systems have reduced false positives and accelerated threat classification, enhancing the effectiveness of cybersecurity teams. Furthermore, the deployment of IoT devices equipped with integrated security sensors facilitates continuous monitoring of assets and processes, thus closing visibility gaps within complex logistical ecosystems.

Together, these technologies signify a paradigmatic shift in how cybersecurity is conceptualized and operationalized within the logistics domain. Rather than relying solely on perimeter defenses, the sector is moving toward embedded, intelligent, and adaptive security frameworks that evolve with threat landscapes.

C. Strategic Responses and Policy

Beyond technological advancements, strategic and policy-driven responses play a critical role in shaping cybersecurity resilience in logistics. Various nations and organizations have adopted standardized frameworks, such as ISO/IEC 27001, to guide the development of comprehensive cybersecurity policies. Bronk (2020) and Demertzis et al. (2022) note that such standards provide a systematic foundation for risk assessment, incident management, and governance structures tailored to digital logistics environments.

Additionally, institutional best practices include the implementation of cybersecurity training programs aimed at enhancing employee awareness, the establishment of cross-functional cybersecurity committees, and the integration of cybersecurity objectives into organizational performance metrics. These efforts reflect a growing recognition that cybersecurity is not solely a technological issue, but also a matter of organizational culture and leadership.

A prominent feature of advanced cybersecurity strategies is the promotion of cross-sector collaboration. Partnerships between government agencies, logistics firms, technology providers, and research institutions have proven effective in sharing threat intelligence, developing sector-specific guidelines, and building collective response capabilities (Bronk, 2020). For example, public-private information sharing initiatives have enabled faster dissemination of threat alerts and mitigation strategies during coordinated attacks on transportation infrastructure.

However, the extent and effectiveness of these strategic responses vary significantly between developed and developing regions. In developed countries, the integration of cybersecurity into logistics operations is typically characterized by strong regulatory support, substantial investment in digital infrastructure, and a well-established cybersecurity workforce (Schislyaeva et al., 2023). These contexts allow for the deployment of sophisticated defense mechanisms, continuous system audits, and the proactive identification of emerging threats.

By contrast, logistics systems in developing countries often face critical constraints, including limited financial resources, inconsistent policy enforcement, and a shortage of skilled cybersecurity professionals. Bronk (2020) and Weaver et al. (2022) report that in such contexts, cybersecurity responses tend to be reactive, focusing on recovery after incidents rather than prevention. This gap underscores the need for capacity-building initiatives, international cooperation, and context-sensitive frameworks that account for regional disparities in technological readiness and institutional maturity.

The comparative perspective offered by these findings emphasizes that there is no one-size-fits-all solution to cybersecurity in logistics. Instead, strategies must be tailored to align with local operational realities, regulatory environments, and technological capabilities. This insight is particularly important for global logistics firms operating across multiple jurisdictions, where harmonizing cybersecurity standards and practices presents an ongoing challenge.

In conclusion, the reviewed literature affirms that cybersecurity in logistics is shaped by a complex interplay of threats, technological innovation, and strategic response mechanisms. Cyber threats such as ransomware, phishing, and DDoS attacks present significant operational and data-related risks that demand urgent attention. In response, technologies like blockchain, AI, and IoT are proving effective in enhancing security capabilities, while strategic policy interventions and international collaboration are essential for fostering systemic resilience. Nonetheless, disparities between regions highlight the importance of adaptable and inclusive approaches to cybersecurity, ensuring that protection efforts are effective across diverse logistics contexts.

The findings of this narrative review contribute to a more integrative understanding of cybersecurity in logistics information systems by bridging the gap between technical, managerial, and regulatory dimensions. While previous studies, such as those by Bronk (2020) and Demertzis

et al. (2022), have documented the growing exposure of logistics infrastructure to cyber threats, they tend to focus primarily on vulnerabilities or isolated technological solutions. This review reaffirms those findings but advances the discourse by organizing the evidence within a broader conceptual framework. This framework incorporates not only technological readiness but also systemic enablers and barriers to cybersecurity implementation, including policy structures, organizational capacity, and intersectoral coordination. Such a multidimensional approach enhances our comprehension of how logistics systems function under the pressures of digital transformation and growing cyber risks.

The thematic analysis from this review underscores the persistence and diversity of cyber threats in logistics systems, particularly the recurring patterns of ransomware, phishing, and DDoS attacks targeting interconnected operational infrastructures (Bronk, 2020). These attacks, often enabled by outdated legacy systems and inadequate cross-organizational security protocols, serve as indicators of deeper structural issues. In many logistics environments, digital modernization efforts have outpaced cybersecurity preparedness, resulting in fragmented and inconsistent implementations. This systemic misalignment suggests that the challenge is not merely technical but also rooted in institutional inertia and resource asymmetry, especially in multi-stakeholder supply chain environments.

This review identifies several systemic factors that hinder effective cybersecurity implementation. The continued reliance on legacy infrastructure emerges as a critical barrier, given its poor compatibility with modern cybersecurity architectures and limited adaptability to evolving threat landscapes. The lack of uniform cybersecurity standards and fragmented regulatory regimes across regions exacerbate these vulnerabilities, especially for logistics firms operating in transnational supply chains. As Dokuchaev and Maklachkova (2023) argue, disparate regulations across jurisdictions often lead to compliance gaps that cybercriminals can exploit. Furthermore, the absence of effective collaboration between government regulators and industry actors hampers the establishment of a cohesive security posture. These issues are compounded by the limited availability of specialized cybersecurity personnel who possess both technical expertise and domain-specific knowledge of logistics systems.

Technological innovations, particularly blockchain, artificial intelligence, and game-theoretic approaches, are central to the evolving cybersecurity landscape in logistics. Blockchain, in particular, holds promise for addressing data integrity and trust issues in multi-party transactions by enabling tamper-proof audit trails and decentralized data sharing (Ugochukwu et al., 2023). However, its integration is not without systemic challenges. The implementation of blockchain requires not only technological infrastructure but also a supportive regulatory ecosystem and interoperable standards to ensure cross-platform functionality. This review reinforces the importance of co-evolving technical innovation with institutional readiness.

Furthermore, emerging studies propose alternative strategic models to address these challenges. For instance, the application of evolutionary game theory in cybersecurity governance, as explored by Chu et al. (2024), illustrates the potential of incentive-based mechanisms to drive ethical behavior and collaborative investment in security infrastructure. Such approaches shift the analytical lens from purely defensive strategies to dynamic systems of interaction among

stakeholders. These strategies offer new perspectives on how organizational behavior, competition, and policy can be aligned to reinforce systemic resilience in logistics networks.

The implications of these findings for public policy are profound. The integrative lens adopted in this review indicates that cybersecurity policies must extend beyond technical controls to address operational procedures, regulatory coordination, and collaborative frameworks. A relevant example can be found in maritime logistics, where Melnyk et al. (2024) argue that cybersecurity policies should incorporate not only minimum technical standards but also transparency requirements, cross-border interoperability protocols, and institutional accountability. The review's synthesis suggests that aligning cybersecurity strategies with broader governance and economic development goals may be more effective in fostering resilience than isolated regulatory mandates.

In light of this, regulatory frameworks need to evolve to support innovation and flexibility while maintaining baseline security. Ugochukwu et al. (2023) advocate for policies that incentivize technological experimentation, such as blockchain pilots or AI-enabled detection systems, within safe regulatory sandboxes. Such adaptive regulatory models can reduce innovation risk while allowing for context-sensitive applications of advanced cybersecurity measures in logistics. Additionally, policy reform should consider resource allocation for workforce development, recognizing the pivotal role of human capital in sustaining secure logistics systems.

Nevertheless, this review also highlights certain limitations within the current body of literature. A predominant focus on developed economies limits the generalizability of findings to emerging markets, where infrastructure, regulatory capacity, and digital maturity may differ significantly. While studies like those by Bronk (2020) provide extensive analysis of cybersecurity in well-resourced contexts, there remains a scarcity of empirical research that captures the operational realities in lower-income countries. This gap limits our understanding of how global logistics actors can harmonize cybersecurity standards while accommodating localized constraints.

Moreover, while technological solutions are frequently presented as panaceas, their efficacy often depends on organizational commitment, user behavior, and contextual adaptation. For instance, AI-powered intrusion detection systems may perform well in controlled environments but face reduced effectiveness in real-world scenarios with incomplete data or unstructured operations (Schislyaeva et al., 2023). Thus, further empirical studies are needed to assess how these technologies perform under diverse operational conditions and to identify best practices for deployment in heterogeneous logistics settings.

Future research should also investigate the intersection between cybersecurity and sustainability goals in logistics. As global supply chains increasingly aim to reduce carbon emissions and embrace circular economy principles, digital systems used for environmental monitoring may become new attack vectors. Integrating cybersecurity with environmental governance in logistics represents an emerging frontier that warrants scholarly attention. Additionally, more interdisciplinary work is needed to explore how cybersecurity intersects with trade policy, labor regulations, and international law, especially in a post-pandemic world where geopolitical tensions influence digital infrastructure governance.

Taken together, the insights generated by this review underscore the importance of systemic, adaptable, and inclusive approaches to cybersecurity in logistics. By extending the conversation beyond technical fixes to encompass strategic, regulatory, and institutional dimensions, this review contributes a more comprehensive perspective on securing digital logistics systems in an era of increasing complexity and interdependence.

CONCLUSION

This review provides a comprehensive synthesis of the current landscape of cybersecurity in logistics information systems, revealing three critical dimensions: the prevalence of sophisticated cyber threats, the promise of emerging technologies, and the necessity of integrated strategic responses. The findings reaffirm that logistics systems are increasingly targeted by ransomware, phishing, and DDoS attacks, which compromise both operational efficiency and data security. Technological innovations such as blockchain, artificial intelligence, and IoT-integrated sensors demonstrate considerable potential in mitigating these threats, especially when supported by advanced detection and real-time response mechanisms.

However, the discussion highlights that systemic barriers remain deeply embedded in logistical infrastructures, particularly due to legacy systems, fragmented regulatory environments, and limited intersectoral collaboration. These challenges necessitate urgent regulatory updates that go beyond technical compliance and foster cross-sectoral partnerships, standardized procedures, and adaptive policy frameworks. There is also a clear need for increased investment in human capital, particularly in training logistics personnel in cybersecurity practices.

Future research should prioritize empirical studies that evaluate the real-world effectiveness of proposed technologies across diverse geographic and operational contexts. Additionally, interdisciplinary approaches that integrate cybersecurity with sustainability and trade governance are recommended to expand the scope of current knowledge. As digital logistics continues to evolve, the strategic implementation of robust cybersecurity frameworks must remain a central focus to ensure system resilience, stakeholder trust, and uninterrupted global supply chain operations.

REFERENCE

Al Firdausi, A. R., & Suprayitno, D. (2023). Application of the Economic Order Quantity (EOQ) Method in Soybean Raw Material Inventory Control at the Haji Maman Tofu Factory in Matraman District, East Jakarta. *Sinergi International Journal of Logistics*, *1*(2), 73–84.

Anugrah, D. F., & Patil, M. B. (2023). The Effect of the Application of Warehouse Management System on Goods Storage at PT Shippindo Logistics Technology. *Sinergi International Journal of Logistics*, *1*(1), 32–41.

Butar, P. A., & Ahmed, A. A. (2023). Analysis of Internal and External Factors of Transport Delay in PT Sari Dumai Oleo. *Sinergi International Journal of Logistics*, *1*(1), 63–72.

Darmiono, D. (2023). Analysing the Impact of Third-Party Involvement on Smooth Distribution in Supply Chain in Indonesia. *Sinergi International Journal of Logistics*, *1*(2), 96–107.

Marnova, B., & Tung, T. M. (2023). Analysis of the layout of the Dangerous and Toxic Goods (B3) warehouse using the 5S method (Seiri, Seiton, Seiso, Seiketsu, and Shitsuke) on PT Mitra Agung Sejati. *Sinergi International Journal of Logistics*, *1*(1), 42–62.

Meilenda, P., & Syarif, A. (2024). Reverse Logistics Analysis of Chips Products Towards Green Supply Chain Management in MSMEs. *Sinergi International Journal of Management and Business*, *2*(4), 198–210.

Sugiarto, M., & Suprayitno, D. (2023). Analysis of Factors Causing Logistics Warehouse Inventory Mismatch at PT Dai Nippon Printing Indonesia. *Sinergi International Journal of Logistics*, *1*(1), 17–31.

Sutejo, M. B., Suprayitno, D., & Latunreng, W. (2023). Controlling Raw Material Inventory using the Economic Order Quantity (EOQ) Method at PT. ICI Paints Indonesia. *Sinergi International Journal of Logistics*, *1*(3), 108–122.

Wibowo, U., Kurniawan, I. E., & Prayitno, H. (2023). Implementation of Safety Risk Management in Aircraft Airffame Maintenance. *Sinergi International Journal of Logistics*, *1*(2), 85–95.

Ansari, A. and Ujjan, R. (2024). Addressing security issues and challenges in smart logistics using smart technologies., 25-48. https://doi.org/10.1002/9781394204472.ch2

Bronk, C. (2020). Operation of transport and logistics in a time of (cyber)insecurity., 33-49. https://doi.org/10.1007/978-3-030-37752-6_3

Canepa, M., Ballini, F., Dalaklis, D., Vakili, S., & Hernandez, L. (2021). Cr cybermar as a solution path towards cybersecurity soundness in maritime logistics domain. Transactions on Maritime Science, 10(1). https://doi.org/10.7225/toms.v10.n01.011

Chu, W., Shi, Y., Jiang, X., Ciano, T., & Zhao, B. (2024). Game theory approach for secured supply chain management in effective trade management. Annals of Operations Research. https://doi.org/10.1007/s10479-023-05792-7

Demertzis, K., Kikiras, P., & Iliadis, L. (2022). A blockchained secure and integrity-preserved architecture for military logistics operations., 271-283. https://doi.org/10.1007/978-3-031-08223-8_23

Dokuchaev, V. and Maklachkova, V. (2023). Cybersecurity impact on the transport security., 1-6. https://doi.org/10.1109/emctech58502.2023.10297009

Melnyk, O., Onishchenko, O., Lohinov, O., Konoplov, A., & Lohinova, L. (2024). Contemporary strategies for advancing cybersecurity in maritime cargo transportation., 389-402. https://doi.org/10.1007/978-3-031-68372-5_21

Schislyaeva, E., Krasovskaya, I., Palkina, E., & Plis, K. (2023). The development of logistics in the context of the knowledge economy: the current state and features of management. E3s Web of Conferences, 371, 04043. https://doi.org/10.1051/e3sconf/202337104043

Ugochukwu, N., Goyal, S., & Paramasivam, G. (2023). Advanced blockchain-based scheme for efficient and secured sharing of customers information in logistics management model using rsa encryption method., 127-138. https://doi.org/10.1007/978-981-99-3716-5_12

Weaver, G., Feddersen, B., Marla, L., Wei, D., Rose, A., & Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: an optimization-based approach. Transportation Research Part C Emerging Technologies, 137, 103423. https://doi.org/10.1016/j.trc.2021.103423