International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Cyber-resilient supply chains: A framework for national security

OJO TITILAYO PRECIOUS *

Department of Global Supply Chain Management and Operations, Faculty of Business, University of Indianapolis, Indianapolis, Indiana, USA.

International Journal of Science and Research Archive, 2025, 14(01), 1368-1378

Publication history: Received on 01 December 2024; revised on 11 January 2025; accepted on 13 January 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.14.1.0081

Abstract

This study examines the critical need for cyber-resilient supply chains in ensuring national security and operational efficiency. It examines the vulnerabilities posed by cyber threats and highlights the role of emerging technologies such as artificial intelligence, blockchain, and advanced analytics in enhancing supply chain resilience. Using the research onion framework, the study adopts a quantitative approach, analyzing quantitative data from reputable statistical sources. The findings emphasize the significance of integrating advanced technologies to mitigate risks, enhance transparency, and secure supply chain operations. The study concludes that proactive adoption of these technologies is vital for countering cyber threats and maintaining the seamless flow of goods and services in an increasingly digital world. The recommendations focus on encouraging technological innovation and collaboration to strengthen cyber resilience in supply chains.

Keywords: Supply Chain Resilience; National Security; Artificial Intelligence; Blockchain Technology; Supply

1. Introduction

The increasing interconnectedness of global supply chains has brought remarkable efficiencies but also heightened vulnerabilities to cyber threats (Nandi et al., 2021). Over the years, supply chain disruptions have been caused by various incidents, including natural disasters and industrial accidents. Notable examples include the fire at the Philips microchip plant in Albuquerque, New Mexico (2000), Hurricane Katrina (2006), and the tsunami in Japan (2011). More recent disruptions include the explosion at the BASF plant in Germany (2016) and the fire at the Meridian Magnesium Products factory in Michigan (2018) (Baryannis et al., 2019). These events highlight the vulnerability of supply chains to unforeseen disruptions and the need for enhanced resilience strategies.

In an era where data serves as the backbone of logistics and operations, cyberattacks on supply chain networks pose significant risks to national security (Sobb et al., 2020). Recent high-profile cyberattacks, such as the SolarWinds incident and the Colonial Pipeline attack, have shown the critical need for robust cybersecurity measures within supply chain networks (Watney, 2022). Sophisticated cyber threats, such as ransomware, phishing, and supply chain infiltration, can disrupt critical infrastructure, compromise sensitive information, and jeopardize economic stability (Pandey et al., 2020). These incidents have highlighted the cascading effects of cyber disruptions, wherein a breach in one node can propagate through the entire supply chain, affecting multiple stakeholders.

The United States among other companies who are key players in the global economy, have faced significant impacts from supply chain disruptions, including shortages of essential goods, delivery delays, and rising production and distribution costs (Oriekhoe et al., 2024). These catastrophes led to significant decreased revenues and sales, and production suspensions that impacted workforce utilization (Ivanov & Dolgui, 2021). In order to address these challenges, businesses and policymakers have increasingly turned to technology to improve supply chain efficiency,

[*] Corresponding author: OJO TITILAYO PRECIOUS

transparency, and agility. Innovations like blockchain, artificial intelligence, the Internet of Things (IoT), and advanced analytics are known to offer promising solutions for optimizing processes, mitigating risks, and ensuring the smooth flow of goods from origin to consumer (Yeboah-Ofori et al., 2022). Despite these advancements, however, critical challenges remain.

The nexus between cyber resilience and national security shows the urgency of adopting proactive strategies. Governments and organizations are increasingly prioritizing the integration of cybersecurity measures into supply chain management (Rowan & Laffey, 2020). However, despite efforts to bolster cybersecurity practices, gaps remain in addressing vulnerabilities that arise from third-party dependencies, inadequate security protocols, and evolving threat landscapes (Watney, 2022). A comprehensive framework for enhancing cyber resilience in supply chains is essential to mitigate risks and enhance preparedness.

The overall aim of this study is focuses on improving the security of supply chains to protect against cyberattacks, which are a growing threat to national security. To achieve this, the study intends to identify key vulnerabilities in supply chains, examines how technologies like AI and blockchain can help prevent cyber risks, and provides solutions to make supply chains stronger.

2. Literature Review

The literature on cyber-resilient supply chains presents the relationship of cybersecurity, supply chain management, and national security. This section looks at key themes such as the impact of cyber threats on supply chains, the role of emerging technologies in enhancing resilience, relevant theoretical frameworks, frameworks proposed for mitigating cyber risks in supply chain systems, and the relevant existing gaps identified.

2.1. Cyber Threats and Supply Chain Vulnerabilities

Cyber threats refer to any malicious attempts or actions designed to compromise the confidentiality, integrity, or availability of digital information, systems, or networks (Yeboah-Ofori et al., 2022). These can include activities such as hacking, data breaches, malware attacks, and ransomware that aim to disrupt, steal, or manipulate data and operational processes. Supply chain vulnerabilities on the other hand refer to weaknesses or gaps in a supply chain's processes, technologies, or systems that expose it to potential risks, including disruptions from cyberattacks, natural disasters, or operational failures (Pandey et al., 2020). These vulnerabilities may arise from reliance on third-party suppliers, outdated technologies, or insufficient risk management practices, making the supply chain susceptible to both cyber and physical disruptions (Shih, 2020).

The increasing reliance on interconnected systems and external providers has amplified cyber risks within supply chains. Pandey et al. (2020) conceptualized the multifaceted nature of cybersecurity risks, emphasizing the ripple effects of disruptions on globalized supply chains. Ransomware attacks, data breaches, and phishing campaigns, as identified by Sobb et al. (2020), remain critical challenges. Incidents such as the SolarWinds breach and Colonial Pipeline attack illustrate how vulnerabilities at a single node can compromise the entire network, eroding trust and operational stability (Watney, 2022). These studies confirms the urgent need for comprehensive strategies to address these threats across the supply chain spectrum.

2.2. Emerging Technologies for Cyber Resilience

Emerging Technologies for Cyber Resilience refer to advanced and innovative technological solutions designed to enhance an organization's ability to anticipate, withstand, recover, and adapt to cyber threats and disruptions (Sobb et al., 2020). These technologies, such as blockchain, artificial intelligence (AI), machine learning, and the Internet of Things (IoT), enable organizations to detect vulnerabilities, mitigate risks, and improve decision-making processes in real-time (Yeboah-Ofori et al., 2022).

This enables the organization to ensure the continuity and security of critical infrastructure and supply chain operations. For instance, blockchain technology helps secures data through immutable records, reducing fraud and enhancing traceability (Rejeb et al., 2021). Artificial intelligence and machine learning enable predictive analytics and threat detection, as shown by Yeboah-Ofori et al. (2022), who highlighted their role in proactively addressing vulnerabilities in supply chain systems. IoT devices further bolster real-time monitoring, facilitating swift responses to anomalies (Modgil et al., 2022). Despite these benefits, challenges such as high implementation costs, interoperability issues, and organizational resistance remain significant barriers (Pandey et al., 2020).

2.3. Theoretical Frameworks for Cyber-Resilient Supply Chains

Several theoretical perspectives guide the development of cyber-resilient supply chains. These frameworks provide a robust foundation for understanding how organizations can strengthen their supply chain resilience. The study focuses on three theoretical perspectives as shown below, considered relevant to this study.

- **Dynamic Capability Theory (DCT):** this framework emphasizes adaptability, advocating the importance of innovation and agility in responding to cyber threats (Ghosh et al., 2022). DCT is particularly relevant when it comes to navigating the evolving nature of cybersecurity risks (Sobb et al., 2020).
- **Resource-Based View (RBV):** RBV advocates leveraging unique resources such as advanced AI and blockchain technologies to establish a competitive edge and mitigate risks (Barney, et al., 2021; Yeboah-Ofori et al., 2022).
- **Institutional Theory:** Highlighting the role of regulatory and normative influences, this theory explores how compliance with cybersecurity standards and collaboration among stakeholders drive resilience-building efforts (Scott, 2005; Watney, 2022).

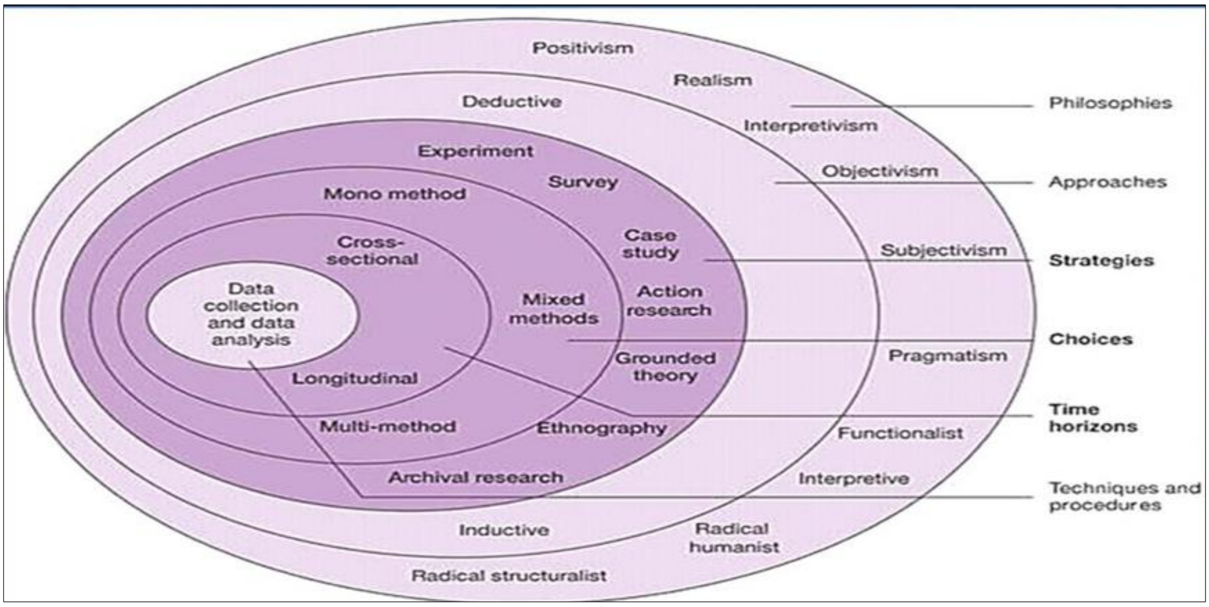
2.4. Frameworks for Enhancing Supply Chain Cyber Resilience

Practical models for mitigating cyber risks emphasize technology integration and stakeholder collaboration. For example, Dursun et al. (2022) proposed a blockchain-based framework that enhances data security, while Vanoy (2023) recommended integrating policy measures with technological solutions. Yeboah-Ofori et al. (2022) advocated for the adoption of machine learning systems to improve threat prediction capabilities. These approaches confirm the importance of multi-layered defense strategies that combine technological innovation with regulatory and organizational measures. However, gaps remain in customizing these models to diverse and dynamic threat environments, particularly in developing regions with limited resources (Pandey et al., 2020).

2.5. Synthesis of Gaps in Literature

Despite substantial advancements, notable gaps persist. Integration of multiple technologies into cohesive frameworks has been underexplored. Additionally, adapting these frameworks to varying geopolitical and economic contexts remains a challenge. Additionally, limited research exists on the practical application of theoretical constructs in real-world supply chain environments. Addressing these gaps requires the development of comprehensive models that integrate technological, organizational, and policy dimensions to build robust, cyber-resilient supply chains.

3. Methodology



Source: Saunders et al. (2012)

Figure 1 Saunders' Research Onion Framework

This section of the study adopts a structured approach based on the Research Onion Framework by Saunders, Lewis, and Thornhill (2019). This framework guides the research design by layering different stages of the research process to ensure a comprehensive and systematic approach. The methodology is divided into several layers, starting from the research philosophy and culminating in the data collection and analysis techniques.

The following outlines the approach adopted for this study:

- **Research Philosophy:** The study is grounded in a pragmatic philosophy, which emphasizes practical solutions to real-world problems. Pragmatism supports the use of both qualitative and quantitative methods, enabling the research to draw on various sources of evidence to develop a comprehensive understanding of cyber resilience in supply chains.
- **Research Approach:** The research adopts a deductive approach, beginning with existing theories and concepts related to cyber resilience and supply chain management. Theoretical frameworks, such as the **dynamic capability theory (DCT),** resource-based view (RBV) and the institutional theory (TPB), are applied to explore the relationship between emerging technologies and supply chain resilience. The study tests the hypotheses derived from these theories, with a focus on identifying causal relationships.
- **Research Strategy:** A quantitative method strategy is employed, which focuses on quantitative surveys. The quantitative surveys capture broader patterns and statistical relationships between variables. The method enables triangulation, improving the reliability and validity of the findings.
- **Research Choice:** The study follows a quantitative method design, utilizing quantitative data collection techniques to achieve a comprehensive analysis. This allows for a deeper exploration of the research objectives, leveraging the strengths of the method to gather rich data and statistical insights.
- **Time Horizon:** The research adopts a cross-sectional time horizon, meaning the data is collected at a single point in time. This is appropriate for understanding the current state of cyber resilience in supply chains and the adoption of emerging technologies. A longitudinal study could be considered for future research to examine changes over time.
- **Data Collection Techniques and Procedures:** Data for this study is collected through quantitative method.. The quantitative data is obtained from reputable statistics platforms such as Statista, Mckinsey and IBM websites. The quantitative data is analyzed through statistical analysis and interpretation of the data from these platforms.

4. Data Analysis and Findings

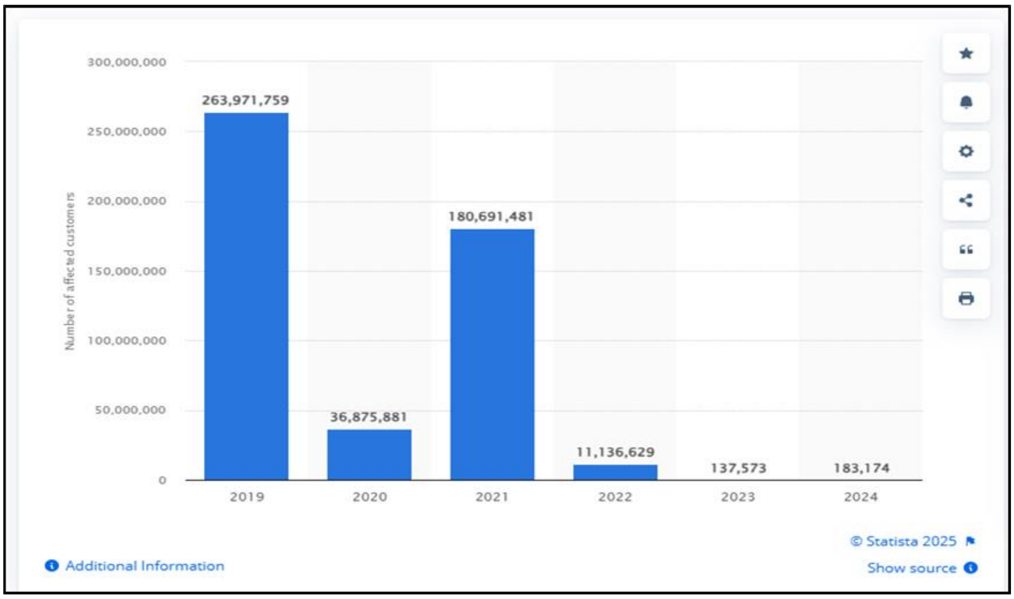
The findings from the analysis conducted on the collected data from the statistical data houses are presented in this section. The data for the different descriptive analysis below were gotten from secondary sources such as Statista, Mckinsey and IBM websites. The descriptive analysis presented in this section are structured in line with the objectives of the study.

4.1. Descriptive Analysis on Current Cybersecurity Challenges and Vulnerabilities in Global Supply Chains

This first objective was formulated to establish the current cybersecurity challenges and vulnerabilities in global supply chains, while also focusing on their implications for national security.

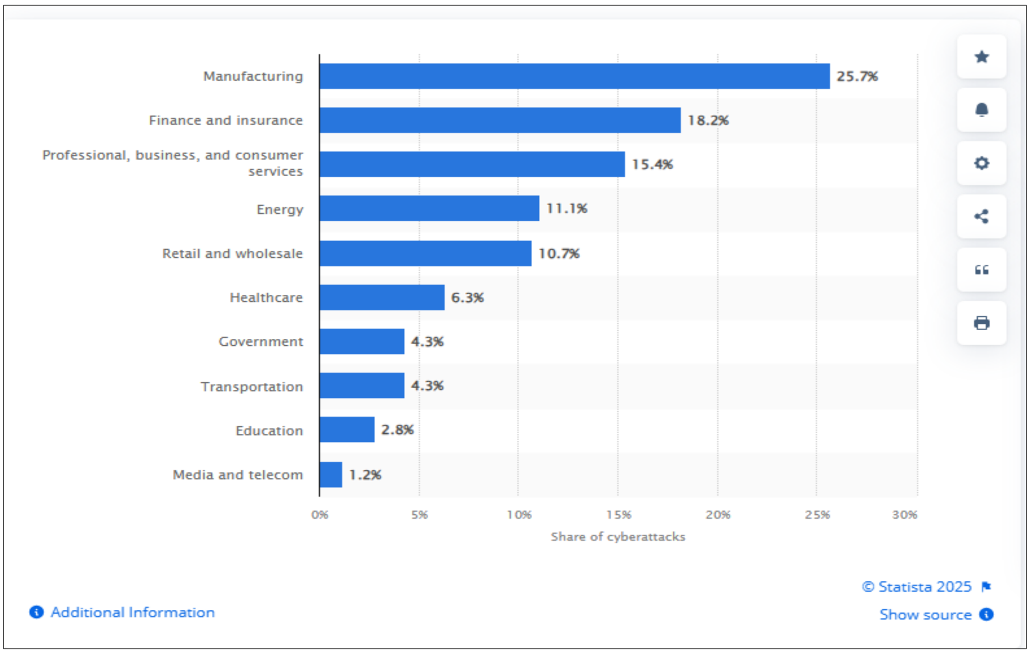
As presented below in Figure 2, supply chain cyberattacks have significantly impacted customers worldwide in recent years. In 2024, approximately 183,174 customers were affected globally, marking a 33% increase from the 137,573 affected in 2023. This upward trend contrasts with the substantial declines observed since the peak of over 263 million impacted customers in 2019. Despite a notable reduction in the number of software packages affected by these attacks from 17,150 in early 2023 to 590 in 2024, the number of impacted customers has risen. This suggests that recent attacks have become more targeted and effective, causing significant disruptions even with fewer compromised software packages.

Common attack vectors include malware infections, phishing, and the exploitation of vulnerabilities in third-party vendors (Pandey et al., 2020; Sobb et al., 2020). The increasing complexity and interconnectivity of modern supply chains have made organizations more susceptible to such attacks, further confirming the need for robust cybersecurity measures to protect both businesses and their customers.



Source: Statista (2024)

Figure 2 Annual number of customers impacted by supply chain cyberattacks worldwide from 2019 to 2024



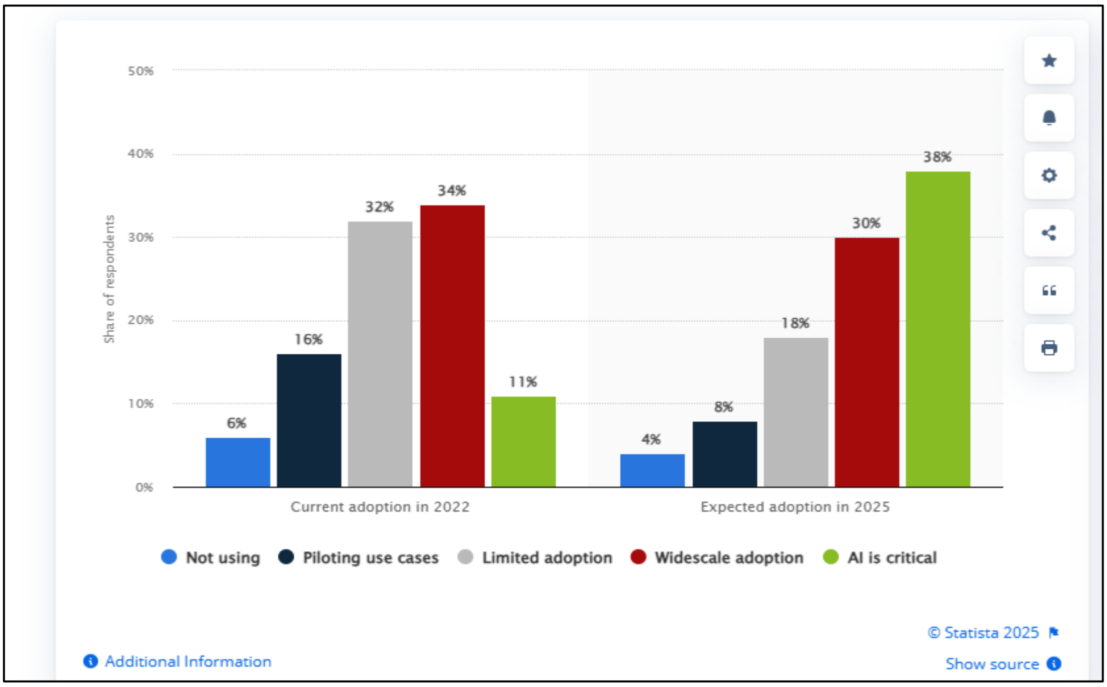
Source: Statista (2024a)

Figure 3 Annual number of customers impacted by supply chain cyberattacks worldwide from 2019 to 2024

Figure 3 presents relevant statistics with respect to the distribution of supplychain cyberattacks across industries worldwide. In 2023, the manufacturing sector experienced the highest share of cyberattacks globally, accounting for nearly 25% of the total incidents. The finance and insurance industry followed, representing approximately 18% of attacks, while professional, business, and consumer services sectors were targeted in about 15.4% of cases (Statiata, 2024a). These statistics highlight the critical need for robust cybersecurity measures across all industries, especially those most frequently targeted by cybercriminals.

4.2. Descriptive Analysis on the Role of Emerging Technologies, such as AI in Enhancing Cyber Resilience within Supply Chains

Emerging technologies, particularly artificial intelligence (AI), are playing an increasingly critical role in enhancing cyber resilience within supply chains. Descriptive analytical findings as shown in Figure 4 and Figure 5 report confirms that AI's ability to process vast datasets, detect anomalies, and predict potential threats, makes it a valuable tool for mitigating cyber risks. Recent studies indicate that AI-powered cybersecurity solutions are widely adopted, with approximately 64% of businesses in the Asia-Pacific region and 57% in Europe reporting significant impacts of AI on supply chain resilience (Statista, 2024c).



Source: Statista (2024b)

Figure 4 Artificial intelligence (AI) adoption rate in supply chain and manufacturing businesses worldwide in 2022 and 2025

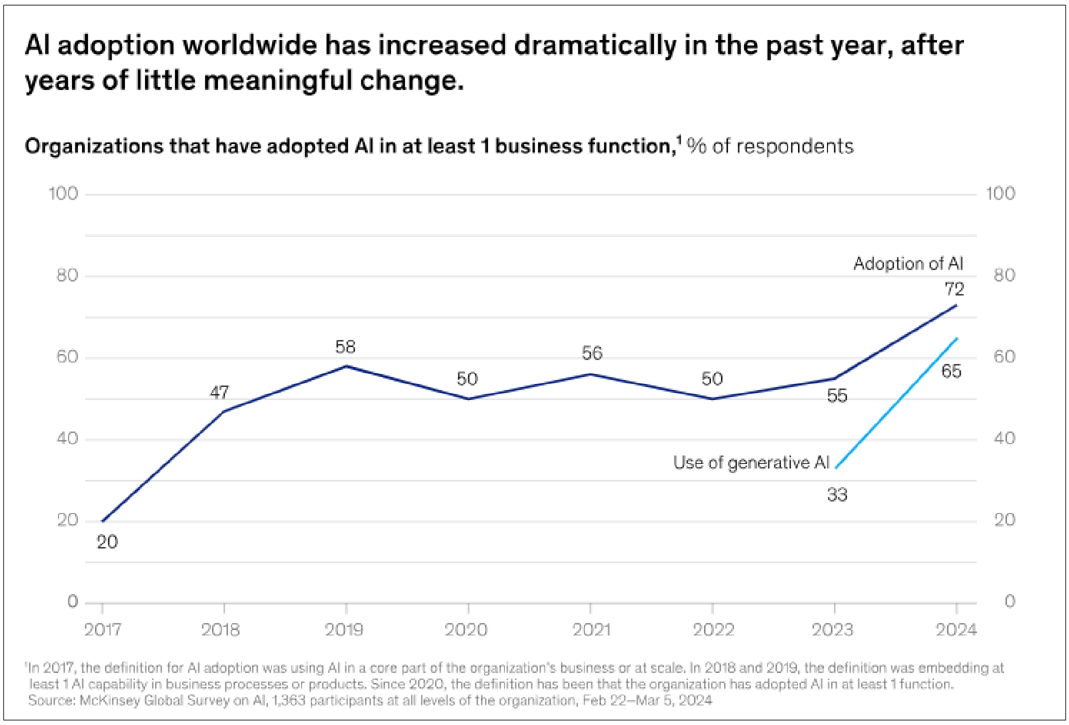
The adoption of artificial intelligence (AI) in supply chain and manufacturing businesses is projected to increase significantly between 2022 and 2025 as presented in Figure 4. In 2022, over one-third of executives anticipated widescale AI adoption within their companies. Only 11% of the executives perceived AI to be critical as of 2022, although this percentage is expected to rise sharply in subsequent years, reaching a projected 38% in 2025 (Statista, 2024b).

In another survey, it was reported that he Asia-Pacific region leads this transformation, with 64% of executives expecting the greatest impact of AI and machine learning (ML) on supply chains by 2025. Europe and North America follow at 57% and 49%, respectively (Statista, 2024c). This indicates a strong commitment to leveraging AI for supply chain optimization in these regions. These developments proves the growing importance of AI in supply chain management, with businesses worldwide recognizing its potential to drive efficiency, resilience, and innovation.

Similarly, Figure 5 shows the findings from a survey conducted by McKinsey in early 2024, which reported that AI adoption has jumped to 72% in 2024, all the way from 55% and 50% in 2023 and 2022 respectively (Singla et al., 2024).

This survey conducted by McKinsey highlights the truly global nature of AI adoption, with substantial growth observed in professional services, manufacturing, and marketing sectors (Singla et al., 2024; Thormundsson, 2024). Supporting this trend, IBM's Global AI Adoption Index 2022 reported an increase in global AI adoption from 31% in 2021 to 35% in 2022 (Armonk, 2022). This growth is largely attributed to businesses recognizing AI's value in navigating post-COVID-19 challenges and advancing digital transformation, despite facing talent and skill shortages (Singla et al., 2024).

These findings therefore supports that AI helps to predict and prevent cyberattacks by identifying vulnerabilities, while machine learning strengthens defenses. On the other hand, blockchain ensures secure data sharing, and altogether these advance technologies enhance cybersecurity and supply chain resilience (Pandey et al., 2020; Sobb et al., 2020).



Source: Singla et al. (2024)

Figure 5 Surge in AI Adoption Worldwide

4.3. Comprehensive Framework for Developing Cyber-Resilient Supply Chains that Support National Security Objectives

This section presents different propositions on the development of a comprehensive framework to ensure cyber-resilient supply chains that support national security objectives. The framework focuses on integrating advanced technologies, such as AI, blockchain, and predictive analytics, to enhance cybersecurity, improve data traceability, and safeguard critical infrastructure.

Table 1 Summarizes the proposed key components of a comprehensive framework for developing cyber-resilient supply chains that support national security objectives J

S/N	Component	Description	Relevant Citations
1.	Strategic Integration of Cybersecurity and National Security Policies	Align cybersecurity strategies with national security objectives. Establish clear guidelines and regulations for collaboration between government, defense, and private sectors.	Pandey (2020); Sobb et al. (2020)
2.	Risk Assessment and Vulnerability Management	Conduct regular cybersecurity audits, vulnerability assessments, and prioritize risks using advanced technologies like AI and predictive analytics.	Benmamoun et al. (2024); Nandi et al. (2021)
3.	Cybersecurity Integration with Supply Chain Operations	Integrate cybersecurity measures at every step of the supply chain, utilizing technologies like blockchain and AI-driven anomaly detection systems.	Modgil et al. (2022); Pandey (2020)
4.	Building Cyber-Resilient Infrastructure	Enhance digital infrastructure with secure communication networks, redundancy in systems, and decentralized data storage.	Pandey (2020); Watney (2022);
5.	Collaboration with International Partners	Foster international cooperation on cybersecurity standards, information sharing, and coordination of responses to global cyber threats.	Ghosh et al. (2022);

6.	Training and Capacity Building	Implement continuous training programs for supply chain professionals to equip them with the necessary cybersecurity skills.	Odimarha et al. (2024)
7.	Legal and Regulatory Frameworks	Establish clear, enforceable laws and regulations that mandate compliance with cybersecurity standards across supply chains.	Tiwari et al. (2023)
8.	Resilient Supply Chain Design	Design flexible and redundant supply chains to mitigate risks from disruptions caused by cyberattacks or natural disasters.	Baryannis et al. (2019); Camur et al. (2024)

5. Discussion on the Theoretical Implications of the Developed Frameworks

The proposed framework for developing cyber-resilient supply chains aligns with the theoretical frameworks examined in this study, such as the Dynamic Capability Theory (DCT), the Resource-Based View (RBV), and Institutional Theory (IT). DCT emphasizes an organization's ability to adapt to changing environments by reconfiguring its capabilities (Teece, 2014). The framework's emphasis on integrating cybersecurity strategies and technologies like AI and blockchain into supply chain operations directly relates to DCT, as these capabilities enable firms to rapidly respond to emerging threats, ensuring resilience against cyber disruptions (Baryannis et al., 2019; Benmamoun et al., 2024). The continuous risk assessments and adaptive infrastructure planning, which are central to the framework, help organizations reconfigure their supply chain processes in response to evolving cyber risks, a key tenet of DCT (Ghosh, 2022). Testing the hypothesis derived from DCT in this context would examine how firms leverage dynamic capabilities, such as technological investments and process reengineering, to enhance their cyber-resilience.

The Resource-Based View (RBV) is another relevant theoretical lens applied in the proposed framework. RBV suggests that competitive advantage stems from resources that are valuable, rare, and difficult to imitate (Barney et al., 2021). Within this framework, organizations that integrate cutting-edge technologies such as blockchain and AI into their supply chains possess unique, inimitable resources that can drive superior performance in the face of cyber threats (Kosasih et al., 2024). Therefore, by emphasizing the role of AI-driven analytics and secure digital infrastructure, the framework proves the importance of leveraging proprietary technology as a source of resilience. From an RBV perspective, organizations with advanced cybersecurity resources, including secure networks and predictive analytics tools, are better positioned to prevent, detect, and recover from cyberattacks, thus enhancing supply chain resilience (Pandey et al., 2020). Therefore, testing hypotheses around the RBV would assess whether firms with more robust cybersecurity resources experience fewer disruptions and faster recovery from cyber incidents.

Institutional Theory (IT), particularly the Theory of Planned Behavior (TPB), also plays a significant role in the framework's design. IT examines how external pressures, such as regulatory compliance and industry standards, shape organizational behavior (DiMaggio & Powell, 1983). TPB, a subset of IT, suggests that behaviors are influenced by intentions, which are in turn shaped by attitudes, subjective norms, and perceived behavioral control (Ajzen, 1991). In the context of the framework, organizations' behaviors regarding cybersecurity integration are influenced by legal mandates and industry best practices, which shape their intention to adopt resilient technologies. The framework's focus on collaboration with international partners and compliance with regulations aligns with TPB's emphasis on institutional pressures influencing organizational decisions (Upadhyay & Shukla, 2025). Testing hypotheses based on IT and TPB shows how external institutional pressures drive the adoption of cybersecurity measures and shape supply chain resilience practices.

6. Conclusion

Combating cyberattacks is essential for efficient supply chain management. Most especially when utilizing technologies like artificial intelligence, blockchain, and analytics strengthens resilience, mitigates risks, and ensures secure and reliable operations in a digitalized world. This research contributes to the growing body of knowledge on supply chain security and provides valuable insights for policymakers, businesses, and stakeholders to fortify global supply chains against evolving cyber threats while ensuring the seamless and secure flow of goods and services.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179-211.

[2] Al-Dweiri, M., Ramadan, B., Rawshdeh, A., Nassoura, A., Al-Hamad, A., & Ahmad, A. (2024). The mediating role of lean operations on the relationship between supply chain integration and operational performance. Uncertain Supply Chain Management, 12(2), 1163–1174. https://doi.org/10.5267/j.uscm.2023.9.010

[3] Allahham, M., & Ahmad, A. (2024). AI-induced anxiety in the assessment of factors influencing the adoption of mobile payment services in supply chain firms: A mental accounting perspective. International Journal of Data and Network Science, 8(1), 505–514. https://doi.org/10.5267/j.ijdns.2023.9.010

[4] Armonk (2022). Global AI Adoption Index 2022. Retrieved on January 5 2024, from: https://newsroom.ibm.com/2022-05-19-Global-Data-from-IBM-Shows-Steady-AI-Adoption-as-Organizations-Look-to-Address-Skills-Shortages,-Automate-Processes-and-Encourage-Sustainable-Operations

[5] Barney, J. B., Ketchen Jr, D. J., & Wright, M. (2021). Resource-based theory and the value creation framework. Journal of Management, 47(7), 1936-1955.

[6] Baryannis, G., Dani, S., & Antoniou, G. (2019). Predicting supply chain risks using machine learning: The trade-off between performance and interpretability. Future Generation Computer Systems, 101, 993–1004. https://doi.org/10.1016/j.future.2019.07.059

[7] Baryannis, G., Dani, S., Validi, S., & Antoniou, G. (2019). Decision support systems and artificial intelligence in supply chain risk management. In Revisiting Supply Chain Risk (pp. 53–71). Springer. https://doi.org/10.1007/978-3-030-18129-4_5

[8] Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: State of the art and future research directions. International Journal of Production Research, 57(7), 2179–2202. https://doi.org/10.1080/00207543.2018.1530476

[9] Benmamoun, Z., Khlie, K., Dehghani, M., & Gherabi, Y. (2024). WOA: Wombat optimization algorithm for solving supply chain optimization problems. Mathematics, 12(7), 1059. https://doi.org/10.3390/math12071059

[10] Camur, M. C., Ravi, S. K., & Saleh, S. (2024). Enhancing supply chain resilience: A machine learning approach for predicting product availability dates under disruption. Expert Systems with Applications, 247, 123226. https://doi.org/10.1016/j.eswa.2024.123226

[11] Chatterjee, S., Rana, N. P., Dwivedi, Y. K., & Baabdullah, A. M. (2021). Understanding AI adoption in manufacturing and production firms using an integrated TAM-TOE model. Technological Forecasting and Social Change, 170, 120880. https://doi.org/10.1016/j.techfore.2021.120880

[12] Chowdhury, P., Paul, S. K., Kaisar, S., & Moktadir, M. A. (2021). COVID-19 pandemic-related supply chain studies: A systematic review. Transportation Research Part E: Logistics and Transportation Review, 148, 102271. https://doi.org/10.1016/j.tre.2021.102271

[13] DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. American sociological review, 48(2), 147-160.

[14] Ghosh, S., Hughes, M., Hodgkinson, I., & Hughes, P. (2022). Digital transformation of industrial businesses: A dynamic capability approach. Technovation, 113, 102414.

[15] Ivanov, D., & Dolgui, A. (2021). A digital supply chain twin for managing disruption risks and resilience in the era of Industry 4.0. Production Planning & Control, 32(9), 775–788. https://doi.org/10.1080/09537287.2020.1768450

[16] Kosasih, E. E., Papadakis, E., Baryannis, G., & Brintrup, A. (2024). A review of explainable artificial intelligence in supply chain management using neurosymbolic approaches. International Journal of Production Research, 62(4), 1510–1540. https://doi.org/10.1080/00207543.2023.2165641

[17] Lim, M. K., Li, Y., Wang, C., & Tseng, M. L. (2021). A literature review of blockchain technology applications in supply chains: A comprehensive analysis of themes, methodologies, and industries. Computers & Industrial Engineering, 154, 107133. https://doi.org/10.1016/j.cie.2021.107133

[18] Modgil, S., Singh, R. K., & Hannibal, C. (2022). Artificial intelligence for supply chain resilience: Learning from COVID-19. The International Journal of Logistics Management, 33(4), 1246–1268. https://doi.org/10.1108/IJLM-03-2022-0138

[19] Nandi, S., Sarkis, J., Hervani, A. A., & Helms, M. M. (2021). Redesigning supply chains using blockchain-enabled circular economy and COVID-19 experiences. Sustainable Production and Consumption, 27, 10–22. https://doi.org/10.1016/j.spc.2020.10.019

[20] Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. World Journal of Advanced Science and Technology, 5(1), 026-030.

[21] Onyango, J. O. (2024). Supply chain solutions for essential medicine availability during COVID-19 pandemic. Journal of Humanitarian Logistics and Supply Chain Management, 14(1), 118–133. https://doi.org/10.1108/JHLSCM-10-2023-0068

[22] Oriekhoe, O. I., Ashiwaju, B. I., Ihemereze, K. C., & Ikwue, U. (2024). Review of big data in FMCG supply chains: US company strategies and applications for the African market. International Journal of Management & Entrepreneurship Research, 6(1), 87–103. https://doi.org/10.5267/j.ijmer.2024.1.005

[23] Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. Journal of Global Operations and Strategic Sourcing, 13(1), 103-128.

[24] Park, A., & Li, H. (2021). The effect of blockchain technology on supply chain sustainability performances. Sustainability, 13(4), 1726. https://doi.org/10.3390/su13041726

[25] Pullman, M., McCarthy, L., & Mena, C. (2024). Breaking bad: How can supply chain management better address illegal supply chains? International Journal of Operations & Production Management, 44(1), 298–314. https://doi.org/10.1108/IJOPM-11-2022-0756

[26] Rowan, N. J., & Laffey, J. G. (2020). Challenges and solutions for addressing critical shortage of supply chain for personal and protective equipment (PPE) arising from Coronavirus disease (COVID-19) pandemic—Case study from the Republic of Ireland. Science of the Total Environment, 725, 138532. https://doi.org/10.1016/j.scitotenv.2020.138532

[27] Sadeghi, K., Ojha, D., Kaur, P., Mahto, R. V., & Dhir, A. (2024). Explainable artificial intelligence and agile decision-making in supply chain cyber resilience. Decision Support Systems, 180, 114194. https://doi.org/10.1016/j.dss.2024.114194

[28] Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson Education.

[29] Saunders, M., Lewis, P. & Thronhill, A. (2012). Research Methods for Busdiness Students (4th ed.). Harlow: Pearson Education Ltd

[30] Scott, W. R. (2005). Institutional theory: Contributing to a theoretical research program. Great minds in management: The process of theory development, 37(2), 460-484.

[31] Shih, W. C. (2020). Global supply chains in a post-pandemic world. Harvard Business Review, 98(5), 82–89.

[32] Singla, A., Sukharevsky, A., Yee, L., & Chui, M. (2024). The state of AI in early 2024: Gen AI adoption spikes and starts to generate value. Retrieved on January 5 2024, from: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai

[33] Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. Electronics, 9(11), 1864.

[34] Statista. (2024). Number of customers affected by supply chain cyberattacks worldwide from 2019 to 2024. Retrieved January 5, 2025, from https://www.statista.com/statistics/1375129/supply-chain-attacks-customers-affected-global/

[35] Statista. (2024a). Distribution of cyberattacks across worldwide industries in 2023. Retrieved January 5, 2025, from https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/

[36] Statista. (2024b). Artificial intelligence (AI) adoption rate in supply chain and manufacturing businesses worldwide in 2022 and 2025. Retrieved January 5, 2025, from https://www.statista.com/statistics/1346717/ai-function-adoption-rates-business-supply-chains/

[37] Statista. (2024c). Impact of artificial intelligence (AI) and machine learning (ML) on supply chain management from 2023 to 2025, by region. Retrieved January 5, 2025, from https://www.statista.com/statistics/1449166/impact-of-ai-ml-on-supply-chains-in-business/?utm_source=chatgpt.com

[38] Sunny, J., Undralla, N., & Pillai, V. M. (2020). Supply chain transparency through blockchain-based traceability: An overview with demonstration. Computers & Industrial Engineering, 150, 106895. https://doi.org/10.1016/j.cie.2020.106895

[39] Thormundsson, B. (2024). Artificial intelligence (AI) adoption worldwide 2022, by industry and function. Retrieved on August 29 2024, from: https://www.statista.com/statistics/1112982/ai-adoption-worldwide-industry-function/

[40] Tiwari, S., Sharma, P., Choi, T. M., & Lim, A. (2023). Blockchain and third-party logistics for global supply chain operations: Stakeholders' perspectives and decision roadmap. Transportation Research Part E: Logistics and Transportation Review, 170, 103012.

[41] Upadhyay, A., & Shukla, A. (2025). Development of circular supply chain implementation model for MSMEs using extended theory of planned behaviour and DEMATEL approach. Management Science Letters, 15(3), 113-122.

[42] Watney, M. (2022). Cybersecurity threats to and cyberattacks on critical infrastructure: a legal perspective. In European conference on cyber warfare and security, 21(1), 19-327).

[43] Wong, L. W., Leong, L. Y., Hew, J. J., Tan, G. W., & Ooi, K. B. (2020). Time to seize the digital evolution: Adoption of blockchain in operations and supply chain management among Malaysian SMEs. International Journal of Information Management, 52, 101997. https://doi.org/10.1016/j.ijinfomgt.2020.101997

[44] Yeboah-Ofori, A., Swart, C., Opoku-Boateng, F. A., & Islam, S. (2022). Cyber resilience in supply chain system security using machine learning for threat predictions. Continuity & Resilience Review, 4(1), 1-36.

[45] Zhang, G., Yang, Y., & Yang, G. (2023). Smart supply chain management in Industry 4.0: The review, research agenda, and strategies in North America. Annals of Operations Research, 322(2), 1075–1117. https://doi.org/10.1007/s10479-021-04393-1