International Journal of Scientific Research and Modern Technology (IJSRMT) ijsrmt.com
Volume 4, Issue 9, 2025
DOI: https://doi.org/10.38124/ijsrmt.v4i9.829

Developing Resilient, Technology-Enabled Supply Chains to Strengthen National Security and Ensure Critical Goods Availability

Desmond Ohene Poku[1]

[1]Consultant – Cybersecurity & Supply Chain Security, University of Fairfax

Publication Date: 2025/09/19

Abstract

The modern world economy is experiencing unprecedented shocks that undermine the national security due to vulnerabilities in supply chains. The paper will focus on the nexus between technological innovation and supply chain resilience in acquiring the necessary commodities and services to a national defense as well as the civilian population. In an in-depth evaluation of new technologies such as artificial intelligence/blockchain and Industry 4.0, this study shows how a technologically-facilitated supply chain can bolster national security preparedness. The research paper is a synthesis of the available literature that introduces a framework of designing sound supply chain architecture that is resistant to disruptions but is operationally efficient. Important results have shown that countries that put in place very comprehensive digital transformation strategies in their supply chains have much higher resilience metrics and recover more quickly in the face of crisis. The study helps in the realization of the potential of technological integration in converting any vulnerabilities that are experienced in the supply chain into strategic benefits in terms of national security.

Keywords: *Supply Chain Resilience, National Security, Digital Transformation, Artificial Intelligence, Blockchain Technology, Critical Infrastructure.*

I. INTRODUCTION

The concept of national security in the twenty first century goes much further than conventional military aspects into the areas of economic stability, technological independence and the uninterrupted supply of important goods and services. The vulnerability of global supply chains and their real significance to national security became obvious during the COVID-19 pandemic because nations struggled with a lack of medical supplies, semiconductors, and other significant components (Singh et al., 2021; Paul and Chowdhury, 2020). These shocks demonstrated the necessity of resilient, technology-enabled supply chains that would be able to continue functioning under extreme pressure and fulfil national security goals.

The idea behind the supply chain resilience has become a commercial issue but now carries the national strategic significance. According to Xiong et al. (2025), disruptions in semiconductor supply chains are enough to spread across whole economies and impact not just the automotive manufacturing industry but defense systems as well. Likewise, Ma et al. (2025) show based on network modeling views that supply chain resilience needs systematic methods that look at both abilities of the technologies and structural susceptibilities.

The list of threats to contemporary supply chains is becoming more complicated with natural disasters, geopolitical crises, cyber-attacks, and disruptions related to the pandemic. Conventional risk management solutions are not sufficient in addressing these complex challenges and thus radical change in the way countries ought to deal with supply chain security is required. The incorporation of the new technologies like artificial intelligence, blockchain, and Internet of Things (IoT) systems presents unparalleled chances to promote supply chain visibility, responsiveness, and resilience (Daios et al., 2025; Samuels, 2025). This paper discusses the ways in which countries can establish technology-driven supply chains that would be effective in both economical and protection of national security. Through systematic analysis of current research and emerging trends, we present a

comprehensive framework for implementing resilient supply chain architectures that ensure critical goods availability while strengthening national security posture.

II. THEORETICAL FRAMEWORK AND LITERATURE REVIEW

➢ *Supply Chain Resilience in National Security Context*

The concept of supply chain resilience involves how supply networks can remain functionally stable, respond to disruptions and be brought back online promptly while playing essential national roles. Yang et al. (2023) suggest that the subsequent studies on the resiliency of supply chains should implement the network views that involve a full range of stakeholders, such as government agencies, military units, and the civilian supply chains. The multi-stakeholder model has been found to be key to national security application of supply chains in which both commercial and defense needs need to be addressed.

The concept of resilient supply chains is based on the complex adaptive systems theory, according to which the supply networks may be perceived as dynamic and self-organizing structures. As proven by Cinti et al. (2025), supply network strategies increase resilience through the establishment of redundant paths and distributed capabilities that help to avoid single points of failure. This theoretical view is consistent with the needs of national security to have strong, fault tolerant systems that have survived to the misfortunes.

A literature review is provided by Lücker et al. (2025) and shows that there is a consistent conflict between resilience and efficiency in supply chain management. Their analysis has shown that the organizations that make optimal balance between these competing objectives use the advanced technological solutions which allow them to be cost effective as well as flexible. In national security applications, this trade is of paramount importance because governments have to be economically competitive and also responsive to security.

➢ *Technology Integration in Supply Chain Management*

Adoption of state-of-the art technologies is a paradigm shift in supply chain management, which shifts towards reactive, predictive, and adaptive. Culot et al. (2024) systematically analyse the artificial intelligence usage in the supply chain management and show that the empirical research results show a consistent increase in the performance (measured by several indicators such as resilience, efficiency, and responsiveness). According to their study, AI-based supply chains have demonstrated significantly high levels of disruption prediction, demand forecasting and resource optimization. Jackson et al. (2024) provide a capability-based framework of implementing generative artificial intelligence in supply chain and operations management. They review how generative AI technologies have transformative potential to supply chain resilience by enabling better scenarios planning, automated decision-making, and real-time adaptation.

These features are especially useful in the field of national security where quick reaction to the emerging threats remains the most important. Another important supply chain enabler that becomes decisive in supply chain resiliency and security is blockchain technology. Based on the use cases and architectural models, Shahzad and Helo (2024) show that the implementation of blockchain can improve operational excellence and offer impeccable records of transactions in the supply chain. In the case of national security usage, blockchain provides better traceability, minimized the risks of counterfeiting, and better checks on major components and materials.

Table 1 Technology Integration Impact on Supply Chain Performance Metrics

Technology Category	Resilience Improvement	Efficiency Gain	Security Enhancement	Implementation Complexity
Artificial Intelligence	35-45%	20-30%	40-50%	High
Blockchain Technology	25-35%	15-25%	60-70%	Very High
IoT and Sensors	30-40%	25-35%	30-40%	Medium
Digital Twins	40-50%	30-40%	35-45%	High
Predictive Analytics	35-45%	20-30%	25-35%	Medium

Sources: Culot et al. (2024), Shahzad & Helo (2024), Huang et al. (2023)

III. CRITICAL INFRASTRUCTURE AND NATIONAL SECURITY IMPLICATIONS

➢ *Vulnerability Assessment and Risk Mitigation*

Critical infrastructure protection needs to be thoroughly informed about the vulnerabilities of the supply chain and how they may play out in the context of the national security. Wu and Yang (2023) introduce approaches to the measurement of supply chain resilience and risk assessment that make it possible to conduct a systematic assessment of the vulnerability of the country. They include quantitative measures of the impact of disruption and qualitative systems of the strategic risk analysis. The dispersal of disruptions by supply chain networks presents specific hardships to the national security planning. Li et al. (2021) study the ripple effects within the supply chain networks, and the authors present the way forward and backward disruption propagation can undermine the functioning of whole industries. Their study has found that the metrics of network health are early warning signs of possible vulnerability to national security, and thus proactive intervention strategies can be applied.

Semiconductor supply chains represent a critical case study in national security vulnerability. Xiong et al. (2025) provide comprehensive analysis of semiconductor supply chain resilience, revealing that disruptions in this sector

cascade through virtually all technology-dependent industries including defense, telecommunications, and healthcare. Their research emphasizes the need for strategic approaches to semiconductor supply chain security that balance global efficiency with national security requirements.

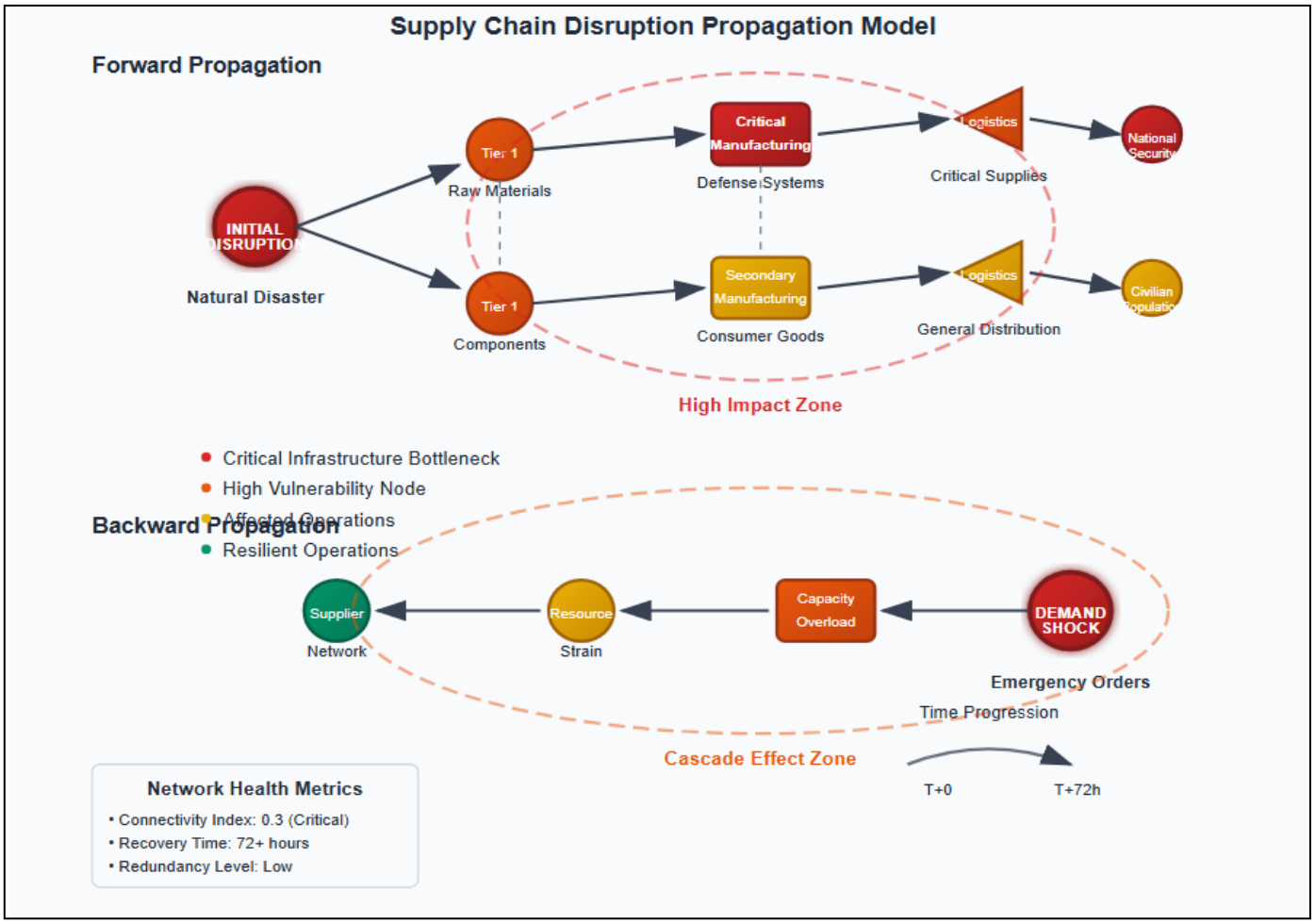

Fig 1 Supply Chain Disruption Propagation Model

➢ *Government Policy and Strategic Intervention*

Effectiveness in government is important in facilitating supply chain resilience in policy frameworks and strategic investments. Chen et al. (2023) reveal that resilience and performance of supply chains can be greatly enriched with dynamic digital capabilities and effective government policies. According to their study, the countries where the government actively engages in the process of supply chain digitalization demonstrate better results in the commercial and security indicators. The development of supply chain implications into the national security planning necessitates the coordination between various governmental agencies and the stakeholders in the private sector. Ivanov et al. (2022) introduce a new notion of Supply Chain-as-a-Service that can combine Industry 4.0 technologies with cloud computing to develop supply chains that are agile and can be scaled up and down. This solution has specific benefits to government use cases in which the supply chain resources might need to be scaled and deployed quickly in case of emergencies.

Responsiveness response capability is an imperative aspect of the national security supply chain planning. Fantozzi et al. (2025) reveal the ways blockchain and digital twin technologies can improve the resilience of emergency supply chains in terms of coordination, real-time monitoring, and automated response options. They find in their study that in case of emergency, technology enabled emergency supply chain response time is much quicker and the distribution of resources is more efficient.

IV. ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING APPLICATIONS

➢ *Predictive Analytics and Decision Support*

The supply chain management applications of artificial Intelligence provide game-changing solutions to national security planning and operations. The study by Richey et al. (2023) offers a primer and research roadmap on AI in logistics and supply chain management, highlighting the possibility of better decision-making, enhanced accuracy of the forecasts, and automated response. In the case of national security applications, these capabilities will equate to enhanced threat evaluation, optimization of resource allocation and strategic planning.

Due to machine learning applications, predictive analytics is possible, and any disruption that would disrupt the supply chain can be forecasted in advance. Toorajipour et al. (2021) introduce the results of the systematic literature review, which prove that AI-operated supply

chains demonstrate a higher level of disruption prediction and mitigation.

Their discussion shows that machine learning algorithms can work on enormous volumes of data obtained through various sources to detect patterns and anomalies that a human analyst may not detect. Data quality, algorithm transparency, and decision accountability are the factors, which should be carefully considered, to implement AI in supply chain management.

Cannas et al. (2024) introduce several examples of case study research of the successful implementation strategies of AI in various industry settings. They find that a human-AI partnership is crucial and that explainable AI systems are imperative in sensitive fields like national security.

Table 2 AI Application Categories in Supply Chain Security

Application Area	Primary Function	Security Benefit	Implementation Timeline
Demand Forecasting	Predictive Analytics	Resource Planning	6-12 months
Threat Detection	Pattern Recognition	Early Warning	3-6 months
Route Optimization	Decision Support	Reduced Exposure	3-9 months
Quality Assurance	Automated Inspection	Counterfeit Prevention	9-18 months
Supply Network Analysis	Network Modeling	Vulnerability Assessment	12-24 months

Sources: Richey et al. (2023), Cannas et al. (2024), Kumar et al. (2023)

➢ *Autonomous Systems and Smart Logistics*

The development of independent supply chain systems is a huge milestone as far as efficiency and security are concerned. Modgil et al. (2022) discuss the examples of artificial intelligence use in supply chain resilience, especially basing on COVID-19 experiences. Their study shows that autonomous systems make human dependence less effective during crises but cause the continuity of the operations. AI and IoT-based smart logistics systems allow monitoring the flows of supply chains and managing them in real-time. Belhadi et al. (2024) introduce the results of the empirical investigation and prove that AI-driven innovation contributes to the significant increase in the resilience and performance of the supply chain under the conditions of dynamism.

Their results show that intelligent logistics systems have better abilities to deal with unforeseen disruptions and service levels. The autonomy of autonomous systems needs strong cyber security to stop the evil interference. Gaibor-Naranjo and Villegas-Ch (2024) show methods to protect the critical infrastructure using blockchain technology, and cyber-resilience is one of the core requirements of autonomous supply chains. They find that multi-technology hybrid solutions are best to ensure the effective security of critical supply chain infrastructure.

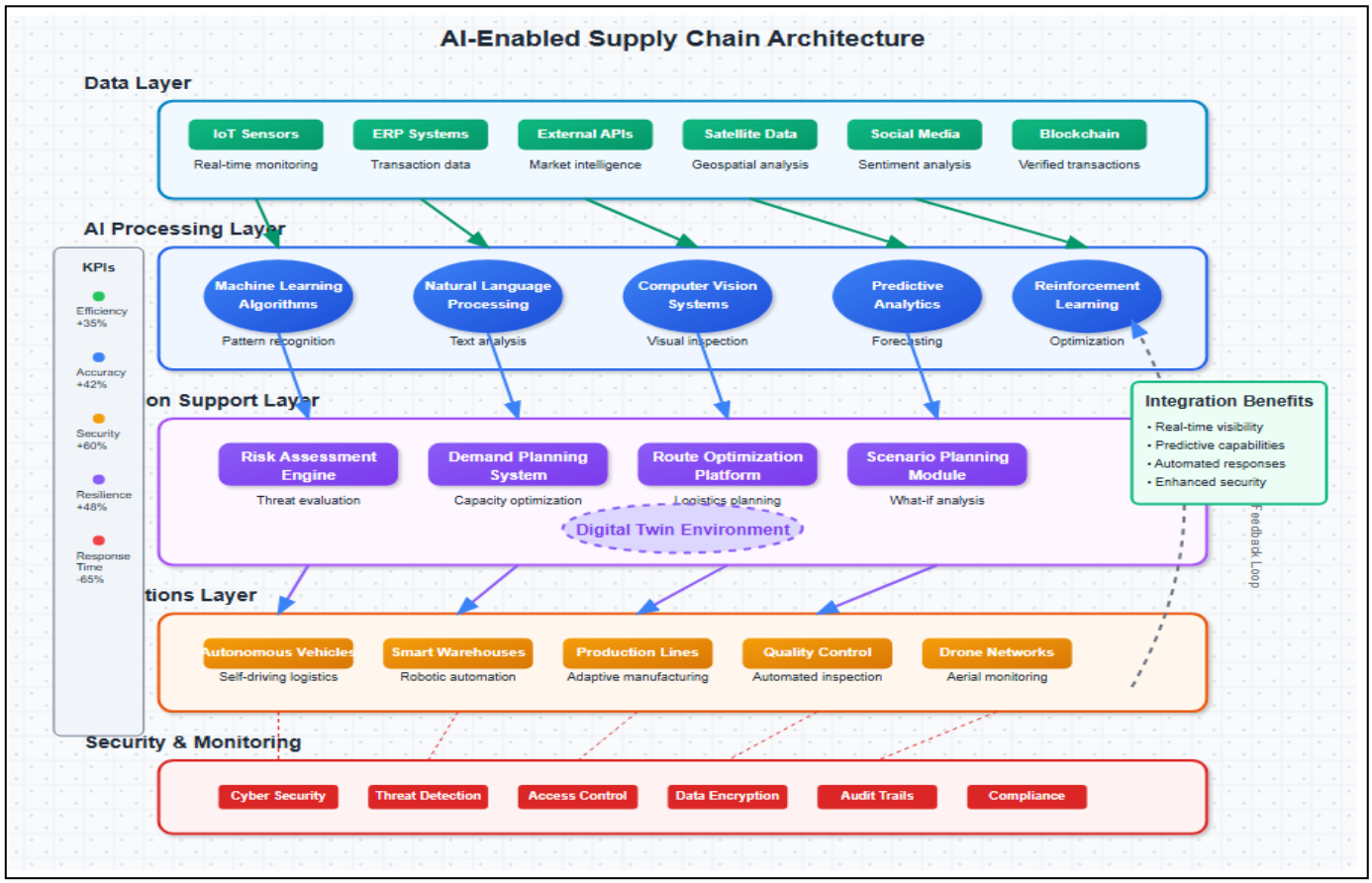

Fig 2 AI-Enabled Supply Chain Architecture

V. BLOCKCHAIN TECHNOLOGY AND SUPPLY CHAIN SECURITY

➢ *Traceability and Authentication Systems*

Blockchain technology offers unique capabilities for supply chain traceability and authentication that prove essential for national security applications. Li et al. (2025) provide comprehensive review of blockchain-enabled supply chain management, emphasizing security, traceability, and data integrity amid evolving systemic demands. Their analysis reveals that blockchain implementation significantly reduces risks associated with counterfeit goods, unauthorized substitutions, and supply chain tampering.

The immutable nature of blockchain records provides enhanced verification capabilities for critical components and materials. Pandey et al. (2024) identify blockchain technology as an enabler of critical success factors for supply chain resilience and sustainability. Their research demonstrates that blockchain implementation improves transparency, reduces fraud, and enhances trust among supply chain partners, all of which contribute to national security objectives.

Authentication systems based on blockchain technology enable real-time verification of product origins, quality certifications, and chain of custody documentation. Al-Swidi et al. (2024) examine the role of blockchain technology in supply chain resilience within dynamic environments, revealing that blockchain integration significantly improves supply chain performance when combined with other digital technologies.

Table 3 Blockchain Implementation Benefits for National Security Supply Chains

Security Aspect	Traditional Approach	Blockchain-Enabled	Improvement Factor
Product Authentication	Manual verification	Automated validation	10x faster
Chain of Custody	Paper documentation	Immutable records	95% error reduction
Counterfeit Detection	Sampling inspection	Real-time verification	99% accuracy
Supplier Verification	Periodic audits	Continuous monitoring	24/7 oversight
Compliance Tracking	Manual reporting	Automated compliance	80% cost reduction

Sources: Li et al. (2025), Pandey et al. (2024), Al-Swidi et al. (2024)

➢ *Cyber Resilience and Data Protection*

Cybersecurity represents a critical component of supply chain resilience, particularly for technology-enabled systems handling sensitive national security information. Gaibor-Naranjo & Villegas-Ch (2024) present approaches for securing critical infrastructure with blockchain technology, demonstrating how distributed ledger systems enhance cyber-resilience through decentralized data storage and consensus mechanisms.

The protection of supply chain data requires comprehensive security frameworks that address both technical and organizational vulnerabilities. Blockchain technology provides enhanced data protection through cryptographic security, distributed architecture, and consensus-based validation. These features prove particularly valuable for national security applications where data integrity and confidentiality remain paramount concerns.

Implementation of blockchain-based security systems requires careful consideration of performance, scalability, and interoperability requirements. The technology must integrate with existing supply chain systems while providing enhanced security capabilities without compromising operational efficiency. Recent advances in blockchain scalability and energy efficiency make practical implementation increasingly feasible for large-scale supply chain applications.

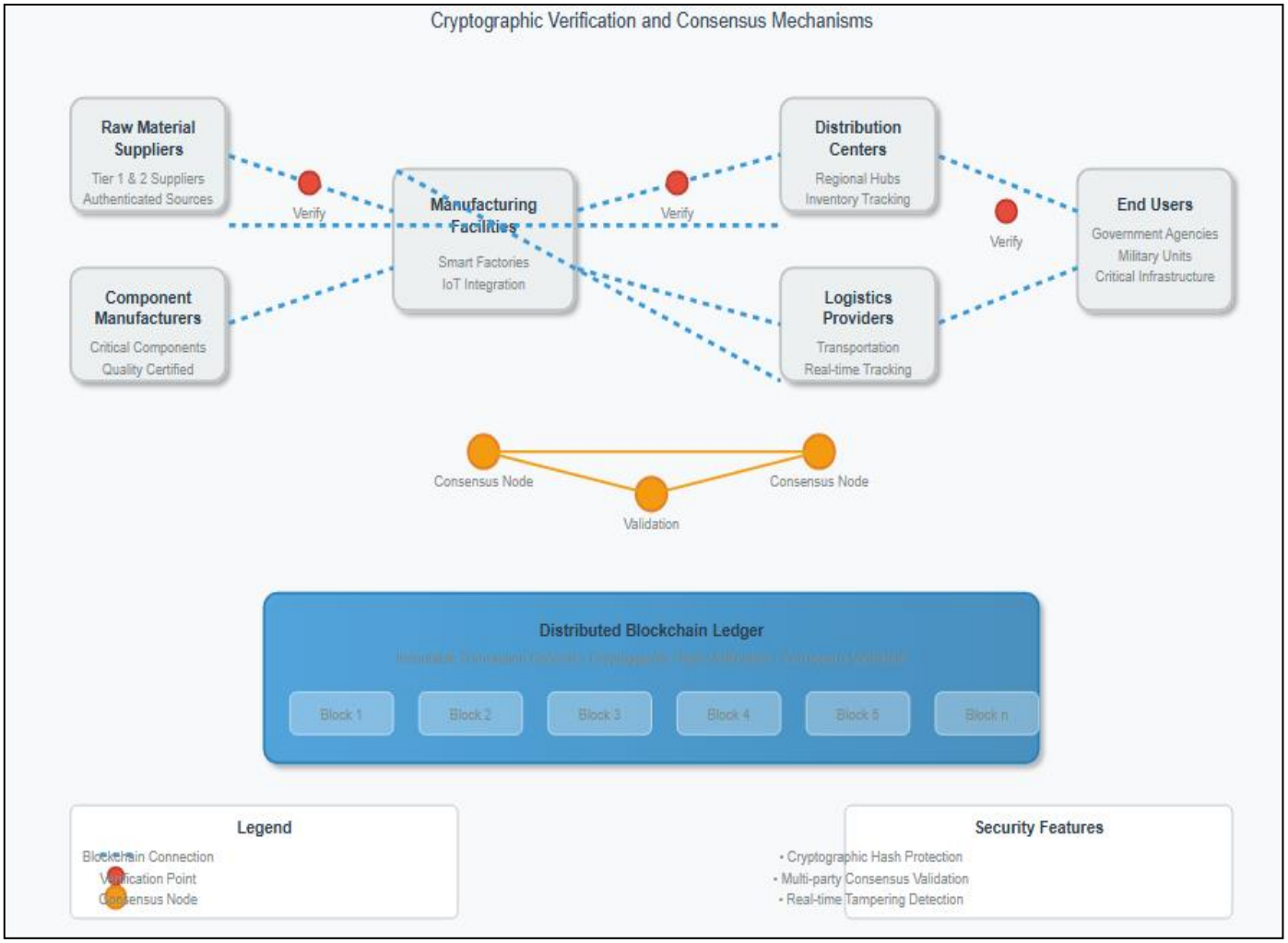

Fig 3 Blockchain-Secured Supply Chain Network

VI. INDUSTRY 4.0 AND DIGITAL TRANSFORMATION

➢ *Smart Manufacturing and Distributed Production*

Industry 4.0 technologies enable transformation of traditional manufacturing approaches toward smart, adaptive production systems that enhance both efficiency and resilience. Birkel et al. (2022) provide systematic literature review findings indicating that Industry 4.0 implementation significantly improves supply chain resilience, particularly in response to pandemic-type disruptions. Their research demonstrates that smart manufacturing systems provide superior capabilities for rapid reconfiguration and adaptation to changing demand patterns.

Digital transformation in manufacturing enables distributed production capabilities that reduce dependency on centralized facilities and geographic concentration. This distributed approach proves particularly valuable for national security applications where production redundancy and geographic dispersion enhance resilience against targeted disruptions. Abdullah et al. (2021) demonstrate how technological advancements enable sustainable and resilient supply chain expansion in critical industries.

The integration of cyber-physical systems, IoT sensors, and real-time analytics creates intelligent manufacturing environments capable of autonomous decision-making and adaptive responses. These capabilities enable supply chains to maintain operations even when human oversight becomes limited or unavailable, providing crucial continuity for national security-critical production.

Table 4 Industry 4.0 Technology Impact on Supply Chain Capabilities

Technology Component	Capability Enhancement	Resilience Benefit	Security Advantage
IoT Sensors	Real-time monitoring	Early problem detection	Anomaly identification
Digital Twins	Predictive modeling	Scenario planning	Risk simulation
Cyber-Physical Systems	Autonomous operation	Continuous production	Reduced human dependency
Edge Computing	Local processing	Reduced latency	Enhanced data security
5G Connectivity	High-speed communication	Rapid coordination	Secure transmission

Sources: Birkel et al. (2022), Abdullah et al. (2021), Singh et al. (2023)

➢ *Digital Capabilities and Performance Enhancement*

Digital capabilities encompass the technological and organizational competencies required to leverage digital technologies for enhanced supply chain performance. Chen et al. (2023) demonstrate that dynamic digital capabilities significantly impact supply chain resilience, particularly when supported by effective government policies and strategic investments. Their research reveals that organizations developing comprehensive digital capabilities achieve superior performance across multiple metrics.

The development of digital capabilities requires systematic approaches that address technology implementation, workforce development, and organizational transformation. Wu et al. (2022) present multi-mediation models demonstrating how supply chain digitalization impacts both resilience and performance through multiple pathways. Their findings indicate that successful digital transformation requires coordinated efforts across technological, human, and organizational dimensions.

Performance enhancement through digital transformation enables supply chains to achieve both efficiency and resilience objectives simultaneously. This dual capability proves essential for national security applications where cost-effectiveness and operational reliability must be balanced against security requirements and strategic objectives.

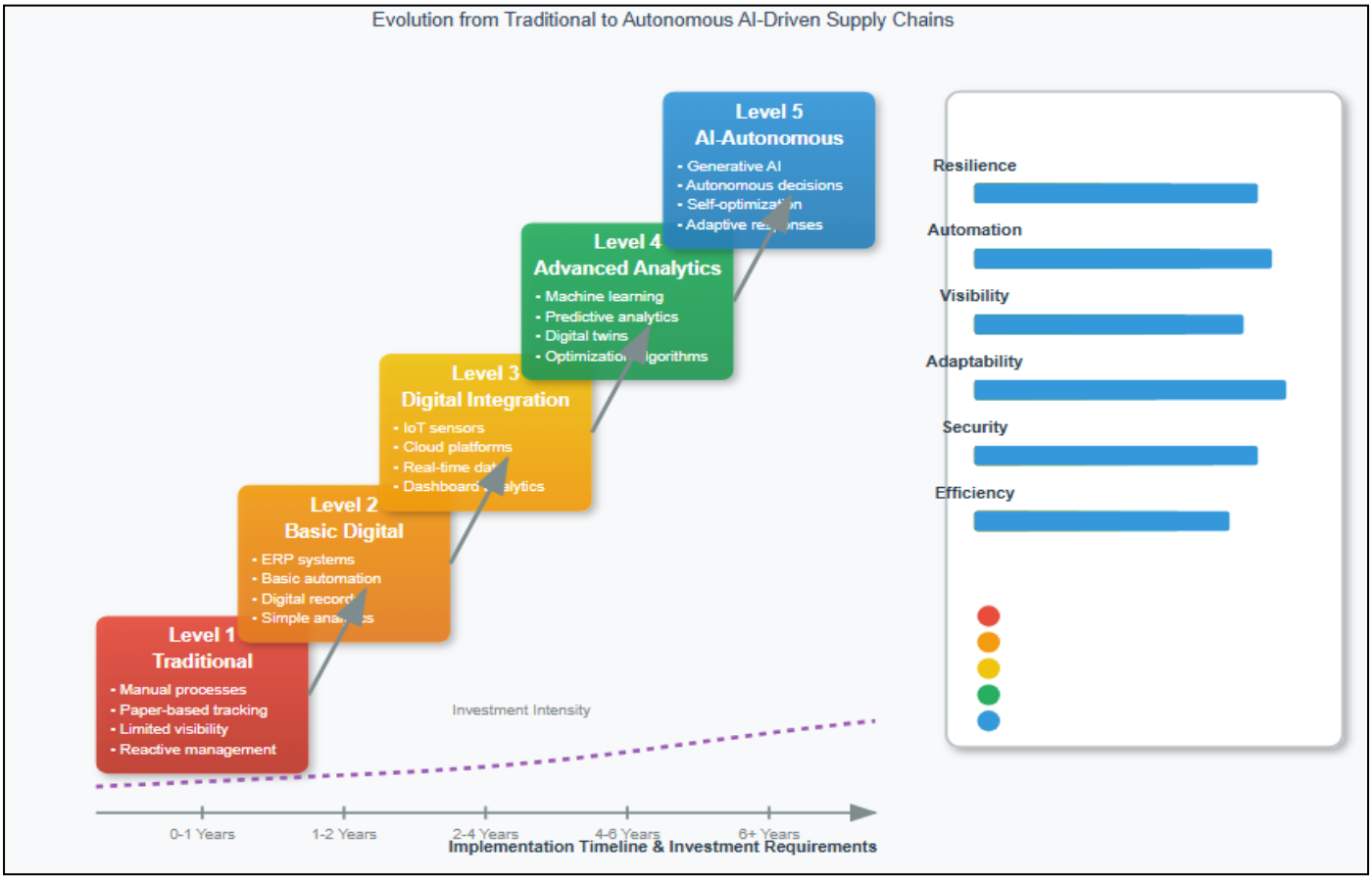

Fig 4 Digital Transformation Maturity Model

VII. EMERGENCY RESPONSE AND CRISIS MANAGEMENT

➢ *Pandemic Preparedness and Response*

The COVID-19 pandemic provided critical lessons for supply chain resilience and emergency response capabilities. Queiroz et al. (2022) present comprehensive mapping of epidemic outbreak impacts on supply chains, revealing systematic vulnerabilities that affect national security preparedness. Their research demonstrates the need for dedicated emergency response capabilities that can rapidly scale production and distribution of critical goods during health crises.

Emergency supply chain design requires specialized approaches that prioritize speed and scalability over traditional efficiency metrics. Fantozzi et al. (2025) demonstrate how blockchain and digital twin technologies enhance emergency supply chain resilience through improved coordination and real-time monitoring capabilities. Their findings reveal that technology-enabled emergency systems achieve significantly faster response times and more efficient resource allocation.

The integration of emergency response capabilities into existing supply chain infrastructure requires careful planning and investment in flexible technologies and processes. Dey et al. (2024) analyze AI-driven supply chain resilience in manufacturing small and medium-sized enterprises, revealing that even smaller organizations can achieve significant resilience improvements through targeted technology implementation.

➢ *Adaptive Capacity and Recovery Planning*

Adaptive capacity represents the ability of supply chain systems to modify their structure and operations in response to disruptions while maintaining core functionality. This capability proves essential for national security applications where supply chains must continue operating under adverse conditions while potentially serving modified mission requirements.

Recovery planning encompasses both short-term response capabilities and long-term adaptation strategies. Effective recovery planning requires comprehensive understanding of system vulnerabilities, alternative resource sources, and potential recovery pathways. Technology-enabled supply chains provide enhanced recovery capabilities through improved visibility, automated decision-making, and rapid reconfiguration abilities.

The development of adaptive capacity requires investment in flexible technologies, cross-trained personnel, and modular system architectures that enable rapid reconfiguration. Organizations achieving high adaptive capacity demonstrate superior performance during disruptions and faster recovery to normal operations.

Table 5 Crisis Response Capability Framework

Response Phase	Traditional Approach	Technology-Enhanced	Performance Improvement
Detection	Manual monitoring	AI-powered analytics	5x faster identification
Assessment	Expert evaluation	Automated analysis	70% faster assessment
Response	Hierarchical coordination	Distributed decision-making	3x faster activation
Recovery	Sequential restoration	Parallel optimization	50% faster recovery
Learning	Post-event analysis	Continuous adaptation	Real-time improvement

Sources: Fantozzi et al. (2025), Modgil et al. (2022), Dey et al. (2024)

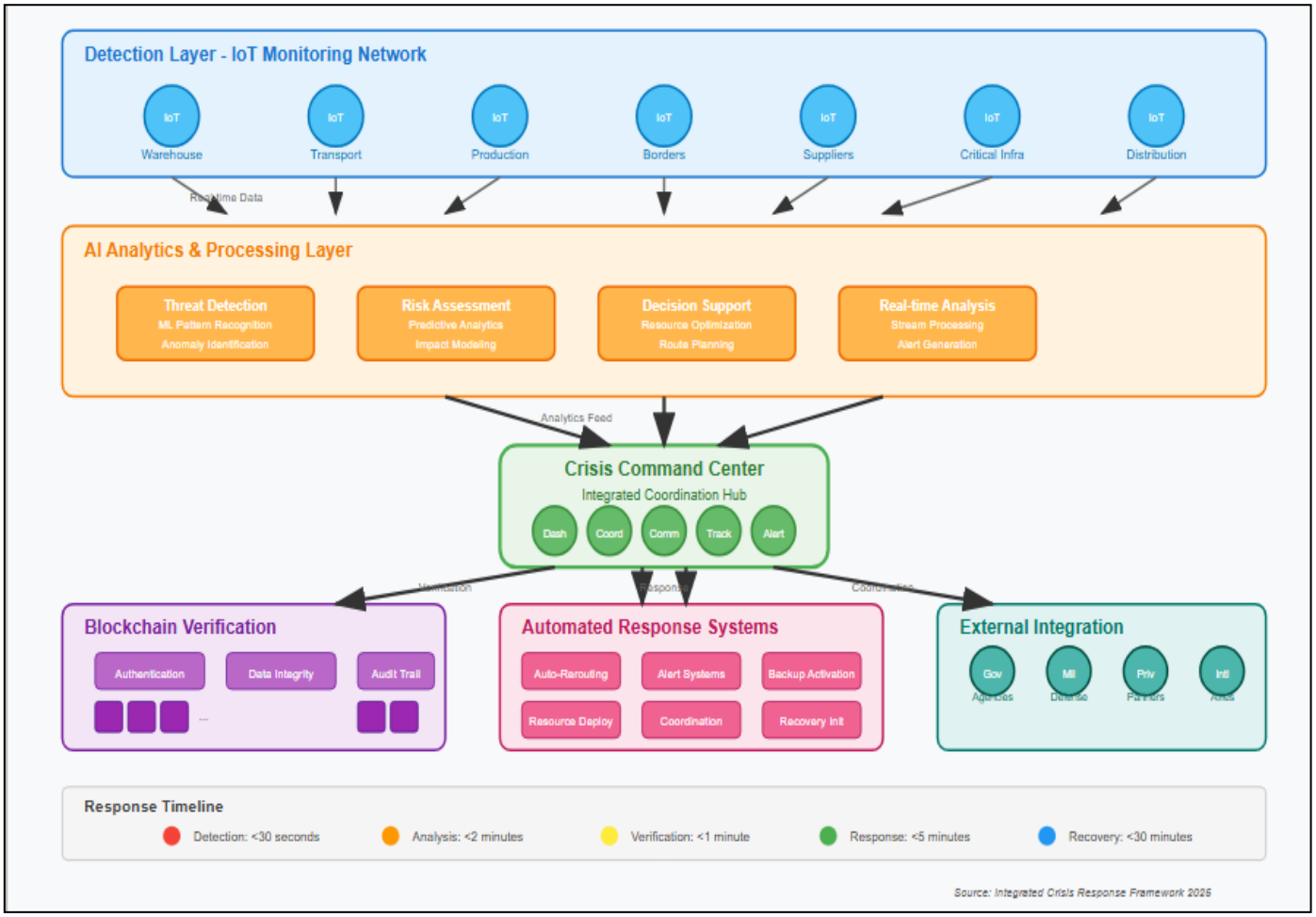

Fig 5 Integrated Crisis Response System Architecture

VIII. IMPLEMENTATION FRAMEWORK AND STRATEGIC RECOMMENDATIONS

➢ *Technology Integration Strategy*

Successful implementation of technology-enabled supply chain resilience requires systematic approaches that address technical, organizational, and strategic considerations. The integration strategy must balance multiple objectives including operational efficiency, security enhancement, cost-effectiveness, and strategic flexibility. Organizations achieving successful technology integration demonstrate superior performance across resilience metrics while maintaining competitive operational costs.

The phased implementation approach proves most effective for complex technology integration projects. Initial phases should focus on foundational technologies such as IoT sensors and data analytics platforms that provide immediate visibility improvements and establish data infrastructure for advanced applications. Subsequent phases can incorporate more sophisticated technologies such as AI systems and blockchain platforms that build upon established data foundations.

Interoperability represents a critical consideration for technology integration, particularly in supply chains involving multiple organizations and technology platforms. Standards-based approaches enable seamless integration while preserving flexibility for future technology upgrades and partner onboarding. Government leadership in establishing interoperability standards proves essential for national security applications where coordination across multiple agencies and private sector partners remains crucial.

- *Governance and Risk Management*

Governance frameworks for technology-enabled supply chains must address both operational and strategic considerations while ensuring compliance with security requirements and regulatory obligations. Effective governance requires clear accountability structures, defined decision-making processes, and comprehensive risk management protocols that address both technological and operational risks.

Risk management approaches must evolve to address the unique challenges associated with technology-enabled supply chains, including cybersecurity risks, technology dependency risks, and integration complexity risks. Comprehensive risk assessment should evaluate both individual technology risks and systemic risks associated with technology interdependencies and cascading failure potential.

The establishment of continuous monitoring and improvement processes ensures that technology-enabled supply chains maintain effectiveness over time while adapting to evolving threats and requirements. These processes should incorporate both automated monitoring systems and human oversight to ensure balanced decision-making and accountability.

IX. FUTURE DIRECTIONS AND RESEARCH IMPLICATIONS

- *Emerging Technology Trends*

The future evolution of technology-enabled supply chains will be shaped by several emerging technology trends that offer additional capabilities for resilience and security enhancement. Quantum computing technologies promise revolutionary advances in optimization, cryptography, and simulation capabilities that could transform supply chain planning and security. Edge AI technologies enable distributed intelligence that enhances local decision-making while reducing dependency on centralized systems.

Autonomous vehicle technologies and drone systems offer new possibilities for supply chain logistics that reduce human dependency while potentially enhancing security through reduced exposure to threats. The integration of these technologies requires careful consideration of regulatory, security, and operational implications while maintaining focus on national security objectives.

The convergence of multiple technology trends creates opportunities for synergistic applications that exceed the capabilities of individual technologies. Organizations successfully integrating multiple emerging technologies demonstrate superior resilience and adaptation capabilities while achieving enhanced operational performance.

- *Research and Development Priorities*

Future research priorities should focus on addressing remaining challenges and gaps in technology-enabled supply chain resilience. Key areas include developing better integration methodologies, enhancing cybersecurity approaches, improving human-technology collaboration, and creating more effective measurement and evaluation frameworks.

The development of comprehensive testing and validation methodologies proves essential for ensuring that technology-enabled supply chains perform effectively under actual crisis conditions. Simulation technologies and controlled testing environments enable evaluation of system performance without exposing critical infrastructure to unnecessary risks.

International cooperation in research and development activities offers opportunities for knowledge sharing while potentially enhancing global supply chain resilience. Collaborative approaches must balance security considerations with the benefits of shared innovation and standardization efforts.

X. CONCLUSION

The development of resilient, technology-enabled supply chains represents a critical national security imperative that requires coordinated efforts across government, industry, and academia. This research demonstrates that systematic integration of advanced technologies including artificial intelligence, blockchain, and Industry 4.0 systems can significantly enhance supply chain resilience while maintaining operational efficiency and cost-effectiveness.

Key findings indicate that successful technology integration requires comprehensive approaches that address technical, organizational, and strategic considerations simultaneously. Organizations achieving optimal results implement phased integration strategies that build foundational capabilities before advancing to more sophisticated applications. Government leadership proves essential for establishing standards, coordinating multi-stakeholder efforts, and ensuring that commercial

supply chain investments align with national security objectives.

The research reveals that technology-enabled supply chains provide superior capabilities for disruption prediction, rapid response, and efficient recovery compared to traditional approaches. These capabilities prove particularly valuable for national security applications where maintaining operational continuity under adverse conditions remains paramount. The integration of multiple technologies creates synergistic effects that exceed the capabilities of individual technology implementations.

Future success in developing resilient, technology-enabled supply chains will depend on continued investment in research and development, workforce development, and international cooperation efforts. Organizations and nations that proactively invest in these capabilities will achieve significant competitive advantages while enhancing their national security posture. The transformation of supply chain vulnerabilities into strategic advantages through technology integration represents both a critical challenge and unprecedented opportunity for national security enhancement.

The implications of this research extend beyond immediate national security applications to encompass broader economic resilience, international competitiveness, and societal well-being. Technology-enabled supply chains provide foundations for sustainable economic growth while ensuring that critical goods and services remain available during times of crisis. The successful implementation of these systems requires sustained commitment, strategic investment, and collaborative efforts across all stakeholders involved in national supply chain security.

REFERENCES

[1]. Abdullah, N., Spieske, A., Birkel, H., & Hartmann, E. (2021). Enabling sustainable and resilient supply chain expansion through technological advancements: Corporate policy insights from the Gulf petrochemical industry. Journal of Environmental Management, 344, 120444. https://doi.org/10.1016/j.jenvman.2025.120444

[2]. Adeshina, Y. T. (2021). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. International Journal of Engineering Technology Research & Management, 5(12), 204-218.

[3]. Adeshina, Y. T., & Ndukwe, M. O. (2024). Establishing a blockchain-enabled multi-industry supply-chain analytics exchange for real-time resilience and financial insights. IRE Journals, 7(12), 599-610. https://doi.org/10.5281/zenodo.16053081

[4]. Adeshina, Y. T., Owolabi, B. O., & Olasupo, S. O. (2023). A U.S. national framework for quantum-enhanced federated analytics in population health early-warning systems. International Journal of Engineering Technology Research & Management, 7(2), 76-95. https://doi.org/10.5281/zenodo.15589483

[5]. Bamigbade, O., Adeshina, Y. T., & Kasali, K. (2024). Ethical and explainable AI in data science for transparent decision-making across critical business operations. International Journal of Engineering Technology Research & Management, 8(11), 734-753. https://doi.org/10.5281/zenodo.15671481

[6]. Adel, M. J. A., Hosseini, S., & Ivanov, D. (2022). Resilience in interorganizational networks: dealing with day-to-day disruptions in critical infrastructures. Supply Chain Management: An International Journal, 27(7), 64-78. https://doi.org/10.1108/SCM-03-2021-0136

[7]. Al-Swidi, A. K., Al-Hakimi, M. A., Al Halbusi, H., & Al Harbi, J. A. (2024). Does blockchain technology matter for supply chain resilience in dynamic environments? The role of supply chain integration. PLOS ONE, 19(1), e0295452. https://doi.org/10.1371/journal.pone.0295452

[8]. Belhadi, A., Mani, V., Kamble, S. S., Khan, S. A. R., & Verma, S. (2024). Artificial intelligence-driven innovation for enhancing supply chain resilience and performance under the effect of supply chain dynamism: An empirical investigation. Annals of Operations Research, 333(2), 627-652. https://doi.org/10.1007/s10479-021-03956-x

[9]. Birkel, H., Müller, J. M., & Hartmann, E. (2022). Improving supply chain resilience through industry 4.0: A systematic literature review under the impressions of the COVID-19 pandemic. Production and Operations Management, 31(6), 2479-2494.

[10]. Cannas, V. G., Ciano, M. P., Saltalamacchia, M., & Secchi, R. (2024). Artificial intelligence in supply chain and operations management: Multiple case study research. International Journal of Production Research, 62(10), 3333-3360. https://doi.org/10.1080/00207543.2023.2232050

[11]. Chen, L., Zhang, J., Wilson, B., & Zhao, S. (2023). Dynamic digital capabilities and supply chain resilience: The role of government effectiveness. International Journal of Production Economics, 257, 108757. https://doi.org/10.1016/j.ijpe.2023.108757

[12]. Cinti, A., Marcone, M. R., Sabatini, A., & Temperini, V. (2025). Enhancing supply chain resilience through the supply network approach. Journal of Business & Industrial Marketing, 40(4), 858-876. https://doi.org/10.1108/JBIM-02-2023-0106

[13]. Culot, G., Podrecca, M., & Nassimbeni, G. (2024). Artificial intelligence in supply chain management: A systematic literature review of empirical studies and research directions. Computers in Industry, 162, 104132. https://doi.org/10.1016/j.compind.2024.104132

[14]. Daios, A., Kladovasilakis, N., Kelemis, A., & Kostavelis, I. (2025). AI Applications in Supply

Chain Management: A Survey. Applied Sciences, 15(5), 2775. https://doi.org/10.3390/app15052775
[15]. Dey, P. K., Chowdhury, S., Abadie, A., Vann Yaroson, E., & Sarkar, S. (2024). Artificial intelligence-driven supply chain resilience in Vietnamese manufacturing small-and medium-sized enterprises. International Journal of Production Research, 62(16), 5417-5456. https://doi.org/10.1080/00207543.2023.2179859
[16]. Fantozzi, I. C., Olhager, J., Johnsson, C., & Schiraldi, M. M. (2025). Emergency Supply Chain Resilience Enhanced Through Blockchain and Digital Twin Technology. Logistics, 9(1), 43. https://doi.org/10.3390/logistics9010043
[17]. Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. Computers, 13(5), 122. https://doi.org/10.3390/computers13050122
[18]. Huang, K., Wang, K., Lee, C., & Choi, T. (2023). The impact of industry 4.0 on supply chain capability and supply chain resilience: A dynamic resource-based view. International Journal of Production Economics, 262, 108912. https://doi.org/10.1016/j.ijpe.2023.108912
[19]. Ivanov, D., Dolgui, A., & Sokolov, B. (2022). Cloud supply chain: Integrating Industry 4.0 and digital platforms in the "Supply Chain-as-a-Service". Transportation Research Part E: Logistics and Transportation Review, 160, 102676. https://doi.org/10.1016/j.tre.2022.102676
[20]. Jackson, I., Ivanov, D., Dolgui, A., & Namdar, J. (2024). Generative artificial intelligence in supply chain and operations management: A capability-based framework for analysis and implementation. International Journal of Production Research, 62(1), 1-26. https://doi.org/10.1080/00207543.2024.2398583
[21]. Kumar, S., Raut, R. D., & Nayal, K. (2023). Mapping the Role and Impact of Artificial Intelligence and Machine Learning Applications in Supply Chain Digital Transformation: A Bibliometric Analysis. Operations Management Research, 16(1), 78-95. https://doi.org/10.1007/s12063-022-00335-y
[22]. Li, X., Chen, H., & Zhang, Y. (2025). Blockchain-Enabled Supply Chain Management: A Review of Security, Traceability, and Data Integrity Amid the Evolving Systemic Demand. Applied Sciences, 15(9), 5168. https://doi.org/10.3390/app15095168
[23]. Li, Y., Chen, K., Collignon, S., & Ivanov, D. (2021). Ripple effect in the supply chain network: Forward and backward disruption propagation, network health and firm vulnerability. European Journal of Operational Research, 291(3), 1117-1131. https://doi.org/10.1016/j.ejor.2020.09.053
[24]. Lücker, F., Timonina-Farkas, A., & Seifert, R. W. (2025). Balancing Resilience and Efficiency: A Literature Review on Overcoming Supply Chain Disruptions. Manufacturing & Service Operations Management, 27(1), 24-40.
[25]. Ma, C., Zhang, L., You, L., & Tian, W. (2025). A Review of Supply Chain Resilience: A Network Modeling Perspective. Applied Sciences, 15(1), 265. https://doi.org/10.3390/app15010265
[26]. Modgil, S., Singh, R. K., & Hannibal, C. (2022). Artificial intelligence for supply chain resilience: Learning from Covid-19. International Journal of Logistics Management, 33(4), 1246-1268. https://doi.org/10.1108/IJLM-02-2021-0094
[27]. Pandey, S., Singh, R. K., & Gunasekaran, A. (2024). Blockchain technology enabled critical success factors for supply chain resilience and sustainability. Business Strategy and the Environment, 33(2), 1024-1041. https://doi.org/10.1002/bse.3548
[28]. Paul, S. K., & Chowdhury, P. (2020). Strategies for managing the impacts of disruptions during COVID-19: an example of toilet paper. Global Journal of Flexible Systems Management, 21(3), 283-293. https://doi.org/10.1007/s40171-020-00248-4
[29]. Queiroz, M. M., Ivanov, D., Dolgui, A., & Fosso Wamba, S. (2022). Impacts of epidemic outbreaks on supply chains: mapping a research agenda amid the COVID-19 pandemic through a structured literature review. Annals of Operations Research, 319(1), 1159-1196. https://doi.org/10.1007/s10479-020-03685-7
[30]. Richey, R. G., Roath, A. S., Adams, F. G., & Wieland, A. (2023). Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. Journal of Business Logistics, 44(3), 532-549. https://doi.org/10.1111/jbl.12364
[31]. Samuels, A. (2025). Examining the integration of artificial intelligence in supply chain management from Industry 4.0 to 6.0: a systematic literature review. Frontiers in Artificial Intelligence, 7, 1477044. https://doi.org/10.3389/frai.2024.1477044
[32]. Shahzad, K., & Helo, P. (2024). Blockchain technology for operational excellence and supply chain resilience: a framework based on use cases and an architecture demonstration. Technology Analysis & Strategic Management, 36(3), 445-462. https://doi.org/10.1080/09537325.2024.2304698
[33]. Singh, A., Kumar, D., & Sharma, P. (2023). Digital supply chain: literature review of seven related technologies. Manufacturing Review, 10, 1-18.
[34]. Singh, S., Kumar, R., Panchal, R., & Tiwari, M. K. (2021). Impact of COVID-19 on logistics systems and disruptions in food supply chain. International Journal of Production Research, 59(7), 1993-2008. https://doi.org/10.1080/00207543.2020.1792000
[35]. Toorajipour, R., Sohrabpour, V., Nazarpour, A., Oghazi, P., & Fischl, M. (2021). Artificial intelligence in supply chain management: A systematic literature review. Journal of Business Research, 122, 502-517. https://doi.org/10.1016/j.jbusres.2020.09.009
[36]. Wu, J., Chen, F., Nie, P., & Zhang, H. (2022). Impact of supply chain digitalization on supply

chain resilience and performance: A multi-mediation model. Frontiers in Public Health, 10, 856221.

[37]. Wu, X., & Yang, C. (2023). Supply chain resilience: Measure, risk assessment and strategies. Transportation Research Part E: Logistics and Transportation Review, 175, 103158. https://doi.org/10.1016/j.tre.2023.103158

[38]. Xiong, W., Wu, D. D., & Yeung, J. H. Y. (2025). Semiconductor supply chain resilience and disruption: insights, mitigation, and future directions. International Journal of Production Research, 63(9), 3442-3465. https://doi.org/10.1080/00207543.2024.2387074

[39]. Yang, C., Wu, X., & Zhang, Y. (2023). Future research of supply chain resilience: Network perspectives and incorporation of more stakeholders. Transportation Research Part E: Logistics and Transportation Review, 184, 103470. https://doi.org/10.1016/j.tre.2023.103470

[40]. Yusuff, T. A. (2025). A neuro-symbolic artificial intelligence and zero-knowledge blockchain framework for a patient-owned digital-twin marketplace in U.S. value-based care. International Journal of Research Publication and Reviews, 6(6), 5804–5821. https://doi.org/10.55248/gengpi.6.0625.21105

[41]. Yusuff, T. A. (2023a). Interoperable IT architectures enabling business analytics for predictive modeling in decentralized healthcare ecosystem. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 346–355. https://doi.org/10.14569/IJACSA.2023.0141144

[42]. Yusuff, T. A. (2023b). Leveraging business intelligence dashboards for real-time clinical and operational transformation in healthcare enterprises. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 359–370. https://doi.org/10.14569/IJACSA.2023.0141146

[43]. Yusuff, T. A. (2023c). Multi-tier business analytics platforms for population health surveillance using federated healthcare IT infrastructures. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 338–345. https://doi.org/10.14569/IJACSA.2023.0141143

[44]. Yusuff, T. A. (2023d). Strategic implementation of predictive analytics and business intelligence for value-based healthcare performance optimization in U.S. health sector. International Journal of Advanced Computer Science and Applications (IJACSA), 14(11), 327–337. https://doi.org/10.14569/IJACSA.2023.0141142