AJEMA GLOBAL RESEARCH NETWORK

AMERICAN Journal of Engineering, Mechanics and Architecture
Volume 1, Issue 10, 2023 ISSN (E): 2993-2637

An AI-Driven Optimization and Risk Mitigation Framework to Strengthen U.S. Supply Chain Resilience and National Economic Security

Babul Sarker*[1], Kamana Parvej Mishu[2], Mohammad Tahmid Ahmed[3], Nadira Kulsum Papri[4], Apurbaa Sarker[5], Md Yousuf Ahmad[6]

[1]*College of Graduate and Professional Studies, Master of Science in Business Analytics (MSBAN), Trine University, 1 University Avenue, Angola, IN-46703, USA*

[2]*College of Graduate and Professional Studies, Master of Science in engineering management, Trine University, 1 University Avenue, Angola, IN 46703*

[3]*College of Graduate and Professional Studies, Master of Science in Business Analytics, Trine University, 1 University Avenue, Angola, IN-46703, USA*

[4]*Graduate Information Technology/Graduate (M.S), Master of Science in Information Technology, University of the Cumberlands, 6178 College Station Drive, Williamsburg, KY 40769, USA*

[5]*Graduate Information Technology/Graduate (M.S), Master of Science in Information Technology University name: University of the Cumberlands, 6178 College Station Drive Williamsburg, KY 40769, USA*

[6]*College of Graduate and Professional Studies, Master of Science in Business Analytics (MSBAN), Trine University, 1 University Avenue, Angola, IN-46703, USA*

**Email: bsarker22@my.trine.edu*

Abstract: The COVID-19 pandemic, geopolitical tensions, and escalating trade conflicts have exposed critical vulnerabilities in U.S. supply chains, threatening national economic security and industrial competitiveness. This paper develops the Strategic AI Supply Chain Optimization and Resilience (SASCOR) framework, an integrated approach that leverages artificial intelligence to enhance supply chain visibility, predictive capacity, and adaptive response mechanisms. Drawing from recent advances in machine learning for demand forecasting, predictive analytics for logistics optimization, and AI-driven risk detection, this study presents a comprehensive governance structure for securing critical supply networks. The framework addresses four critical dimensions: real-time visibility enhancement, predictive risk mitigation, dynamic optimization algorithms, and collaborative ecosystem governance. By synthesizing insights from cross-industry implementations including last-mile delivery optimization, manufacturing ERP integration, and cybersecurity threat detection this research provides actionable strategies for project managers and policymakers to fortify U.S. supply chain infrastructure against systemic disruptions while maintaining competitive advantage in global markets.

Keywords: Supply Chain Resilience, AI Optimization, National Economic Security, Risk Mitigation, Predictive Logistics, Supply Chain Governance

Introduction

The integrity of U.S. supply chains has emerged as a critical determinant of national economic security, with recent global disruptions underscoring the vulnerability of interconnected industrial networks. The confluence of pandemic-induced shortages, semiconductor supply constraints, and geopolitical trade restrictions has revealed structural fragilities in legacy supply chain architectures that rely on static forecasting and reactive risk management. These disruptions have cascaded

across sectors, from automotive manufacturing stalled by chip shortages to healthcare systems strained by medical supply bottlenecks, demonstrating that supply chain resilience is no longer merely an operational concern but a strategic national imperative.

Artificial intelligence presents transformative potential for addressing these vulnerabilities through predictive analytics, dynamic optimization, and real-time visibility enhancement. The deployment of machine learning models for demand forecasting, route optimization, and supplier risk assessment offers capabilities far exceeding traditional supply chain management approaches. However, the integration of AI into supply chain operations introduces novel complexities, including algorithmic dependencies, data security vulnerabilities, and the need for cross-organizational governance frameworks that transcend traditional enterprise boundaries.

The economic security implications of supply chain fragility extend beyond individual enterprises to encompass national competitiveness and strategic autonomy. The concentration of critical manufacturing capabilities in geopolitically sensitive regions, coupled with just-in-time inventory practices optimized for efficiency rather than resilience, has created systemic risks that threaten industrial continuity .Addressing these challenges requires governance frameworks that balance optimization efficiency with redundancy engineering, ensuring that AI-driven enhancements do not inadvertently concentrate risk or create single points of failure .

Recent scholarship has illuminated the potential for AI to enhance supply chain resilience through diverse mechanisms. Convolutional neural networks combined with long short-term memory (LSTM) architectures have demonstrated superior performance in revenue forecasting and demand prediction, enabling more responsive inventory management. Similarly, the integration of AI-powered Enterprise Resource Planning (ERP) and Supply Chain Management (SCM) systems has shown capacity to harmonize information flows across fragmented supply networks, reducing the bullwhip effect and improving crisis response capabilities. However, these technical advances must be complemented by governance frameworks that address cybersecurity vulnerabilities, data privacy concerns, and the ethical implications of automated supply chain decisions.

This paper addresses these imperatives by developing the Strategic AI Supply Chain Optimization and Resilience (SASCOR) framework, which integrates technical AI capabilities with risk governance structures to enhance U.S. supply chain resilience. The framework emphasizes four critical capabilities: real-time visibility through IoT and sensor integration, predictive risk assessment using machine learning, dynamic optimization algorithms that balance efficiency with redundancy, and collaborative governance mechanisms that facilitate information sharing across supply chain partners while protecting competitive and security interests.

Theoretical Foundations: Supply Chain Resilience in the AI Era

A. Conceptualizing Supply Chain Resilience

Supply chain resilience encompasses the capacity to anticipate, adapt to, and recover from disruptive events while maintaining operational continuity and competitive positioning. Traditional resilience frameworks emphasize redundancy and inventory buffering as primary mitigation strategies. However, the complexity and velocity of modern supply chain disruptions ranging from cyberattacks to geopolitical shocks demand more dynamic, intelligence-driven approaches capable of real-time adaptation.

The integration of AI into supply chain resilience strategies represents a paradigm shift from reactive recovery to proactive adaptation. Machine learning models can detect early warning signals of disruption by analyzing diverse data streams including weather patterns, geopolitical indicators, supplier financial health, and logistics network performance. This

predictive capacity enables organizations to implement contingency measures before disruptions cascade, transforming resilience from a cost center into a competitive advantage.

B. AI Applications in Supply Chain Optimization

Contemporary AI applications in supply chain management span demand forecasting, inventory optimization, route planning, and supplier selection. Deep learning architectures, particularly hybrid models combining convolutional neural networks with recurrent structures, have demonstrated superior performance in capturing nonlinear relationships and temporal dependencies in supply chain data. These capabilities are critical for managing the volatility characterizing post-pandemic supply environments, where historical patterns may no longer predict future demand.

The optimization of last-mile delivery operations exemplifies AI's transformative potential. AI-driven route optimization systems can process real-time traffic data, weather conditions, and delivery priorities to dynamically adjust logistics operations, reducing costs while improving service levels. Similarly, predictive maintenance applications using IoT sensor data can anticipate equipment failures before they disrupt production schedules, enhancing manufacturing continuity.

C. Risk Taxonomy for AI-Enabled Supply Chains

AI-enhanced supply chains face distinctive risk categories requiring specialized governance approaches. Technical risks include model drift, where predictive accuracy degrades as supply conditions evolve; adversarial attacks targeting AI systems to disrupt logistics operations; and integration failures between AI platforms and legacy enterprise systems. Operational risks encompass over-reliance on automated decision-making, algorithmic bias in supplier selection, and the concentration of critical AI infrastructure in vulnerable geographic locations (Begum et al., n.d.; Begum, 2022).

Strategic risks involve the potential for AI-driven optimization to inadvertently eliminate redundancies that provide resilience, creating hyper-efficient but fragile supply networks. The pursuit of just-in-time optimization through AI must be balanced against the need for buffer inventory and diversified supplier bases that provide shock absorption capacity. Additionally, data security risks are amplified as supply chain AI systems require extensive data sharing across organizational boundaries, creating attack surfaces for cyber adversaries.

The Strategic AI Supply Chain Optimization and Resilience (SASCOR) Framework

A. Framework Architecture

The SASCOR framework operationalizes supply chain resilience through four integrated capability pillars: Visibility Enhancement, Predictive Intelligence, Dynamic Optimization, and Collaborative Governance. Unlike traditional supply chain frameworks that treat these capabilities as sequential functions, SASCOR emphasizes their continuous interaction and mutual reinforcement.

Figure 1 illustrates the SASCOR framework architecture, depicting the bidirectional relationships between visibility infrastructure, predictive analytics, optimization engines, and governance mechanisms. The framework's central hub represents the integration layer where data from diverse sources converges to inform decision-making across all four pillars.

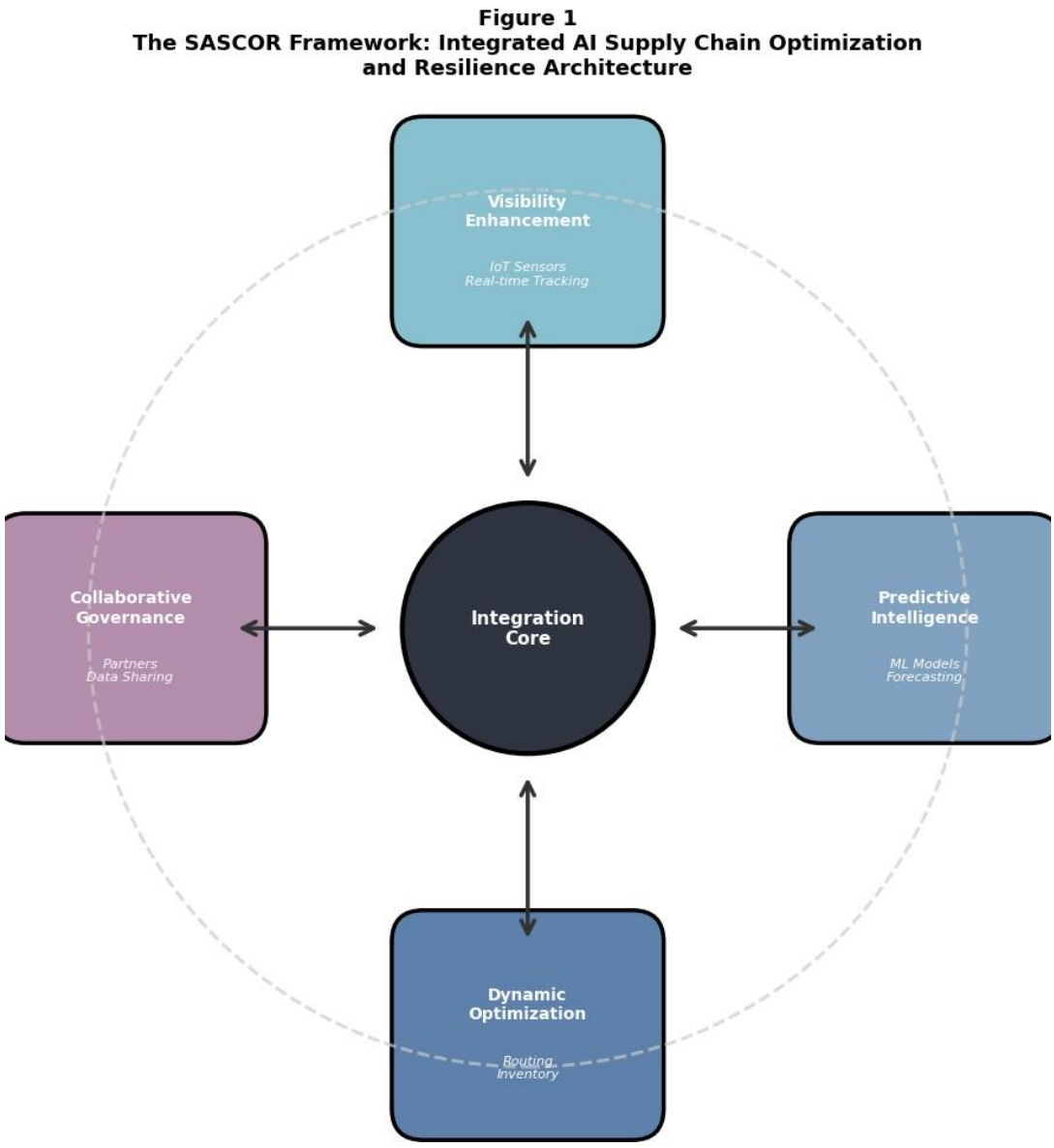

Figure 1. The SASCOR Framework: Integrated AI Supply Chain Optimization and Resilience Architecture

B. AI-Driven Risk Assessment Matrix

Table 1 presents the AI-Driven Supply Chain Risk Assessment Matrix (AI-SCRAM), which categorizes supply chain risks across operational, strategic, and external dimensions while specifying AI-enabled mitigation strategies and performance indicators.

Table 1. AI-Driven Supply Chain Risk Assessment Matrix (AI-SCRAM)

Risk Category	Risk Type	AI Mitigation Strategy	Key Performance Indicator	Data Source
Risk Category	Risk Type	AI Mitigation Strategy	Key Performance Indicator	Data Source
Operational	Demand Volatility	ConvLSTM forecasting models with multi-variable inputs (Mishu et al., 2024)	Forecast accuracy (MAE < 5%), Inventory turnover ratio	POS data, economic indicators, social sentiment
Operational	Logistics	Real-time route	On-time delivery	GPS telemetry,

	Disruption	optimization using reinforcement learning	rate, Cost per mile	weather APIs, traffic patterns
Operational	Supplier Failure	Predictive analytics for supplier financial health monitoring	Supplier risk score, Early warning detection rate	Financial statements, credit ratings, news sentiment
Strategic	Concentration Risk	Network analysis algorithms for dependency mapping	Supplier diversification index, Single-source criticality score	Procurement data, supplier location intelligence
Strategic	Cyber Vulnerability	AI-powered threat detection for supply chain	Mean time to detection, Incident response	Security logs, network traffic, threat
Risk Category	Risk Type	AI Mitigation Strategy	Key Performance Indicator	Data Source
		systems (Thakur et al., 2026)	latency	intelligence
External	Geopolitical Shock	NLP analysis of geopolitical risk indicators and trade policy	Risk exposure score, Scenario simulation accuracy	News feeds, regulatory databases, sanctions lists
External	Trade Policy Change	Machine learning models for tariff and compliance impact assessment	Compliance cost prediction accuracy, Regulatory lag time	Trade databases, customs records, policy documents

The matrix emphasizes that AI-driven risk mitigation requires diverse data integration beyond traditional enterprise data, incorporating external signals ranging from social media sentiment to satellite imagery. The framework advocates for multi-model ensembles that combine different AI architectures such as the ConvLSTM approach for time-series forecasting and natural language processing for geopolitical risk assessment—to provide robust predictions across varied risk categories.

C. Dynamic Optimization and Redundancy Balancing

Table 2 presents the Optimization-Resilience Balancing Matrix (ORBM), which guides decision-makers in calibrating AI-driven efficiency optimization against resilience requirements.

Table 2. Optimization-Resilience Balancing Matrix (ORBM)

Supply Chain Function	Efficiency Optimization	Resilience Enhancement	Balancing Strategy	AI Application
Inventory Management	Minimize carrying costs through demand	Strategic buffer stock for	Dynamic safety stock	Predictive analytics

	forecasting	critical components	algorithms that adjust to risk levels	with risk-weighted optimization (Begum, n.d.; Begum, 2022)
Supplier Selection	Lowest cost bid optimization	Diversified supplier base with geographic distribution	Multi-objective optimization considering cost, risk, and performance	Supplier scoring models integrating risk metrics (Hussain et al., 2025)
Transportation Routing	Shortest path/minimum fuel consumption	Alternative route redundancy for critical lanes	Real-time rerouting capabilities with pre-positioned alternatives	Reinforcement learning for dynamic routing (Thakur et al., 2026)
Supply Chain Function	Efficiency Optimization	Resilience Enhancement	Balancing Strategy	AI Application
Production Scheduling	Maximum throughput/utilization	Flexible capacity for surge demand	Modular production planning with AI-enabled capacity switching	Generative AI for scenario planning (Hussain et al., 2025)
Information Sharing	Minimal data exchange (competitive protection)	Transparent visibility for coordination	Tiered data sharing with privacy-preserving AI techniques	Federated learning and secure multi-party computation (Jobullah et al., 2024)

The ORBM addresses the fundamental tension between lean optimization and resilient redundancy. Traditional supply chain management often treated these objectives as mutually exclusive, but AI enables adaptive optimization that modulates efficiency based on risk conditions. For instance, inventory optimization algorithms can automatically increase safety stocks when predictive models detect elevated disruption risks, then reduce buffers when conditions stabilize.

Implementation Pathways and Governance

A. Phased Implementation Strategy

The implementation of SASCOR requires staged deployment to manage complexity and ensure organizational readiness. Phase 1: Visibility Infrastructure involves deploying IoT sensors, RFID tracking, and data integration platforms to establish real-time supply chain visibility. This phase

addresses the data foundation requirements for subsequent AI applications, ensuring data quality and interoperability across supply chain.

Phase 2: Predictive Capability Development focuses on training and deploying machine learning models for demand forecasting, risk prediction, and supplier performance assessment. This phase requires careful attention to model validation, bias detection, and the integration of human expertise with algorithmic predictions to avoid over-reliance on automated systems.

Phase 3: Optimization Integration involves deploying AI-driven optimization engines that can dynamically adjust supply chain operations based on predictive insights. This includes automated reorder point adjustment, dynamic routing, and capacity allocation. Governance mechanisms must ensure that optimization decisions align with strategic resilience objectives and do not inadvertently concentrate risk.

Phase 4: Ecosystem Collaboration extends SASCOR capabilities across supply chain networks, enabling coordinated response to disruptions through shared visibility and collaborative planning. This phase addresses data sharing governance, cybersecurity protocols, and the development of shared standards for AI.

B. Cybersecurity and Data Governance

The integration of AI into supply chain operations amplifies cybersecurity risks, as supply chain systems become targets for adversaries seeking to disrupt critical infrastructure. The SASCOR framework incorporates AI-powered cybersecurity mechanisms, including anomaly detection for supply chain transactions, behavioral analytics for access control, and automated response to detected threats .

Data governance frameworks must address the tension between information sharing for supply chain coordination and the protection of competitive and security-sensitive data. The framework advocates for tiered data governance models that classify supply chain
information according to sensitivity levels, with AI-enabled anonymization and aggregation techniques enabling collaborative insights without exposing proprietary details.

C. Workforce and Change Management

The transformation of supply chain operations through AI requires significant workforce adaptation, including upskilling supply chain professionals in data literacy, AI interpretation, and human-machine collaboration. The framework emphasizes augmentation rather than replacement of human decision-makers, positioning AI as a tool for enhancing supply chain manager capabilities rather than automating their roles entirely (Sarkar et al., 2021; Begum, 2022).

Change management strategies must address resistance from supply chain partners who may perceive data sharing requirements as threatening competitive advantages. The framework advocates for value demonstration through pilot projects that demonstrate mutual benefits of AI-enabled collaboration, building trust and willingness for deeper.

Sector-Specific Applications and Case Implications

A. Manufacturing and Industrial Production

Manufacturing supply chains face particular challenges regarding component availability and production continuity. The application of generative AI for rapid prototyping, combined with predictive maintenance and demand forecasting, enables more responsive manufacturing operations . However, the integration of AI into manufacturing supply chains must navigate export control regulations and intellectual property protection requirements, particularly when AI systems involve dual-use technologies or cross-border data flows.

The SASCOR framework addresses these challenges through compliance-embedded AI that incorporates regulatory constraints into optimization algorithms, ensuring that efficiency gains do

not violate export controls or IP protection requirements. This approach is particularly critical for advanced manufacturing sectors where supply chain disruptions can have national security implications.

B. Healthcare and Critical Medical Supplies

Healthcare supply chains demonstrated acute fragility during the COVID-19 pandemic, with shortages of personal protective equipment, ventilators, and pharmaceuticals exposing life-threatening vulnerabilities. AI-enabled supply chain resilience in healthcare requires particular attention to regulatory compliance, product authentication, and the ethical implications of allocation decisions during scarcity.

The framework advocates for strategic stockpiling optimization using AI models that predict likely shortage scenarios and optimal stockpile locations, balancing carrying costs against the criticality of medical supply availability. IoT-enabled cold chain monitoring ensures integrity of temperature-sensitive supplies, while predictive analytics anticipate demand surges during health emergencies.

C. Defense and Critical Infrastructure

Defense supply chains present unique resilience requirements given their national security implications and the potential for targeted adversarial disruption. The SASCOR framework emphasizes supply chain security alongside efficiency, incorporating cybersecurity measures, supplier vetting, and alternative sourcing strategies that ensure continuity under contested conditions.

AI applications in defense supply chains must address the threat of adversarial machine learning, where competitors or adversaries may attempt to poison training data or manipulate AI systems to create vulnerabilities. The framework advocates for robust AI architectures that incorporate adversarial training and continuous validation to detect and mitigate such attacks.

Policy Implications and National Economic Security

A. Strategic Autonomy and Supply Chain Sovereignty

The concentration of critical supply capabilities in geopolitically sensitive regions poses strategic risks that market-driven optimization alone cannot address. The SASCOR framework supports strategic reshoring and friend-shoring decisions by providing data-driven

assessments of supply chain vulnerabilities and the costs/benefits of supplier diversification. AI models can simulate the impact of various reshoring scenarios on costs, lead times, and resilience, informing policy decisions regarding industrial incentives and strategic investments.

B. Regulatory Frameworks for AI in Critical Infrastructure

The deployment of AI in supply chains for critical infrastructure sectors requires regulatory frameworks that ensure security, reliability, and ethical operation without stifling innovation. The framework advocates for risk-based regulation that calibrates oversight intensity to the criticality of supply chain functions and the potential consequences of AI system failures. This approach requires close coordination between regulatory agencies, industry stakeholders, and AI developers to establish standards for AI validation, cybersecurity, and data governance.

C. International Cooperation and Standards

Supply chain resilience increasingly depends on international coordination, as even domestic supply chains rely on global inputs and markets. The SASCOR framework supports international standards development for AI-enabled supply chain interoperability, data sharing protocols, and cybersecurity best practices. Such standards can facilitate the trusted exchange of supply chain information across borders while protecting national security and commercial interests.

Conclusion

The resilience of U.S. supply chains is foundational to national economic security, industrial competitiveness, and societal welfare. This paper has presented the Strategic AI Supply Chain Optimization and Resilience (SASCOR) framework, which integrates artificial intelligence capabilities with comprehensive risk governance to address the complex challenges facing modern supply networks.

By synthesizing advances in predictive analytics, dynamic optimization, and cybersecurity, the framework provides a structured approach to enhancing supply chain visibility,

anticipating disruptions, and adapting operations in real-time. The AI-Driven Supply Chain Risk Assessment Matrix (Table 1) and Optimization-Resilience Balancing Matrix (Table 2) offer practical tools for supply chain managers to navigate the tension between efficiency and resilience.

The implementation of AI in supply chain operations is not merely a technical upgrade but a strategic transformation requiring organizational adaptation, workforce development, and collaborative governance across supply chain ecosystems. As global supply chains face increasing volatility from climate change, geopolitical conflict, and technological disruption, the capabilities enabled by the SASCOR framework will be essential for maintaining U.S. economic security and competitive advantage.

Future research should address the evolving challenges of AI governance in supply chains, including the integration of quantum computing for optimization, the development of autonomous supply chain systems, and the international harmonization of AI supply chain standards. The continued evolution of these capabilities will determine the resilience of U.S. industry in an era of unprecedented supply chain complexity.

References

Begum, S. (2022). Optimizing capital deployment in post-pandemic America: AI-powered predictive analytics for startup resilience and growth. International Journal of Computer Applications Technology and Research, 11(12), 700–710.

Khan, Muhammad Ismaeel, Hassan Tahir, Md Ismail Jobiullah, Ali Raza A. Khan, Sakera Begum, and Ihtasham Hafeez. "Enhancing IoT Security: A Lightweight Cloning Approach for RFID/NFC Access Control Systems." Cuestiones de Fisioterapia 52, no. 2 (2023): 231-248.

Kou, G., Peng, Y., & Wang, G. (2014). Evaluation of clustering algorithms for financial risk analysis. Information Sciences, 275, 1-12.

Crook, J. N., Edelman, D. B., & Thomas, L. C. (2007). Recent developments in consumer credit risk assessment. European Journal of Operational Research, 183(3), 1447-1465.

Lessmann, S., Baesens, B., Seow, H. V., & Thomas, L. C. (2015). Benchmarking state-of-the-art classification algorithms for credit scoring. European Journal of Operational Research, 247(1), 124-136.

Kou, G., Chao, X., Peng, Y., Alsaadi, F. E., & Herrera-Viedma, E. (2019). Machine learning methods for systemic risk analysis. Technological and Economic Development, 25(5), 716-742.

Thomas, K. (2021). Generation AI: The Rise of the Resilient Entrepreneur. Katerina Thomas

Ibrahim, I. (2022). Future-Ready Retail: How to Reimagine the Customer Experience, Rebuild Retail Spaces and Reignite Our Shopping Malls and Streets. Kogan Page Publishers

Gupta, A., Wright, C., Ganapini, M. B., Sweidan, M., & Butalid, R. (2022, February 12). State of AI ethics report (Volume 6). arXiv preprint arXiv:2202.07435

Hutson, J., Jeevanjee, T., Vander Graaf, V., Lively, J., Weber, J., Weir, G., Arnone, K., Carnes, G., Vosevich, K., Plate, D., & Leary, M. (2022). Artificial intelligence and the disruption of higher education: Strategies for integrations across disciplines. Creative Education, 13(12).

Miscovich, P. (2021). The intelligent, experiential and competitive workplace: Part 1. Journal of

AI, Robotics & Workplace Automation, 1(1), 70–86
Gallardo-Gallardo, E., & Collings, D. G. (2021). Talent management for the future of work. In New Directions in the Future of Work (pp. 35–54). Emerald Publishing Limited
Puchakayala, P. R. (2022). Data quality management for effective machine learning and AI modelling, best practices and emerging trends. International Research Journal of Innovations in Engineering and Technology
Marwala, T. (2022). Heal Our World: Securing a Sustainable Future. Jonathan Ball Publishers.
Tang, J., Lin, H., Fan, X., Yu, X., & Lu, Q. (2022). A topology-based evaluation of resilience on urban road networks against epidemic spread: Implications for COVID-19 responses. Frontiers in Public Health, 10, 1023176.
Soetan, O., & Olowonigba, J. K. (2021). Decentralized reinforcement learning collectives advancing autonomous automation strategies for dynamic, scalable and secure operations under adversarial environmental uncertainties. GSC Advanced Research and Reviews, 9(3), 164–183. https://doi.org/10.30574/gscarr.2021.9.3.0294