CHAPTER 19

Cognitive Supply Chains: Integrating Human-AI Collaboration and Cybersecurity for Sustainable Value Creation in the Era of Industry 5.0

*Fiza Shaikh**

ABSTRACT

Industry 5.0 ushers in a new manufacturing and supply chain paradigm that prioritizes human-AI collaboration, personalization, sustainability, and robust cybersecurity. This paper proposes the Cognitive Supply Chain (CSC) framework, which integrates Artificial Intelligence, human expertise, explainable AI, digital twins, blockchain transparency, green logistics, and cybersecurity to create resilient, ethical, and secure supply networks. By embedding cybersecurity strategies throughout the CSC, organizations can protect data integrity, ensure trust, and sustain value creation while adapting to dynamic global challenges. This study develops a comprehensive CSC model and discusses the multifaceted role of cybersecurity in enabling secure operations and ethical governance within Industry 5.0 supply chains.

Keywords: Collaboration; Sustainability; Ethical; Blockchain transparency.

1.0 Introduction

The evolution from Industry 4.0 to Industry 5.0 involves a significant shift from automation-centric systems to human–machine synergistic environments emphasizing sustainability, personalization, and security alongside efficiency. While Industry 4.0 introduced interconnected smart devices and AI-driven automation, this advance also exposed supply chains to complex cybersecurity threats including data breaches, system disruptions, and malicious attacks.

Industry 5.0's focus on human creativity and sustainable development necessitates integrating cybersecurity within supply chain frameworks to safeguard sensitive data, ensure operational continuity, and maintain stakeholder trust. This paper extends the Cognitive Supply Chain (CSC) concept by embedding robust cybersecurity protocols as foundational to secure and sustainable supply chain ecosystems.

**Student, Department of MCA, Dr. Moonje Institute of Management and Computer Studies, Nashik, Maharashtra, India (E-mail: skfizra92@gmail.com)*

DOI: 10.17492/JPI/ICISI2025/251219 *ISBN: 978-93-49790-69-8*

Research Objective: To formulate and articulate a Cognitive Supply Chain framework that integrates AI, human intelligence, sustainability, and cybersecurity to enhance supply chain resilience, transparency, customization, and trustworthiness in Industry 5.0.

2.0 Literature Review

2.1 Industry 4.0 and security limitations

Industry 4.0's rapid adoption of IoT, cloud computing, and automation brought unprecedented efficiency gains but exposed vulnerabilities. Cyberattacks targeting supply networks, data manipulation, and disruption of automated processes revealed security gaps requiring urgent attention (Ghobakhloo *et al.*, 2023).

2.2 Industry 5.0 principles with cybersecurity focus

Industry 5.0 principles emphasize human-centered design, ethics, sustainability, and resilience supported by trustworthy AI and secure digital infrastructures (Narula *et al.*, 2024). Cybersecurity now forms an essential dimension to protect supply chain data, AI decision-making processes, and interconnected assets.

2.3 Research gap

Current supply chain research predominantly addresses automation and efficiency but seldom integrates cybersecurity with human-AI collaboration and sustainability in a holistic framework. The proposed CSC with embedded cybersecurity addresses this lacuna.

3.0 Cognitive Supply Chain Framework with Cyber Security

This revised CSC framework integrates five pillars:

- *Human-AI collaboration:* AI systems provide actionable insights into demand forecasting and logistics while humans apply contextual knowledge and ethical judgment. Cybersecurity ensures protected communication channels, secure AI model training, and defense against adversarial AI attacks.
- *Explainable AI (XAI):* XAI improves transparency of AI-driven decisions. Cybersecurity safeguards the integrity of AI explanations and prevents data leakage or manipulation through secure software design and controlled user access.
- *Digital twins and blockchain transparency:* Digital twins simulate supply chain operations in real time, while blockchain secures transaction records. Cryptographic methods, authentication, and network security prevent data breaches and ensure system availability, authenticity, and anonymity.

- *Green logistics and sustainability:* IoT-enabled sustainable logistics rely on connected devices monitoring resource usage. Securing IoT networks and devices from cyber threats ensures data accuracy and operational reliability necessary for sustainability goals.
- *Cybersecurity:* Cybersecurity underpins all dimensions, encompassing encryption, intrusion detection, identity and access management, and threat intelligence. It maintains the confidentiality, integrity, and availability of supply chain data and digital assets, enabling trusted collaboration among stakeholders.

4.0 Conceptual Model

Dimension	Technologies	Human Role	Cybersecurity Focus	Sustainability & Value Impact
Human-AI Collaboration	AI, ML, Secure Communication	Contextual insight & ethics	Protect AI models, secure data exchange	Personalized service, adaptive risk management
Explainable AI (XAI)	Transparent AI frameworks	Ethical oversight	Secure explanation layers to prevent leaks	Trust, compliance, accountability
Digital Twins & Blockchain	Simulation, IoT, Blockchain	Scenario planning, validation	Encryption, authentication, intrusion detection	Traceability, ethical sourcing
Green Logistics	IoT, Circular Economy	Strategic sustainability	IoT device and network security	Carbon reduction, resource efficiency
Cybersecurity (Cross-cutting)	Encryption, Access Control, IDS, Firewalls	Security governance, risk management	Continuous threat monitoring, incident response	Protects data integrity enabling sustainable operations

5.0 Seven Steps Suggested

In the Cognitive Supply Chain Framework: Human–AI Collaboration and Cybersecurity in Industry 5.0:

1. *Assessment and Strategy Phase:* The first step in implementing a Cognitive Supply Chain (CSC) framework involves thoroughly assessing the existing supply chain processes. Organizations must conduct a detailed audit of current operations, identifying inefficiencies, risks, and opportunities where cognitive technologies can add value. Along with this, readiness evaluation plays a crucial role in determining the maturity of digital infrastructure, workforce skills, and cybersecurity practices. Finally, aligning the CSC objectives with Industry 5.0 principles—sustainability, resilience, and

human-centric collaboration—ensures the framework supports both business performance and societal goals.

2. *Data and Infrastructure Setup:* Once the strategy is in place, the next step is to establish robust data and infrastructure foundations. This involves integrating structured and unstructured data from diverse sources such as ERP systems, IoT devices, RFID tracking, and customer feedback. A key enabler here is the creation of digital twins—virtual replicas of supply chain networks that simulate demand, logistics, and production scenarios. Securing this infrastructure with cloud platforms and blockchain technologies ensures transparency, reliability, and resilience in the data-driven ecosystem.
3. *Human–AI Collaboration Layer:* The hallmark of Industry 5.0 is human–AI collaboration, where intelligent systems support but do not replace human decision-makers. AI tools provide predictive analytics, anomaly detection, and optimization models, while humans bring contextual knowledge, ethical judgment, and accountability. Collaborative platforms like natural language processing (NLP) chatbots and augmented reality interfaces allow workers to interact seamlessly with AI insights. To maximize benefits, organizations must invest in employee training programs that develop AI literacy, digital ethics, and collaborative decision-making skills.
4. *Cybersecurity Integration:* Cybersecurity is integral to the cognitive supply chain, as interconnected networks face increasing threats from cyberattacks. Organizations must begin by identifying risks, including vulnerabilities in IoT devices, supplier contracts, and logistics systems. Protection measures such as multi-factor authentication, AI-powered intrusion detection systems, and continuous monitoring safeguard sensitive data and operations. Compliance with global standards such as ISO 28000 and GDPR further strengthens resilience. Embedding cybersecurity into every layer of the CSC framework ensures that innovation does not come at the expense of security.
5. *Pilot Implementation:* Before scaling the CSC framework, organizations should conduct a pilot test in a selected supply chain segment, such as procurement or warehouse management. This allows teams to validate the effectiveness of AI-human collaboration and evaluate the cybersecurity measures in real-world conditions. Key performance indicators (KPIs) such as lead time reduction, improved forecasting accuracy, and minimized disruptions are monitored closely. The pilot phase provides actionable insights and builds confidence among stakeholders, reducing resistance to broader adoption.
6. *Scaling and Optimization:* Following successful pilots, the CSC framework can be scaled across the entire supply chain ecosystem. This expansion involves integrating suppliers, logistics partners, and customers into the collaborative system. Continuous

learning AI models adapt to disruptions such as geopolitical risks, pandemics, or climate-related challenges, ensuring resilience. Optimization also involves refining workflows, upgrading security measures, and continuously training the workforce to remain aligned with evolving technologies. This step transforms isolated improvements into systemic, industry-wide benefits.

7. *Sustainability and Continuous Improvement:* The final step emphasizes sustainability and long-term adaptability, aligning with Industry 5.0's focus on human-centric and eco-friendly growth. Organizations should adopt green AI models that optimize energy use and reduce emissions throughout the supply chain. Measuring environmental impact—such as carbon footprint reduction and waste minimization—becomes part of routine performance reviews. Continuous feedback loops between humans and AI ensure that strategies evolve to meet emerging challenges. This ongoing process not only strengthens competitiveness but also promotes social responsibility and sustainable value creation.

6.0 Implications for Industry 5.0 Supply Chains

The enhanced CSC model supports:

- *Resilience:* Rapid threat detection and mitigation protect supply continuity.
- *Trust:* Robust security policies and transparent AI foster stakeholder confidence.
- *Sustainability:* Accurate and reliable data enable informed environmental decision-making.
- *Ethical Compliance:* Secure AI and blockchain systems uphold fairness and accountability.

Organizations embedding this CSC framework balance technological innovation with human-centric, ethical, and secure supply chain practices, necessary for competing in Industry 5.0.

7.0 Conclusion and Future Research

The Cognitive Supply Chain enriched with cybersecurity transforms supply chains into secure, transparent, and sustainable ecosystems driven by human-AI collaboration. Cybersecurity safeguards the integrity of digital systems essential for resilient operations and ethical governance. Future research should focus on developing adaptive cybersecurity solutions for AI-driven supply chains, socioeconomic impacts of secure CSCs, and standardization of security practices within Industry 5.0 frameworks.

References

1. Ghobakhloo, M. *et al.* (2023). Innovative Solutions for Enhancing Supply Chain Resilience in Industry 5.0. Journal of Industrial Engineering.
2. Narula, R., Tortorella, G.L., Sharma, A. (2024). Synergizing Human-AI Collaboration for Personalized Supply Chains. International Journal of Production Research.
3. Tortorella, G.L. *et al.* (2024). Demand-Driven Supply Chains Enhanced by Industry 5.0 Technologies. Supply Chain Management Review.
4. Silva, E. *et al.* (2023). Explainable AI in Ethical Supply Chain Decision Making. AI Ethics Journal.
5. Ivanov, D. (2023). Blockchain and Digital Twins for Supply Chain Transparency and Resilience. Operations Management Quarterly.
6. Rehman, M. *et al.* (2024). Green Logistics and Sustainability in Cognitive Supply Chains. Sustainability Journal.

DOI: 10.17492/JPI/ICISI2025/251219 *ISBN: 978-93-49790-69-8*