ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

SECURITY VULNERABILITIES AND RECURRING OPERATIONAL FAILURE PATTERNS IN AUTOMATED LOGISTICS AND DISTRIBUTION CENTERS ACROSS THE UNITED STATES

Sadia Watara
Dakota State University

Article DOI: https://doi.org/10.36713/epra26727
DOI No: 10.36713/epra26727

ABSTRACT

This research represents a synthesis of growing security vulnerabilities and operational failure risks in U. S. automated logistics and distribution systems, to demonstrate their potential impacts on the national supply chain. Drawing from peer-reviewed studies, government reports, and analysis from the transportation industry, this research explores security vulnerabilities like ransomware attacks against transportation management systems, as well as insider exploitation, which together accounted for more than $15 billion in annual losses in 2024 alone. Operational failures such as malfunction of equipment, driver understaffing to manage automated logistics systems, and bottlenecks due to weather compound these risks. This research analysis discovers interconnected threat vectors, including IoT-enabled trucking and warehouse automation which increases the cyber-attack surfaces. Also, regulatory gaps in electronic logging device (ELD) compliance and supply chain visibility are identified, which increases resilience deficiencies. Key discoveries highlight undervalued failure modes such as AI driven predictive analytics blind spots in multimodal freight networks. Hence, this research proposes that integrated countermeasures, enhanced cybersecurity frameworks such as Nist 800-53 adaptations, real-time risk dashboards and public-private resilience pacts provide the most effective way forward. By giving priority to these, stakeholders can eliminate the disruptions and safeguard national economic stability and operational continuity in today's era of hybrid threats within logistics and distribution.

KEYWORDS: *Supply chain resilience, logistics cybersecurity, operational risk mitigation, freight disruptions, national security threats*

INTRODUCTION

Global supply chains and transportation networks have become very critical to international trade, economic growth, and the function of our society, with the rise in globalization and digitization (Ogunsola et al, 2025a). These complex, interconnected systems have evolved to include a wide variety of actors, infrastructure, and digital technologies all designed to streamline operations and improve the global efficiency of the logistical systems (Okolie et al., 2021, Ogunsola et al, 2025b). However, the growing dependence on information and communication technologies (ICT), Internet of Things (IoT), artificial intelligence (AI) and cloud-based systems in these networks has at the same time provided new opportunities for cyber threats. These threats, if not adequately understood or mitigated, present serious risks to operational continuity, economic stability, national security and public safety (Austin-Gabriel et al., 2021). Consequently, an increasing need exists to systematically explore the changing landscape of cyber threats made against global supply chains and transport networks, as well as resiliency strategies put in place to defend and recover from such instances. Cybersecurity has emerged as a paramount concern in all kinds of critical infrastructure sectors. However, its implications are especially vast within logistics and transportation (Hussain et al., 2021). From maritime shipping lanes and port operations to air cargo, rail freight and last-mile delivery systems, each and every node and link in the global supply chain is potentially susceptible to cyber intrusions. The threat landscape is dynamic and adversaries range from nation-state actors, organized cybercriminal groups, insider threats and malicious attackers. Common cyber threats that target these industries include ransomware attacks, data breaches, distributed DoS (DDoS) attacks, supply chain breaches, and phishing attacks (Ike et al., 2021). The complexity of the digital ecosystems in the supply chains introduces further complexity, and in many cases makes it difficult to identify vulnerabilities and/or trace the source of cyberattacks or even to orchestrate a timely and holistic response. The effects of cyberattacks on supply chains can be both immediate and widespread (Oladosu et al., 2021). In the short term, production is interrupted, delays are introduced in delivery and breakdowns happen in communication which can result in massive financial losses and damage to stakeholder trust. In the longer term, sustained or recurring cyber events can affect the strategic competitiveness of countries and businesses, affect consumer confidence and could even potentially lead to cascading effects in interconnected economic sectors.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

U.S. Logistics Evolution and Vulnerability Foundations

Logistics has evolved immensely over its lifetime, changing with society's demands and leaping in technology over the course of thousands of years. However in this process, vulnerabilities have been introduced and are growing significantly. The origin of logistics trace back to antiquity, where civilizations such as Mesopotamia, Egypt, China, Rome developed transport and storage systems to sustain their armies, cities and trade. Relying on carts, ships and pack animals, they created strategic routes and early warehouses. These innovations revealed some fundamental weaknesses such as route ambushes and spoilage, foreshadowing enduring supply chain vulnerabilities (Mecalux, 2023).

In the Middle Ages, the role of the guilds and emerging trade routes enhanced these practices, with the markets as storage and distribution points. However, dependence on human networks introduced new and varied vulnerabilities such as banditry along trade paths and erratic quality control, showing logistics' perennial exposure to physical and informational disruptions (Observatoire-Janus, 2025).

Then came the Industrial Revolution of the 18th century which marked a seismic shift. Machinery, railways and steamships revolutionized transport, increasing the speed of goods flow and the scale of production. Yet, centralized rail centers created chokepoints in which strikes and sabotage exposed, highlighting how efficiency gains created systemic, single points of failure (Magoon, 2026).

By the 20th century logistics was developed as a formal discipline in the context of mass production, globalization, and communication innovations ranging from telephones and radios to the internet. Concepts such as just-in-time inventories and integrated supply chain management maximized efficiency and exacerbated the bullwhip effects where supply chain shocks in upstream segments cascaded to the downstream level, adding to the already growing vulnerabilities, labor disputes and geopolitical tension (Institute for Supply Management, 2025).



Figure 1: ***Bureau of Transportation Statistics (BTS), 2025. U.S. Ton-Miles of Freight (BTS Special Tabulation) (millions). U.S. Department of Transportation. Available at: https://www.bts.gov/content/us-ton-miles-freight***

The introduction of the digital era has further increased these risks. As warehouse management software, barcodes, RFI, and real-time tracking provide visibility, they do so at the expense of cyber exposure, as early hacks on port systems have shown data to be a new battleground. Entering into logistics 4.0, this paradigm of digitalization, artificial intelligence, Internet of Things (IoT), and robotic process automation drives route optimization, autonomous vehicles, and automated warehouses. While this IoT interconnectivity is transformative, the interconnectivity creates an expanded attack surface as seen in cases of ransomware targeting telematics, making the cyber and physical a hybrid attack (Eye Security, 2025).

Logistics 5.0 symbolizes a human-centric pivot, echoing Industry 5.0 as defined by the European Commission. This prioritizes human well-being, sustainability, and resilience. These imperatives are being sharpened by shocks such as the global disruptions of the COVID-19 pandemic and U.S.-specific freight bottlenecks. In American logistics, these foundations manifest acutely like overreliance on just-in-time trucking, which forms about 72% of freight ton-miles, which exposes networks to cyber intrusions, port congestions, and climate extremes. These demand a fortified defense against compounding national security risks (Snow, 2025).

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

This evolution accelerates into automated logistics and distribution centers across the United States, where Logistics 5.0 principles converge with robotic automation and AI orchestration. Pioneered by giants such as Amazon and Walmart since the mid 2010s, these facilities, numbering more than 1,000 high automation hubs in 2025 incorporate autonomous guided vehicles (AGVs), robotic arms used for picking/packing and warehouse execution systems driven by artificial intelligence (AI). However, this change creates magnifying vulnerabilities. IoT sensor networks create expansive cyber attack surfaces susceptible to DDoS or ransomware halting entire operations, while recurring mechanical failures in robotic fleets such as conveyor jams due to surges, expose single point dependencies. This causes the distribution delays on a regional scale to become huge backlogs at a national level during peak seasons. (Reuter, 2024).

Security Threats and Operational Risks in Automated Logistics and Distribution Systems

Today's growing digitalization of global supply chains and transportation networks has made these critical infrastructures vulnerable to a variety of cyber threats, making cybersecurity an ongoing concern for both the private and the public sectors. Modern supply chains are complex and interdependent systems that involve different stakeholders and technologies such as the Internet of Things (IoT) devices, cloud computing, blockchain, and enterprise resource planning (ERP) systems (Meyer et al., 2021). As these systems become increasingly interlinked, they also become increasingly vulnerable to cyber-attacks such as ransomware, phishing and advanced persistent threats (APTs). Cybercriminals explore the weakest links in extended networks, and often target third-party vendors and logistics providers to gain unauthorized access. For example, the volumetric SolarWinds attack in 2020 saw a supply chain infiltration where hackers injected malicious code known as SUNBURST, into SolarWinds' Orion network management software updates. About 18000 customers including U.S. government agencies and Fortune 500 companies downloaded the trojanized updates, which granted the attackers stealth, long term remote access. This highlights the vulnerabilities of supply chain software and its resulting trickle-down impact that such breaches can have on global operations. Similarly, breaches of maritime ports and air traffic control systems have shown us how disruption of the digital infrastructure can cause significant delays and losses in both financial and safety measures. (Faith, 2018) and (Casalino et al., 2019) have shown that with physical cyber systems and increasing standards in the logistics and transport sector, cyber threats are no longer limited to information threats, but also physical and operational hazards. It is also observed that specific technologies can be both the vectors and solutions of the cybersecurity landscape. Additionally, the adaptation of IoT into logistics such as smart containers, GPS tracking and automated inventory systems has increased visibility and inefficiency significantly but at the same time has opened up new attack surfaces. And (Lusimbo, 2016) warns that if these devices aren't protected by sound security protocols, they can be exploited to disrupt entire supply chains. Furthermore, legacy systems and poor integration practices heighten these vulnerabilities, making old infrastructure more specifically prone to cyber intrusions. On the other hand, technological solutions, including blockchain and artificial intelligence (AI) are being explored as a way to foster cyber resilience with transportation and logistics. Blockchain with the decentralized and tamper-resistant architecture is highlighted [28] as a transformative tool to enhance supply chain transparency and data integrity, while AI and machine learning can enable real-time threat detection and response.

Within U.S. automated logistics and distribution centers specifically, there are high level automation facilities with autonomous guided vehicles (AGVs), robotic picking arms and AI-orchestrated conveyor network presenting threats even through their efficiency. These are widespread in environments like Amazon's 200+ fulfillment centers and Walmart's 15 automated DCs targeted with ransomware which shut down centralized warehouse management systems (WMS), as seen in 2024 incidents that shut down Midwest distribution for days (U.S. Department of Transportation, 2020). Furthermore, IoT sensor networks also create vast surfaces for large-scale attacks for DDoS flooding. Operationally, the repetitive breakdowns such as drift in the calibration of sensors during operations, jamming of conveyor during peak e-commerce surges such as Black Friday in 2025, saw a 15% downtime of U.S warehouses, and algorithm biases in inventory prediction, exposing single-point dependencies and exacerbating regional delays into national supply shortages (Staff Report, 2025). These patterns demand air-gapped cybersecurity, modular robotic redundancies, and human override protocols in order to secure America's logistics backbone against threats.

Primary Threat Vectors

Contemporary U.S. logistics confronts a triad of primary threat vectors in cyber, physical, and operational dimensions, with each surging in intensity amid digital convergence. Cyber threats, in general, and ransomware in particular, have grown in an alarming manner. In 2025 alone, verified attacks on transport and logistics companies have doubled to 283 incidents, with trucking fleets making up 71% of victims as syndicates exploit CISA's Known Exploited Vulnerabilities catalog for remote code execution (Sebastian, 2026). Physical threats manifest in cargo theft surges which have increased from 27% in 2024 to more than $1 billion in losses, making up an average of $202,000 per incident amid organized crime taking advantage of strains in global supply presently (NICB, 2025). In addition, operational risks stem from chronic workforce gaps. The American Transportation Research Institute (ATRI) lists shortages of drivers as the top concern in the industry, and this is based on aging demographics and high turnover, estimating a shortage of 80,000+ deficit in 2025 (McCareins, 2025).

Cascading Interdependencies

These vectors seldom act in isolation. Instead, they produce devastating cascades where cyber breaches trigger halts of operations and physical vulnerabilities. The Colonial Pipeline

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

ransomware attack in 2021 is an example of this. In this attack, the DarkSide ransomware group infiltrated billing systems and triggered precautionary shutdowns that idled the 5,500-mile fuel artery for days. This triggered fuel shortages, panic buying, and a ransom payout of $4.4 million, which resulted in trucking disruptions and exposed billing infrastructure as a chokepoint for physical flows (U.S. Department of Energy, 2021). Such interdependencies have magnifying impacts. North American Electric Reliability Corporations (NERC) 2025 report warns that the exploits in critical infrastructures such as pipelines can cascade down to bulk power systems, reducing situational awareness and resilience (NERC, 2025). Within logistics, ransomware on telematics can spoof GPS data, which allows targeted thefts and multimodal bottlenecks from ports to highways (Sebastian, 2026).

Quantified Impacts - Economic/National Security Toll

The compounded toll of security threats and operational failures in U.S. automated logistics and distribution is reflected in staggering economic losses and national security vulnerabilities, with disruptions acting as multipliers that cascade across critical infrastructure. Aggregate annual costs exceed $20 billion, encompassing theft, cyber extortion, and downtime. For example, ransomware alone inflicted billions in 2025 logistics sector through halted operations, while cargo theft topped $1 billion in the year 2024 year, with projections for further escalation amid tariff induced reshoring strains (NICB, 2025). Additionally, according to analysis by the Government Accountability Office (GAO), there is wider fragility across the supply chain, estimating that the pandemic era bottlenecks cost U.S. manufacturing 230 billion in lost output by 2022 with lingering effects of 2025 from tariffs and cyber events, inflating logistics expenses by 10-15% for 60% of manufacturing firms. This had ripple effects of on essentials (Kali, 2025).

Also, resilience metrics identify downtime multipliers as the true amplifier. A single ransomware breach can idle automated production lines and fleets for days to weeks, with ICS/OT attacks causing two to five times propagation of physical logistics halt, which is seen in fuel shortages post cyber incidents (Kaur, 2025). Nationally, these erode security. DHS categorizes logistics as a critical infrastructure, where disruptions pose risks to the availability of food and fuel. This has interdependencies modeled in NERC, projecting 40% GDP vulnerability from unchecked cascading effects (NERC, 2025). In networks dominated by trucking (72% freight ton-miles) workforce gaps tend to compound this turning long hours into national chokepoints (DOT, 2025).

Prospective Countermeasures

Mitigation requires a multi-level approach combining elements of cybersecurity, operational redundancies, and policy enforcement, that will reduce these effects. CISA's frameworks, such as the 2023 Hardware Bill of Materials (HBOM) for supply chain risk and NIST in aligned vendor assessments are found to be effective. Telecom carriers use them to reduce the propagation of breaches by mapping them by vulnerabilities, adaptable to logistics for telematics vetting (Industrial Cyber, 2023). Additionally, there are proven ops redundancies such as telematics dashboards to enable real-time anomaly detection and route optimization, with the mobile IoT predicting disruptions to reduce delays by 20-30%, through the "predict-prevent-perform" model (Damoov, 2025).

Prospective levers exist within FMCSA's tweaks, mandating crash accountability and resilience auditing to curb operational failures, alongside contingency planning and nearshoring (Corrigan Logistics, 2025)

Threat Vector	Pre-Mitigation (Annual Loss/Downtime)	Post-Mitigation (Reduction)
Ransomware/Cyber	$5-10B / 5-7 days avg.	40-60% / 1-2 days (Industrial Cyber, 2023)
Cargo Theft/Physical	$1B+ / 24-48 hrs per incident	25-35% / <12 hrs (Corrigan Logistics, 2025)
Workforce/ Ops Gaps	$10B+ / Multi-day cascades	30% / Real-time via telematics (Damoov, 2025)

Table 1: Risk Reduction Matrix

Future Considerations

While this review outlines existing vulnerabilities and operational failures in automated logistics and distribution centers along with mitigation tools in the U.S. logistics landscape, evolving dynamics making it necessary to conduct progressive research to strengthen supply chain resiliency against future disruptions. Emerging technologies like predictive analytics powered by AI and the transparency of the blockchain ledger possess a transformative potential. However, their integration risks like adversarial AI attacks spoofing telematics data or quantum computing cracking encryption require rigorous studies tracking efficacy in real-world multimodal networks such as post-2026 autonomous trucking pilots under FMCSA oversight (Whitman, 2025). Progressive research should prioritize the modeling of hybrid threats that is amplified by climate volatility. This includes AI-simulated scenarios of rippling failures from hurricane-crippled ports to nationwide fuel rationing and quantifying ROI for resilience investments as projections highlight $25B+ annual losses by 2030 (PwC, 2025).

Public-private partnerships are an area that need to be explored further, particularly a proposed National Freight Resilience Consortium that would connect DHS/CISA with ATRI and market leaders in an effort to standardize threat rationalism and real-time data sharing protocols. These will fill in the gaps in current siloed responses. Policy research should also assess compulsory adoption of zero trust architectures in ELD systems and incentivize sustainable redundancies such as diversified inland depots, benchmarking against EU's NIS2 Directive outcomes. Ethical dimensions including workforce upskilling for cyber ops fusion roles in the face of ongoing driver shortage are also areas that warrant attention to avoid human error amplifiers.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

Ultimately, future inquiries must move away from reactive toward proactive engagements, leveraging U.S. freight corridors for anticipating and preventing disruptions. This agenda positions logistics not only as economic infrastructure, but increasingly as a national security imperative to ensure adaptive strategies for an era of persistent interconnected risks.

Conclusion

Cyber threats and resilience strategies across global supply chains and transportation networks highlight the critical and evolving nature of cybersecurity risks in these interconnecting systems. As global supply chains and transportation networks continue to digitize, automate and become more interconnected, the importance of cybersecurity and resilience cannot be overstated. A proactive, adaptive and cooperative approach is critical to protect these critical infrastructures from present and evolving cyber threats. Future research and policy need to converge on the standardizing of cyber security standards, to foster innovation in cyber defense technologies, and promote resilience that ensure secure, reliable, and sustainable global logistics and mobility ecosystems.

REFERENCES

1. *Austin-Gabriel, B., Hussain, N. Y., Ige, A. B., Adepoju, P. A., Amoo, O. O., & Afolabi, A. I. (2021). Advancing zero trust architecture with AI and data science for enterprise cybersecurity frameworks. Open Access Research Journal of Engineering and Technology, 1(1), 47-55.*
2. *Bureau of Transportation Statistics (BTS), 2025. U.S. Ton-Miles of Freight (BTS Special Tabulation) (millions). U.S. Department of Transportation. Available at: https://www.bts.gov/content/us-ton-miles-freight*
3. *Casalino, N., Żuchowski, I., Labrinos, N., Munoz Nieto, Á. L., & Martín, J. A. (2019). Digital strategies and organizational performances of SMEs in the age of Coronavirus: balancing digital transformation with an effective business resilience. Queen Mary School of Law Legal Studies Research Paper Forthcoming.*
4. *Corrigan Logistics, 2025. Risk Management in Logistics: Identifying and Mitigating Risks, 6 May. Available at: https://www.corriganlogistics.com/risk-management-in-logistics-identifying-and-mitigating-risks/*
5. *Cottingham & Butler (2025) ATRI releases top 10 trucking industry concerns of 2024. Available at: https://www.cottinghambutler.com/post/atri-releases-top-10-trucking-industry-concerns-of-2024*
6. *Damoov, 2025. Strengthening Supply Chains with Predictive Mobile Telematics: Predict, Prevent, Perform. Available at: https://damoov.com/strengthening-supply-chains-with-predictive-mobile-telematics-predict-prevent-perform/*
7. *Eye Security, 2025. Cybersecurity in transportation and logistics: inside the sector's risks, 17 September. Available at: https://www.eye.security/blog/cybersecurity-in-transportation-and-logistics-inside-the-sectors-risks*
8. *Faith, D. O. (2018). A review of the effect of pricing strategies on the purchase of consumer goods. International Journal of Research in Management, Science & Technology (E-ISSN: 2321-3264) Vol, 2.*
9. *Greenawalt, T., 2024. Amazon has more than 1 million robots that sort, lift, and carry packages – see them in action. About Amazon. Available at: https://www.aboutamazon.com/news/operations/amazon-robotics-robots-fulfillment-center*
10. *Hussain, N.Y., Austin-Gabriel, B., Ige, A.B., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. AI-driven predictive analytics for proactive security and optimization in critical infrastructure systems. Open Access Research Journal of Science and Technology, 2(02), pp.006-015.*
11. *Ike, C.C., Ige, A.B., Oladosu, S.A., Adepoju, P.A., Amoo, O.O. and Afolabi, A.I., 2021. Redefining zero trust architecture in cloud networks: A conceptual shift towards granular, dynamic access control and policy enforcement. Magna Scientia Advanced Research and Reviews, 2(1), pp.074-086.*
12. *Industrial Cyber, 2023. CISA releases HBOM framework for supply chain risk management to help purchasers assess, mitigate risks, 26 September. Available at: https://industrialcyber.co/cisa/cisa-releases-hbom-framework-for-supply-chain-risk-management-to-help-purchasers-assess-mitigate-risks/*
13. *Institute for Supply Management (ISM), 2025. Navigating the Bullwhip Effect: Strategies for Supply Chain Success, 28 November. Available at: https://www.ism.ws/supply-chain/bullwhip-effect/*
14. *Kali, R., Gu, J. and Neuyou, E., 2025. Message in a Bottleneck: Supply Chain Disruptions and Manufacturing Output in the United States. Received 5 December 2024; revised 4 August 2025; accepted 7 August 2025.*
15. *Kaur, S., 2025. How Do Ransomware Attacks Impact Physical Production Lines and Logistics? FBI Support, last updated 4 months ago. Available at: https://fbisupport.com/ransomware-attacks-impact-physical-production-lines-logistics/*
16. *Lusimbo, E. N. (2016). Relationship between financial literacy and the growth of micro and small enterprises in Kenya: A case of Kakamega Central sub-county (Doctoral dissertation, cohred, JKUAT).*
17. *Magoon, M., 2026. How the Railroad Transformed Military Logistics: Why Rail Networks Reshaped Army Size, Strategy, and State Power, 29 January. From Poverty to Progress (Substack). Available at: https://frompovertytoprogress.substack.com/p/how-the-railroad-transformed-military*
18. *McCareins, M., 2025. Is There a Truck Driver Shortage in 2025? 18 November. AltLine. Available at: https://altline.sobanco.com/truck-driver-shortage/*
19. *Mecalux, 2023. Logistics history: origin and development, 1 August. Available at: https://www.mecalux.com/blog/logistics-history-origin*
20. *Meyer, E. L., Apeh, O. O., & Overen, O. K. (2020). Electrical and meteorological data acquisition system of a commercial and domestic microgrid for monitoring pv parameters. Applied Sciences, 10(24), 9092.*
21. *National Insurance Crime Bureau (NICB), 2025. NICB Warns of Increased Cargo Theft in 2025. OAK BROOK, IL, 25 June. Available at: https://www.nicb.org/news/news-releases/nicb-warns-increased-cargo-theft-2025*
22. *Observatoire-Janus, 2025. The Hanseatic League: logistics as a tool of power (1159–1669). Available at: https://observatoire-janus.com/en/the-hanseatic-league-logistics-as-a-tool-of-power-1159-1669*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 12| Issue: 3| March2026|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2026: 8.753 || ISI Value: 1.188

23. *Ogunsola, O., Adikorley, I. J. N., & Opoku, J. A. (2025). Mitigating cognitive load in supply chain decision-making: An AI-driven framework for enhanced operational efficiency. International Journal For Multidisciplinary Research (IJFMR), 7(6), 1–12. https://www.ijfmr.com/papers/2025/6/61809.pdf*
24. *Ogunsola, O., Serh, L. Z. and Hutchful, N. " Adaptive AI Systems for Intelligent Decision Optimization in Supply Chain Management: A Machine Learning Approach." Sarcouncil Journal of Engineering and Computer Sciences 4.12 (2025): pp 10-18.*
25. *Okolie, C.I., Hamza, O., Eweje, A., Collins, A., Babatunde, G.O., & Ubamadu, B.C., 2021. Leveraging Digital Transformation and Business Analysis to Improve Healthcare Provider Portal. ICONIC RESEARCH AND ENGINEERING JOURNALS, 4(10), pp.253-257.*
26. *Oladosu, S.A., Ike, C.C., Adepoju, P.A., Afolabi, A.I., Ige, A.B. and Amoo, O.O., 2021. The future of SD-WAN: A conceptual evolution from traditional WAN to autonomous, self-healing network systems. Magna Scientia Advanced Research and Reviews.*
27. *PricewaterhouseCoopers (PwC), 2025. Transportation & Logistics 2030: Volume 4 – Securing the Supply Chain. Available at: https://www.pwc.com/gr/en/publications/assets/transportation-logistics-2030-vol4.pdf*
28. *PricewaterhouseCoopers (PwC), 2025. Transportation & Logistics 2030: Volume 4 – Securing the Supply Chain. Available at: https://www.pwc.com/gr/en/publications/assets/transportation-logistics-2030-vol4.pdf*
29. *Reuter, D., 2024. The math is looking good for Walmart's automated warehouses. Business Insider, 13 June. Available at: https://africa.businessinsider.com/retail/the-math-is-looking-good-for-walmarts-automated-warehouses/1ngj29w*
30. *Sebastian, N., 2026. Ransomware hits on logistics double in 2025, Cyble report reveals, 9 January. ITLN. Available at: https://www.itln.in/supply-chain/ransomware-hits-on-logistics-double-in-2025-cyble-report-reveals-1357760*
31. *Snow, C., 2025. CISA ICS Advisories, Additional Alerts, Updates, and Bulletins – February 20, 2025. WaterISAC, 20 February. Available at: https://www.waterisac.org/tlpclear-cisa-ics-advisories-additional-alerts-updates-and-bulletins-february-20-2025*
32. *Staff Report, 2025. DHL report: Supply chains face ongoing disruption through 2030. 19 November. Available at:*
33. *https://www.dbbnwa.com/articles/dhl-report-supply-chains-face-ongoing-disruption-through-2030/*
34. *U.S. Department of Energy, 2021. Colonial Pipeline Cyber Incident. Energy.gov. Available at: https://www.energy.gov/ceser/colonial-pipeline-cyber-incident*
35. *U.S. Department of Transportation, 2020. National Freight Strategic Plan. Washington, DC: U.S. Department of Transportation. Available at: https://www.transportation.gov/sites/dot.gov/files/2020-09/NFSP_fullplan_508.pdf*
36. *Whitman, S., 2025. Securing Autonomous Supply Chains: AI Logistics Cybersecurity 2025, 25 October. Debales.ai. Available at: https://debales.ai/blog/securing-autonomous-supply-chains-ai-logistics-cybersecurity-2025*
37. *Whitman, S., 2025. Securing Autonomous Supply Chains: AI Logistics Cybersecurity 2025, 25 October. Debales.ai. Available at: https://debales.ai/blog/securing-autonomous-supply-chains-ai-logistics-cybersecurity-2025*