AI AND TECHNOLOGY-ENABLED SUPPLY CHAIN SECURITY

Goh, P. G. [(1)], Teo, H. L. J. [(2)], Lim, R. S. [(3)], Syahirah, A [(4)]

(1) Centre for Maritime Studies, National University of Singapore, Singapore, bizgpg@nus.edu.sg

(2) Centre for Maritime Studies, National University of Singapore, Singapore, jteo@nus.edu.sg

(3) Centre for Maritime Studies, National University of Singapore, Singapore, lrs@nus.edu.sg

(4) Centre for Maritime Studies, National University of Singapore, Singapore, muya@nus.edu.sg

Keywords: Supply Chain, Security, Fraud, AI, Counterfeit Detection.

ABSTRACT: Supply chain security encompasses different areas, such as damage, theft, fraud, and counterfeits. Cargo security has always been an important factor in international trade, especially with ongoing maritime and supply chain disruptions. In consumer products, companies and consumers also have to deal with fake products and fake vendors. We will look at case studies and examples of how AI can be used in cargo tracking and routing, as well as the use of AI to detect fraud and counterfeits.

1. INTRODUCTION

The contemporary global supply chain landscape is highly susceptible to a wide array of disruptions such as natural disasters, geopolitical tensions, cyberattacks, and pandemics [1]. These disruptions, coupled with the increasing complexity of supply networks, pose significant challenges in achieving resilient and secure operations.

In recent years, the use of advanced, Industry 4.0 technologies such as robotics, data analytics, 3D printing, Internet of Things, blockchain, and Artificial Intelligence (AI), offers a transformative opportunity to bolster supply chain resilience and security as noted by several studies [2, 3, 4, 5].

Supply chain security is "the part of the supply chain management that focuses on the risk management of external suppliers, vendors, logistics, and transportation" by identifying, analysing, and mitigating risks associated with outside organisations as part of the company's supply chain. It includes both physical security – theft, piracy, counterfeiting, sabotage, terrorism, etc; and cybersecurity – malware attacks, piracy, unauthorised access, etc [6]. Amidst the increased digitalisation, the threat surface to cybersecurity risks has increased significantly. According to BlueVoyant's survey in 2023, the mean number of cyber breaches in their respondents' supply chain that negatively impacted their organisations increased by 26% - from 3.29 in 2022 to 4.16 in 2023. This is despite 47% of the respondents monitoring their supply chain vendors for cyber risk monthly or more, and 44% of the respondents briefing their senior management at least monthly [7]. IBM reported that the average cost of a data breach in 2024 has increased year-on-year by 10% to USD4.88m with a mean containment time of 258 days, with cost savings of USD2.2m arising with the use of AI in prevention [8]. Aside from cybersecurity, issues in supply chain security often arise in the physical supply chain, and with increasing digitalisation, the ability to use data and AI to better secure the physical supply chain has also improved.

This paper examines the role of AI and technology in strengthening the security of supply chains and integrates various frameworks into a comprehensive model utilising AI to bolster physical supply

chain security while addressing the interconnected challenges of modern supply chain systems. With industry examples, it demonstrates how AI and analytics form a crucial link between physical and cyber supply chains, leading to enhanced security outcomes and improved overall performance.

2. BACKGROUND

2.1 Supply Chain Security

Supply chain security can be defined by the actions and polices undertaken by stakeholders to protect the supply chain with the objective of being free from danger of criminal activities such as piracy, theft, counterfeiting, smuggling, terrorism, etc [9]. Supply chain security management involves integrating traditional security principles into the holistic governance of supply chains, particularly in a global context [10], continually adjusting as criminal methods change, and protecting the weakest link due to the interconnected nature of supply chains [9]. Supply chain security measures can be preventive or corrective [11], with preventive measures consisting of physical and non-physical security, while corrective measures focus on minimising the adverse effects caused by security-related risks.
Resiliency is "the ability of the organisation to respond should that adverse event occur". Supply chain resiliency is to "take actions before a disruption to ensure operational continuity after a disruption", "the expected outcome of proactive Supply Chain Risk Management and Supply Chain Security", with metrics of "Time To Recover (TTR) and Time To Survive (TTS)" [12]. Supply chain resilience refers to the ability of a supply chain to adapt to and recover from disruptions. It includes the capacity to anticipate risks, minimise operational downtime, and maintain continuity in the flow of goods and services. Key factors contributing to resilience include flexibility, redundancy, agility, and visibility. Deloitte's Supply Chain resilience report defines visibility, flexibility, collaboration and control as the four main pillars of resilience [13]. Supply chain security is the "application of policies, procedures, processes, and technologies to ensure the security, integrity, and uninterrupted flow of products while moving through the supply line" [14]. As such, supply chain security falls within the broader context of supply chain resilience, which aims at being responsive and agile to cope with disruptions and return to normal operations in the shortest possible time [15, 16, 17]. According to Hinsta *et al.* [10], supply chain security management usually falls into these five categories: cargo management, facility management, information management, human resource management, and company management systems. Company management systems would involve the evaluation of security in both their internal processes as well as external vendors and customers.

With the recent global uncertainty in geo-politics and operating environment, the global supply chains had started to transit from efficient supply chains to resilient supply chains, especially drawing lessons from the COVID-19 pandemic. This means a shift from lean to agile, specialised to flexible, consolidation to collaboration, reactive to predictive and enterprise-focused to network-focused. While efficient supply chains could be addressed using techniques such as six-sigma, Kaisen, etc, resilient supply chains involve proactive visibility, predictivity, flexibility in a much more concerted efforts through the supply chain network [18].

Supply chain security, in contrast, involves safeguarding the entire chain from physical, cyber, and information security threats. This includes protecting against cyberattacks, intellectual property theft, fraud, and supply chain sabotage [6]. As threats, both cyber and physical, to supply chains increase, ensuring robust security mechanisms is becoming as important as resiliency in mitigating potential risks.

Figure 1: Characteristics of Efficient supply chains versus Resilient supply chain (Deloitte [18]).

Counterfeiting entails replacing luxury goods with inferior items, often disguised through reused, authentic-looking, or imitation packaging bearing false branding [19]. In 2022, the size of the counterfeit market (and therefore loss to the brands and manufacturers) was estimated $1.1 trillion, and is expected to hit $1.79 trillion in 2030 [20]. These counterfeits also includes products in critical application: the World Health Organization estimates that 1 in 10 medical products in low- and middle-income countries is substandard or falsified [21], while the Semiconductor Industry Association in the US estimated that 15% of spare parts semiconductors in US supply chains are counterfeits [22].

The Center for Strategic & International Studies (CSIS) commented that the global economy still depend on maritime supply chains, but "face a variety of threats both present and future stemming from geopolitical tensions and environmental factors" [23]. While the International Chamber of Commerce – Commercial Crime Services' International Maritime Bureau (IMB) reported a decrease in maritime piracy incidents in 2024, it is expected that the global turmoil would alter shipping routes, especially in areas of conflict [24]. Ukraine, world's largest exporter of sunflower oil (50% of world's), the third largest of barley (18%), the fourth largest of maize (16%) and the fifth largest of wheat (12%) – dropped its exports by more than 90% [25]. Even though Ukraine now exports through the humanitarian corridor, its agriculture production had decreased [26]. The Houthi attacks at the Red Sea had raised the attention of ship owners and many had chosen to route longer via the Cape of Good Hope [27] with the traffic in Suez Canal adversely affected as a result [28]. The supply chain continues to remain vulnerable and at mercy of these conflicts, and given the scale of these losses, addressing security has become paramount.

2.2 Digitalisation in Supply Chain

The disruptions brought about by Covid-19 have made adoption of digitalisation and Industry 4.0 technologies such as AI, blockchain, data analytics, Internet of Things (IOT) and 3D printing more prevalent, allowing companies to react more quickly to changes in supply and demand [29, 30]. In today's complex operating environment, different technologies need to come together in an integrated and seamless way [31, 32].

Digitisation in turn has built up the data upon which machine learning and AI can be applied. Fernando, Al-Madani, and Shaharudin [30] found that blockchain, AI and machine learning were among the most effective technologies in mitigating the disruptions from Covid-19, while Vishwakarma, *et al.* [33] point to the potential transformative of AI in improving efficiency, sustainability and resilience.

The use of AI and analytics lies at the intersection of the physical supply chain and the cyber supply chain, on data obtained through IT systems and sensors in various functions of sales, logistics, manufacturing and procurement along the supply chain [34].

3. AI IN SUPPLY CHAIN SECURITY

AI lies on top of a layer of technologies that span the entire supply chain, with the analysis of multiple sources of data from manufacturing, inventory management, transportation, point of sales, etc enabling supply chains that are smarter, more efficient and sustainable.

AI can significantly augment both preventive and corrective measures used to enhance supply chain management security. Through the analysis of big data from various sources ranging from shipping data to video feed to the monitoring of crime data, AI can detect anomalies and potential threats in the supply chain by identifying irregular patterns and behaviours of the operators or of the physical goods on the preventive end, allowing for prompt intervention. On the corrective end, AI-powered systems can swiftly respond to security breaches or disruptions by automating responses, rerouting shipments, or activating contingency plans with minimal human intervention, thus minimising downtime and losses. By combining AI's ability to analyse large volumes of data quickly with real-time responsiveness, organisations can strengthen their supply chain resilience and ensure smoother operations in the face of potential security threats.

Combining and adapting the various frameworks on supply chain security, supply chain resilience, and use of AI and data analytics [11, 32, 34, 35] we may envision the use of AI in supply chain security as:

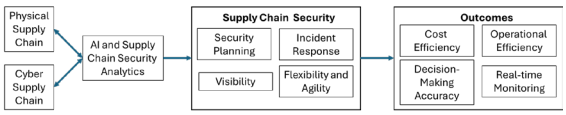

Figure 2: AI in Supply Chain Security.

4. EXAMPLES OF THE USE OF AI IN SUPPLY CHAIN SECURITY

4.1 Transported Asset Protection Association (TAPA)

Formed in 1997 with the mission to minimise cargo losses from the supply chain, the Transported Asset Protection Association (TAPA) is a coalition of supply chain security stakeholders - manufacturers, shippers, carriers, insurers, service providers, law enforcement, and government agencies in the Americas, Asia Pacific and Europe, Middle East and Asia (EMEA) regions [36].

In 2022, TAPA launched the TAPA Intelligence System (TIS), a risk management and loss prevention tool which provides members with information on cargo crimes as well as information on facilities, trucking operators and secure parking locations which meet the TAPA Security Standards [37].

The TIS is a tailored supply resilience intelligence tool that helps companies understand the impact of cargo theft losses on individual routings, in local, regionally and international markets, based on cargo crime incidents recorded by the Association.

Through TIS's Incident Reporting, members and the public can submit anonymised information on cargo crime incidences, whilst members are able to access the collective database of crime incidences

through the Data Explorer and Cargo Crime modules. Information on the location and specifications of TAPA-certified sites are also provided. Various types of incidents are captured, as well as security certification levels of facilities (FSR), transportation (TSR), and parking locations (PSR).

TAPA members utilise the TIS to protect the security of their employees, assets, and cargoes by acquiring knowledge of geographically riskier areas where cargo crime groups are most active. This enables companies to reduce their risks by planning their supply chains to avoid known 'hotspots' for criminal attacks.

This information can be exported for further analysis or for use in security programmes. Companies can also use these data for risk assessment and for insurance to build into their underwriting and actuarial calculations. They are also better equipped to do risk mitigation using Smart Route Planning module (route-based insurance) to avoid hotspots, and leverage on TAPA-certified partners for their warehouse and transportation services (Figure 3).

Figure 3: Visualisation of Incident and Certified Facility Locations [38].

McKinsey mentions in 2021 that "successfully implementing AI-enabled supply-chain management has enabled early adopters to improve logistics costs by 15 percent, inventory levels by 35 percent, and service levels by 65 percent, compared with slower-moving competitors." [39]. With the increased implementation of AI in supply chain over the years, the collective supply chain will achieve more improvements and derive more value from the use of these technologies.

AI can be harnessed to analyse a multitude of data sources such as historical data, market conditions, weather patterns, and geopolitical events, to identify potential supply chain risks as noted by Ernst & Young [40]. Generative AI adds user friendliness to end-user engagement allowing for tech-enabled planning efforts across the whole decision chain and could be prompted to "produce risk assessments, scenario simulations and mitigation strategies on demand to help planners manage and mitigate the risks proactively".

In the Smart Route Planning module within the TIS, AI plays a vital role in optimising analysing historical data and predicting potential risks along transportation routes. AI leverages a rich set of historical crime data such as theft, hijacking, and vandalism, and identifying patterns and trends. AI algorithms can process large volumes of historical data and pinpoint regions or routes that are frequently targeted by criminals. For example, AI can flag specific areas with a high frequency of cargo thefts, allowing businesses to adjust their logistics operations and reroute shipments away from these hotspots. By factoring in data on crime rates, the security status of parking areas, and the performance of various transport operators, AI helps businesses identify safer, lower-risk routes, and optimise their planning processes. This proactive approach strengthens resilience by minimising the likelihood of encountering security issues during transportation.

Other than crime patterns, other security-related factors can be considered by AI when recommending routes such as security ratings of transportation facilities, parking areas, and warehouses that meet TAPA Standards. By ensuring shipments pass through secure, TAPA-certified facilities, businesses can minimise the risk of cargo theft during transit and ensure better protection for goods in storage. AI's ability to integrate this data into the route planning process helps companies maintain high levels of security throughout the entire journey, from origin to destination, and avoid regions with fewer security measures in place.

One of the most powerful ways that TIS contributes to the resilience of supply chains is its quantification of risk. In a constantly evolving global supply chain landscape, businesses need clear, actionable data to understand their vulnerabilities and assess the level of risk they face. TIS's ability to convert crime incident data into quantifiable metrics is a critical enabler of supply chain resilience, helping companies make data-driven decisions that strengthen their security posture and prepare them for future challenges.

By tracking and measuring trends in cargo crime over time, TIS helps businesses identify areas where risk levels are changing (increasing or decreasing). This quantification allows companies to gauge their overall exposure to risk, providing them with a clearer picture of where potential disruptions may arise. Businesses can use this data to adjust their supply chain strategies and bolster their resilience. For example, if a certain region or route shows an upward trend in theft incidents, companies can proactively implement measures such as strengthening security, partnering with TAPA-certified providers, or exploring alternative routes. Quantifying risk in this way makes businesses more agile, adaptable and better able to maintain the continuity of their operations, even when external threats escalate.

Quantification plays a vital role in enhancing a company's resilience by improving its approach to risk management and insurance. With clearer, more accurate data on cargo theft incidents, businesses can build stronger, customised risk profiles for their supply chains. This can lead to more competitive insurance premiums and better coverage terms, ensuring that companies are financially protected in the event of a loss. More importantly, by integrating the insights from TIS into their security strategies, companies demonstrate a proactive approach to risk mitigation, which can further reduce the likelihood of loss and foster resilience within the supply chain. With better access to data on past incidents and risk factors, companies are empowered in a stronger position to negotiate terms with insurers and to build more resilient, secure operations.

Another key benefit of the TIS in terms of quantification is its impact on long-term strategic planning. As businesses gather more data on cargo crime patterns, they are better equipped to identify systemic risks and vulnerabilities within their operations. The ability to measure and track risk levels over time allows companies to refine their security practices and invest in measures that directly contribute to resilience. This might mean investing in secure parking locations, collaborating with trusted partners, or deploying advanced tracking and monitoring technologies to ensure the safety of goods in transit. Through continuous measurement and assessment, businesses can better make informed decisions to build more resilient supply chains capable of weathering disruptions from crime, natural disasters, and/or other external factors.

Ultimately, the ability to quantify risks with precision strengthens not only the immediate security of cargo but also the resilience of the entire supply chain. As businesses can more accurately assess their vulnerabilities, they can take pre-emptive actions to safeguard their assets, ensuring that they remain operationally resilient even when faced with significant challenges. With data-backed insights that allow for rapid response and long-term planning, companies are empowered to bolster the resilience of their supply chains in a dynamic, data-driven way.

4.2 Supply Chain Security in Consumer Goods / E-Commerce

E-commerce has seen rapid growth and is projected to reach revenue of US$4,791b in 2025. While the rate of growth has slowed in recent years since after the COVID-19 pandemic, it is expected to continue growing, with a CAGR of 7.83% as the user penetration across all markets continues to grow [41].

The relative ease of setting up e-commerce websites and the proliferation of online transactions, products, and marketplace vendors has led to an increase in fraudulent transactions due to the ease of fraudulent products infiltrating into the supply chain via different forms, including the use of influencers, fake reviews, counterfeit products, and scam merchants which create fake listings to get payment [42].

The e-commerce expansion led to a growing number of packages and consequently, heightened pressure on postal and courier services. For customs agencies, monitoring these shipments became challenging due to the enormous volume with the declaration and inspection of shipments becoming progressively harder. Furthermore, the pandemic led many IP owners to focus on tasks other than brand protection, unintentionally enabling counterfeit activities to thrive [43].

Counterfeit and pirated products have been a perennial issue in global trade, reaching an estimated 3.3% of the world trade in 2016 [44]. OECD [42] found that the imports of these products increased together with the prevalence of e-commerce with small parcels being the main mode of distribution.

Given the sheer volume of transactions, the use of AI is critical in automating the process of sifting through millions of items to identify potential fraud. Machine learning helps to identify unusual vendors and transactions, replicating at vast scale what human does in flagging out potential issues, and more effectively without having to massively and unrealistically increase the manpower to verify transactions.

Fake products can potentially be identified through scanning their various physical properties for discrepancies, and AI enables the timely analysis of large numbers of data points. In the consumer space, apps such as Entrupy [45] and Authentique Verify [46] allow consumers to take pictures of products using their smart phone, which would then do a verification check on their authenticity. Other solutions leverage on AI analysis of smells to authenticate products such as sneakers via their scent profiles [47].

4.3 Toll

The Toll Smart Warehouse and Transportation Security System is designed to enhance safety and security both outside and within the warehouse environment itself. This system leverages on AI technology and analytics to monitor and manage various aspects of security operations efficiently.

Working with partners Visium and Rapid Global, Toll utilises smart cameras with key AI checkpoints integrated into the operations to maintain control over access and staff compliance. These include license plate and facial recognition to verify that only authorised vehicles and personnel enter the premises. Drivers and workers can be inducted in advance through an app that allows them to provide their photos so that onsite verification and entry will be seamless.

The system also includes real-time dashboards, reports, and alerts (Figure 4 Top). Trigger alerts can be set whenever individuals check in or exit the facility, when a vehicle exceeds its permitted dwell time, or if no workers have checked in by a specific time.

To promote safety and reduce the risk of accidents, camera scans also provide warning alerts when workers are not wearing the appropriate personal protective equipment (PPE), as well as when there is close proximity between moving forklifts and workers risking potential contact (Figure 4 Bottom)

The implementation of the system in Toll was done in stages. After installation of the cameras and hardware, time was given for the contractors and workers to be progressively inducted into the system, before compliance was fully enforced. At various stages, it was important to help create awareness amongst the users, so that it became part of the standard operating procedures. Thereafter, with the

system running at the steady state, the company was able obtain real-time insight and reports and focus on exception management. Compliance rate significantly increased from 40% to 95% as a result.

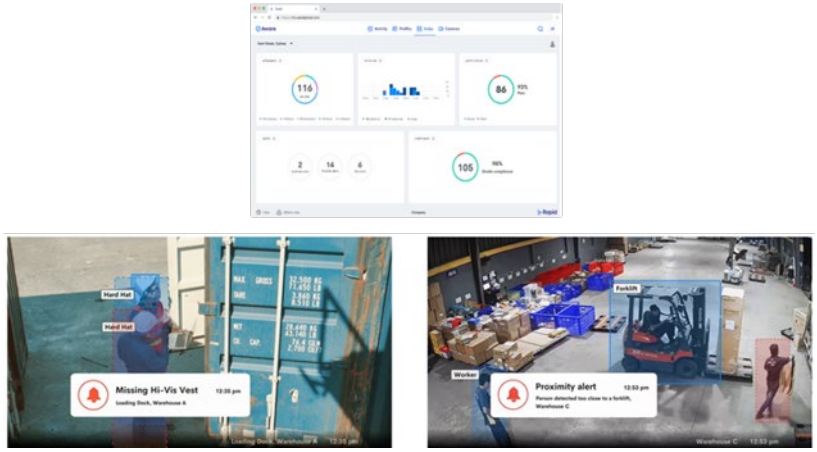

Figure 4: Real-time Dashboard of Key Indicators (top). Missing PPE and Forklift Proximity Alert (bottom) (Source: Toll Group)

4.4 Using AIS Data for Supply Chain Security

The Automatic Identification System (AIS) is crucial for enhancing maritime safety, security, and navigation. Initially developed as a tool for ships to avoid collision, AIS has since evolved into broader applications such as tracking, intelligent operations, and transportation planning [48, 49, 50]. However, manipulation of AIS technology has risen, especially in the context of deceptive shipping [51]. Vessels have deliberately disabled or tampered with their AIS transponders to avoid detection, carry out illicit activities, or bypass sanctions. These practices significantly threaten maritime safety and pose critical risks to global supply chain security in many ways [52]. For instance, illegal ship-to-ship transfers and conducting improper procedures endanger the environment and increase the potential for oil spills. Allianz [53] reported that shadow tankers turning off their AIS transponders concealing their identity have been involved in at least fifty incidents including fires, engine failures, collisions, loss of steerage, and oil spills.

Historically, terrestrial networks and satellite AIS encountered several technical limitations, such as geographical coverage issues. These limitations allowed many actors to use them as reasons for the inaccurate reporting of their AIS messages. Thereafter, vessels were outfitted with receivers to counter these limitations. However, due to such developments, dark shipping tactics also evolved to take on more sophisticated methods of AIS manipulation [51]. For instance, a dark vessel would switch off its transponder at the beginning of the operation and back on at the end, resulting in a period of absence within the AIS, also commonly referred to as "AIS gaps".

Various digital countermeasures in the realm of artificial intelligence have been proposed, including SEA.AI and MHI AIRIS. SEA.AI utilises AI and machine vision technology to identify potential collision threats in the short to medium range, regardless of the time of day and can identify larger vessels not fitted with AIS up to a range of 7.5km, smaller craft up to 3km, and potentially hazardous objects up to 700m away [54]. AIRIS, or Artificial Intelligence Retraining In Space, comprises an Earth-observation camera and an AI-equipped data processor. It deploys its AI to detect targets such as dark

ships in a time-efficient manner compared to traditional and manual methods of identifying covert ships [55]. and can automatically process the required data for identification and without depending on AIS.

To provide an overview of the challenges associated with AIS disabling or manipulation, the MAritime Digital Efficiency (MADE) research programme at the Centre for Maritime Studies, National University of Singapore, is conducting a study to analyse the cases involving such practices. One project under this initiative addressed the difficulty in creating vessel trajectories due to unreliable or inaccurate AIS messages by introducing a novel clustering algorithm to enhance maritime traffic flow visualisation while another project builds on this finding and proposes an improved visualisation of the movement of shipping routes over time during periods of AIS disruption.

5. DISCUSSION

The above examples around tracking, monitoring and identification of security in global supply chains, shipping, warehousing and distribution, and e-commerce retail, show that AI can be a promising tool in enhancing supply chain resilience and security, building on top of the data feed that they gather from their ongoing operations. The automation and aggregation of this data gathering also makes the use of AI more effective over time. The use of AI can be analysed using the framework in Figure 2.

In the case of TAPA, it can be seen that AI helps in improving their decision making by quantifying risks and providing predictive capabilities to help businesses stay ahead of emerging threats. This helps businesses to make informed decisions about resource allocation, insurance, and security investments, and thereby also improves their cost and operational efficiency.

The use of AI in warehouse security for Toll also helps in improving cost and operational efficiency, while enabling real-time monitoring in identifying security risks and also operational non-compliance.

In the case of e-commerce, AI allows for the automation of verification of vast number of products along the whole supply chain enhancing cost and operational efficiency. End-users are also enabled to verify the products bought, enhancing visibility, accuracy and confidence in the distribution channels.

Similarly, AI provides alternatives to manipulation of AIS and boost safety and security through enhancing the visibility of the ship, and the supply chain, allowing for real-time monitoring, operational efficiency and better decision-making accuracy by all the stakeholder in the vicinity and beyond.

Despite the promising benefits of AI in enhancing supply chain resilience and security, several challenges must be addressed. Effective AI models require access to high-quality data from multiple sources [56]. Integrating data from diverse systems across the supply chain can be complex and time-consuming. While AI enhances security, it also introduces new vulnerabilities. The reliance on AI systems for decision-making raises concerns about the integrity of these systems and the potential for cyberattacks targeting AI models themselves [57]. Data privacy is also an important consideration in the exchange of information across businesses in the supply chain and ensuring that there are benefits to the various parties. Implementing AI and other advanced technologies can require significant upfront investment, and smaller companies may face challenges in adopting them.

6. CONCLUSION

AI and technology-enabled solutions are transforming the way supply chains manage risk, resilience, and security. From predictive analytics (reactive) to real-time monitoring and enhanced cybersecurity (proactive), AI technologies provide a powerful toolkit for building more agile, resilient, and secure supply chains. While challenges remain in terms of data integration, cost, and cybersecurity, the benefits of AI in enabling faster responses to disruptions, enhancing risk management, and improving security

make it an indispensable tool for modern supply chain operations. As technology continues to evolve, AI and related technologies will play a pivotal role in shaping the future of resilient and secure supply chains.

The future of AI in supply chain resilience and security is promising. Advancements in quantum computing and AI-driven decision-making algorithms will further enhance predictive capabilities and optimisation. Additionally, the integration of 5G technology with AI can significantly improve real-time communication, further improving supply chain monitoring and decision-making.

The increasing emphasis on sustainability will also drive AI adoption, with AI technologies being leveraged to optimise resource use, reduce carbon footprints, and enhance circular economy initiatives. Moreover, AI-driven innovations such as autonomous vehicles, drones, and robotic process automation will continue to shape the future of supply chain operations. The overall supply chain will reap absolute benefits and advantages when all stakeholders are fully exploiting AI.

7. ACKNOWLEDGMENTS

We sincerely thank TAPA and Toll Group for their insights and examples used in this paper.

8. REFERENCES

[1] Kleindorfer, Paul R., and Germaine H. Saad. 2005. "Managing Disruption Risks in Supply Chains." *PRODUCTION AND OPERATIONS MANAGEMENT* 53-68. https://doi.org/10.1111/j.1937-5956.2005.tb00009.x.

[2] Yang, M, M Fu, and Z Zhang. 2021. "The adoption of digital technologies in supply chains: drivers, process and impact." *Technological Forecasting & Social Change.* https://doi.org/10.1016/j.techfore.2021.120795.

[3] Zouari, D, S Ruel, and L Viale. 2020. "Does digitalising the supply chain contribute to its resilience?" *International Journal of Physical Distribution & Logistics Management.* https://doi.org/10.1108/IJPDLM-01-2020-0038.

[4] Zhao, N, J Hong, and K H Lau. 2023. "Impact of supply chain digitalization on supply chain resilience and performance: A multi-mediation model." *International Journal of Production Economics.* https://doi.org/10.1016/j.ijpe.2023.108817.

[5] Weking, J, M Stocker, M Kowalkiewicz, M Bohm, and H Krcmar. 2020. "Leveraging industry 4.0 – A business model pattern framework." *International Journal of Production Economics.* https://doi.org/10.1016/j.ijpe.2019.107588.

[6] Hewlett Packard Enterprise. 2025. *Supply Chain Security.* https://www.hpe.com/sg/en/what-is/supply-chain-security.html.

[7] BlueVoyant. 2023. "The State of Supply Chain Defense Annual Global Insights Report."

[8] IBM. 2024. "Cost of a Data Breach Report."

[9] Jażdżewska-Gutta, M, and P Borkowski. 2022. "As strong as the weakest link. Transport and supply chain security." *Transport Reviews* 42(6): 762-783. https://doi.org/10.1080/01441647.2022.2056656.

[10] Hinsta, J, X Gutierrez, P Wieser, and A-P Hameri. 2009. "Supply Chain Security Management: an overview." *International Journal of Logistics Systems & Management* 5 No. 3-4: 344-355. https://doi.org/10.1504/IJLSM.2009.022501.

[11] Zailani, S H, K S Subramaniam, M Iranmanesh, and M R Shaharudin. 2015. "The impact of supply chain security practices on security operational performance among logistics service providers in an emerging economy: Security culture as moderator." *International Journal of Physical Distribution & Logistics Management* 45(7): 652-673. https://doi.org/10.1108/IJPDLM-12-2013-0286.

[12] Defense Acquisition University. 2025. *Supply Chain Resiliency (SCR).* https://www.dau.edu/acquipedia-article/supply-chain-resiliency-scr.

[13] Deloitte. 2024. *Building Resilient Supply Chains: A Multi-dimensional Approach.* https://www2.deloitte.com/dk/da/pages/strategy-operations/articles/Building-Resilient-Supply-Chains-A-Multi-dimensional-Approach.html.

[14] Defense Acquisition University. 2025. *Supply Chain Security.* https://www.dau.edu/glossary/supply-chain-security.

[15] Christopher, M, and H Peck. 2004. "Building the Resilient Supply Chain." *The International Journal of Logistics Management* 15(2): 1-14. https://doi.org/10.1108/09574090410700275.

[16] Ralston, P, and J Blackhurst. 2020. "Industry 4.0 and resilience in the supply chain: a driver of capability enhancement or capability loss?" *International Journal of Production Research* 5006-5019. https://doi.org/10.1080/00207543.2020.1736724.

[17] Belhadi, A, S Kamble, S Fosso Wamba, and M M Queiroz. 2022. "Building supply-chain resilience: an artificial intelligence-based technique and decision-making framework." *International Journal of Production Research* 4487-4507. https://doi.org/10.1080/00207543.2021.1950935.

[18] Deloitte. 2023. "Supply Chain Resilience."

[19] de Boissieu, E, G Kondrateva, P Baudier, and C Ammi. 2021. "The use of blockchain in the luxury industry: supply chains and the traceability of goods." *Journal of Enterprise Information Management.* https://doi.org/10.1108/JEIM-11-2020-0471.

[20] Corsearch. 2024. *Trade in Counterfeit Goods Market Set To Reach $1.79 Trillion in 2030.* 05 15. https://corsearch.com/about/press-releases/trade-in-counterfeit-goods-market-set-to-reach-1-79-trillion-in-2030/.

[21] World Health Organization. 2024. *Substandard and falsified medical products.* 12 03. https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products.

[22] Semiconductor Industry Association. 2018. "Detecting and Removing Counterfeit Semiconductors in the U.S. Supply Chain."

[23] Center for Strategic & International Studies. 2024. *The State of Maritime Supply-Chain Threats.* 11 04. https://www.csis.org/analysis/state-maritime-supply-chain-threats.

[24] ICC International Maritime Bureau. 2025. "PIRACY AND ARMED ROBBERY REPORT FOR THE PERIOD 1 January – 31 December 2024." London.

[25] European Council. 2024. *How the Russian invasion of Ukraine has further aggravated the global food crisis.* 01 27. https://www.consilium.europa.eu/en/infographics/how-the-russian-invasion-of-ukraine-has-further-aggravated-the-global-food-crisis/.

[26] International Information Group. 2024. *Ukraine exports 55 mln tonnes of cargo via Black Sea corridor - ministry.* 06 27. https://interfax.com/newsroom/top-stories/103797/.

[27] Armed Conflict Location & Event Data. 2025. *Red Sea Attacks: Interactive Map.* https://acleddata.com/yemen-conflict-observatory/red-sea-attacks-dashboard/.

[28] International Monetary Fund. 2025. *Port Monitor Suez Canal.* https://portwatch.imf.org/pages/chokepoint1.

[29] Shahzadi, G, F Jia, L Chen, and A John. 2024. "AI adoption in supply chain management: a systematic literature review." *Journal of Manufacturing Technology Management* 35(6): 1125-1150. http://dx.doi.org/10.1108/JMTM-09-2023-0431.

[30] Fernando, Y, M Al-Madani, and M S Shaharudin. 2023. "COVID-19 and global supply chain risks mitigation: systematic review using a scientometric technique." *Journal of Science and Technology Policy Management* 6: 1665-1690. http://dx.doi.org/10.1108/JSTPM-01-2022-0013.

[31] Singh, D, A Sharma, R K Singh, and P S Rana. 2024. "Augmenting supply chain resilience through AI and big data." *Business Process Management Journal.* https://doi.org/10.1108/BPMJ-04-2024-0260.

[32] Raid, M, M Naimi, and C Okar. 2024. "Enhancing Supply Chain Resilience Through Artificial Intelligence: Developing a Comprehensive Conceptual Framework for AI Implementation and Supply Chain Optimization." *Logistics* 8(4): 111. https://doi.org/10.3390/logistics8040111.

[33] Vishwakarma, L P, Singh, R K, R Mishra, and M Venkatesh. 2024. "Exploring the motivations behind artificial intelligence adoption for building resilient supply chains: a systematic literature review and

future research agenda." *Journal of Enterprise Information Management* 37(4): 1374-1398. https://doi.org/10.1108/JEIM-11-2023-0606.

[34] Ivanov, D, A Dolgui, and B Sokolov. 2019. "The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics." *International Journal of Production Research* 57(3): 829-846. https://doi.org/10.1080/00207543.2018.1488086.

[35] Ababou, M. 2024. "Conceptual framework of Artificial Intelligence Integration within Supply Chain." *Revue Internationale De La Recherche Scientifique (Revue-IRS)* 2(3): 792-804. doi:https://doi.org/10.5281/zenodo.11191146.

[36] Transported Asset Protection Association. 2024. *TAPA.* https://www.tapaonline.org/.

[37] Transported Asset Protection Association. 2025. *TAPA EMEA intelligence service.* https://tapaemea.org/incident-service/.

[38] Transported Asset Protection Association. 2025. *TIS.* https://database.tapa-global.org/site/dashboard.

[39] McKinsey & Company. 2021. *Succeeding in the AI supply-chain revolution.* 04 30. https://www.mckinsey.com/industries/metals-and-mining/our-insights/succeeding-in-the-ai-supply-chain-revolution.

[40] Ernst & Young. 2024. *How supply chains benefit from using generative AI.* 01 09.https://www.ey.com/en_gl/insights/supply-chain/how-generative-ai-in-supply-chain-can-drive-value.

[41] statista. 2024. *eCommerce - Worldwide.* 11. https://www.statista.com/outlook/emo/ecommerce/worldwide.

[42] OECD. 2021. *E-Commerce Challenges in Illicit Trade in Fakes: Governance Frameworks and Best Practices.* Paris: OECD Publishing.

[43] OECD. 2024. "Illicit Trade in Fakes under the COVID-19."

[44] OECD/EUIPO. 2021. *Global Trade in Fakes: A Worrying Threat.* Paris: OECD Publishing.

[45] Entrupy. 2025. Luxury Authentication. https://www.entrupy.com/luxury-authentication/

[46] Authentique. 2023. *Authentique.* https://www.authentique.com/.

[47] Osmo. 2024. *Osmo Introduces AI-Powered Scent Sensors for Authentication.* 11 25. https://www.osmo.ai/blog/osmo-introduces-ai-powered-scent-sensors-for-authentication.

[48] Lee, E, A J Mokashi, S Y Moon, and G Kim. 2019. "The Maturity of Automatic Identification Systems (AIS) and Its Implications for Innovation." *Journal of Marine Science and Engineering* 7 (9): 287. doi:https://doi.org/10.3390/jmse7090287.

[49] Spire Maritime. 2019. "Introduction to Automatic Identification Systems (AIS)." https://spire.com/whitepaper/maritime/introduction-to-automatic-identification-systems-ais/.

[50] Tetreault, B. 2005. "Use of the Automatic Identification System (AIS) for Maritime Domain Awareness (MDA)." *Proceedings of OCEANS 2005 MTS/IEEE.* Washington, DC, USA: IEEE. 1-5. doi:https://doi.org/10.1109/OCEANS.2005.1639983.

[51] Domballe, J. 2023. "Maritime State of Play Report: Deceptive shipping practices — Emerging company trends." *S&P Global.* 10 23. https://www.spglobal.com/market-intelligence/en/news-insights/research/maritime-state-of-play-report-deceptive-shipping-practices.

[52] Melnyk, O, S Kuznichenko, and O Onishchenko. 2024. "Impact of AIS Manipulation on Shipping Safety." *LEX PORTUS* 31-39. doi:https://doi.org/10.62821/lp10403.

[53] Allianz. 2024. "Safety and Shipping Review 2024." Munich.

[54] The Maritime Executive. 2024. *SEA.AI Employs Machine Vision and AI Improving Maritime Safety and Security.* 08 26. https://maritime-executive.com/features/sea-ai-employs-machine-vision-and-ai-improving-maritime-safety-and-security.

[55] Spectra. 2024. *How AI can help satellites track 'dark ships' from space.* 10 28. https://spectra.mhi.com/how-ai-can-help-satellites-track-dark-ships-from-space.

[56] Pu, Z, C-L Shi, C O Jeon, J Fu, S-J Liu, C Lan, Y Yao, Y-X Liu, and B Jia. 2024. "ChatGPT and generative AI are revolutionizing the scientific community: A Janus-faced conundrum." iMETA 3(2). doi:https://doi.org/10.1002/imt2.178.

[57] Huang, K, Wang Y, B Goertzel, Y Li, S Wright, and J Ponnapalli. 2024. Generative AI Security Theories and Practices. Springer. https://doi.org/10.1007/978-3-031-54252-7.