The Strategic Threat of Supply Chain Attacks: A National Security and Economic Perspective

.

ABSTRACT

|  |
| --- |
| **Aim:** To examine the strategic threat of supply chain attacks considering national security and economic perspective.  **Problem Statement:** The high significance of interconnectivity between production and supply of goods and services bridging the chain among the manufacturers, suppliers and distributors has given opportunities to attackers to seize the opportunity. These surreptitious attacks exploit the benefits, and the susceptibilities attributed with the interwoven network causing serious threats to businesses and organizations around the world.  **Significance of Study:** The over reliance of organizations and businesses on sophisticated suppliers’ chain has necessitated the quest to protect it from attack to avoid interruption of the transportation network for goods and services. Thus, examining the strategic threat of supply chain attacks with linkages to national security and economic perspective is important.  **Methodology:** Published articles that are recent and relevant to supply chain attacks are considered in putting this review manuscript together. The methodology employs the use of search engine on the google website and scopus index journals.  **Discussion:** The supply chain security nature can be strengthened via the implementation of third-party risk management programs, maintenance of continuous monitoring, executing thorough audits and enforcement of robust evaluation processes. The fundamental principles behind the connective web involved in supply chain were examined. Some of the general threats characterized with supply chain include environmental and climate risks; fluctuations in the economy, geopolitical conflict; transport and logistics and many more. The defense of supply chain attacks can be further fortified against emerging threats through collaborative research with reliable cybersecurity experts, updating various policies of security and limiting access to vendors. Additionally, regulatory compliance, operational stability, clients and partners trust alongside data protection are keys to securing supply chain.  **Conclusion:** In conclusion, there is need to establish strategic steps against threats of supply chain attacks for sustainable economic and national security. The recommended solutions to this menace are crime displacement; incident occurrence prevention; logistics and criminology; and many more. |

***Keywords:*** *Supply Chain Attacks, National Security, Economic Perspective, Operational Stability, Cybersecurity Experts*

1. INTRODUCTION

Supply chain is defined as the required organizations’ network via downstream and upstream interconnections in the various activities and processes that produce value in products and services form in the hands of the ultimate customer. The processes can be in diverse, similar or same companies [1]. The various building blocks making up a supply chain can be situated literally throughout the globe and linked via using transport network. This transport network is structured to adopt economy of scale when conveying products to consignee from consignor in a supply chain via links and nodes. This signifies that the transport network only substantially incorporates the supply chain with the satisfaction of its transport demands. Thus, numerous various supply chains can be available at the same place and the same time in the transport network [2]. This shows that the connection between transport activities and supply chains would be better defined with complexity theory, particularly if the relations between components are the research object [3].

Taking a critical look at transport from the perspective of a system, logistics can be observed to be made up of various levels, resources, infrastructure and material identified as the three logistics stages. A logistics system comprises of nodes and links, where nodes are locations that are geoically fixed such as terminals and factories while the elements relating the nodes are referred to as the links i.e., the conveyance modes. The first stage of the system is materials flow because it is the purpose for which the system exists. Conveying materials from one location to another entails the flow of movable resources such as trains, Lorries, ships and airplanes. Infrastructures such as harbors, roads, terminals and airports are needed for these movable resources [4].

The intricacy in logistics can best be described by demonstrating the four flows often required in logistics activities. Resources and material flows have been previously mentioned. These two flows symbolize the “physical” section of logistics, but the remaining two flows, information flow and monetary stream, are just as essential in making the system work [5]. The four logistic flows need infrastructure and geoically fixed constructions to fulfill the logistics scope. Some of the infrastructure belongs to one company and is exclusively used by them while some is owned or co-owned by governments. The necessary infrastructure and the four flows of logistics are the five requirements for the fulfillment of logistics. However, there are some challenges threatening excellent supply chains. Part of which is the cargo thief [6].

The aim of the cargo thief is to remove goods from the goods flow by attacking the resources movement and the infrastructure used. The information flow can also be utilized by a potential perpetrator to better plan and facilitate the goods theft or commit a fraud targeting capital flow. The primary three elements which are resources movement, goods flow and infrastructure of the five requirements for logistics fulfillments have been previously utilized. The routine activity theory from criminology was utilized as the reference frame to describe the connections between the potential perpetrators and transport network, where the theft opportunity is a function of each unique configuration of the five requirements for logistics fulfillments and then subjugated by a potential perpetrator [7].

The medicine, food, products and energy which are needed to support way of life is provided by the global supply chain [8]. Numerous various entities account for or depend upon the global supply chain effectiveness including law enforcement, regulators, private-sector businesses, public-sector buyers and other domestic and foreign partners. The global system depends upon an interrelated web of transportation pathways and infrastructure; cyber and energy networks; and information technology. These interdependencies enhance economic activity they serve to circulate risk across a broad geoic location or industry that emanates from a regional or local disruption [9]. Supply chains are now wide networks interwoven with digital threads that enhance connectedness and efficiency in the sophisticated web of modern trade. However, there is cost implication attached to interconnectivity because hostile cyber actors are targeting the supply chains increasingly to take advantage of weaknesses to cause sabotage, disruption or even financial gain [10].

Today’s world is complicatedly woven, with businesses depending on sophisticated ecosystems of distributors, suppliers and manufacturers. This complex connection, the supply chain, enhances our economic prosperity and technological advancements. However, this interconnectivity originated a threatening undercurrent which is the supply chain attacks. These furtive cyberattacks adventure vulnerabilities within this interconnected network, causing a powerful threat to organizations around the world. A supply chain attack is like an unknown viper causing danger on an organization’s trust in its collaborators. An organization’s digital defenses are often infiltrated by attackers via exploiting the accorded weaknesses of the supply chain partners [11]. This can be apparent through compromised tainted hardware components, software updates or malicious third-party services. Disruption of operations, stealing of sensitive data and potential orchestration of further havoc on downstream targets are usually achieved once access is gotten [6].

Dangers of supply chain attacks are often being amplified by several factors which include the trust factor, the ripple factor and elusive shadows. The trust factor usually bridges an inherent trust between the suppliers and partners resulting in lax scrutiny of hardware components, software updates and third-party services. This blind space gives the attackers great opportunity. A cascading domino effect can be triggered by a single compromised partner with the ripple effect which may impact many organizations and millions of potential users [12]. A tainted software update can be rippled via an entire industry causing operational disorder and a trajectory of data breaches. Nonetheless, supply chain attacks have been recognized as masters of disguise because they adroitly cloak themselves within trusted systems which make detection to be a very difficult task. The damage might already become permanent when the alarm bells ring [1].

The flow of goods and services can be stopped by supply chain threats and identifying them is the key to financial stability and business continuity. The threats of supply chain are broad ranging from cyber and compliance to environmental and operational [13]. The whole supply chain can be affected by these top supply chain risks requiring proper management. Globalization has added regulatory, national security and sustainability to the mix which makes the management of the global supply chain to become more critical. The supply chain can be stopped by these external threats in its tracks causing disruption and additional cost. In 2023, with the total number of victims being more than 54 million, the supply chain attacks have surged by more than 2,600% since 2018. The total average number of supply chain breaches having negative influence on companies has risen by 26% when compared between 2022 and 2023 [14].

Furthermore, operational risks can result into delays, quality issues or cost increases across the entire supply chain. For instance, a machine breakdown in a factory can terminate production and interrupt product delivery. The production cycle is affected by such interruptions and may cost millions [10]. It is imperative for supply chain professionals and leaders to be very diligent with their supply chain management with risks minimization. The development of a risk mitigation strategy is feasible if the supply chain security threats are known to enhance the smooth running of the supply chain. This review article addresses the strategic threat of supply chain attacks with consideration to national security and economic perspective.

2.0 GEneral Threats attributed to Supply Chain and suggestions on how they can be ameliorated

The influence of threats on supply chain is overwhelming irrespective of the nature of the adopted supply chain method or risk. It can originate from operational interferences and deteriorate into substantial financial losses, regulatory penalties and reputational damage [10]. The various threats that are attributed to supply chain are discussed thus:

* **Environmental and Climate Risks**

Natural calamities such as hurricanes, floods and earthquakes can interfere with the supply chains by delay in transportation, stoppage in production and infrastructural damage. More costs are required for the replacement of equipment, repair and recognizing optional routes with the aforementioned environmental risks [7]. There is need to invest in planning of business continuity for effective operation after a disaster. Waste reduction and improvement in the efficiency of resources can attained using green sources to enhance the resilience of the supply chain. Unexpected climate change can be prepared ahead using integrated supply chain solutions. This can be achieved via general efficiency and increasing sustainability [11].

* **Fluctuations in the Economy**

The supply chain can be greatly influenced by fluctuations in economy via increase in costs for overall business operations, energy, fuel and labor. The price and costs of imported goods can be impacted by the fluctuations in currency thereby influencing the financial planning and supply chain budget. A detailed supply chain risk management technique is essential. There may be sudden increase in the costs of material resulting from economic downturns and inflation. In return, this makes it difficult for manufacturers to acquire the raw materials at friendly and workable prices. Nonetheless, there may be reduction in the consumers’ demand due to economic recessions which consequently add more tension on the supply chain [4]. The economic risks can be alleviated via establishing better supplier relationships, diversification of suppliers and adopting financial and insurance tools. The demand can be excellently predicted while optimizing the inventory through the use of real time data and predictive analytics. With these measures, the economic fluctuations can be adequately managed while the supply chain resilience is perfectly maintained [9].

* **Inadequate Transparency and Visibility**

There are feasibilities of high risks and inefficiencies resulting from inadequate transparency and visibility in the supply chain network. Transparency entails revealing open communication and practices with suppliers to fix and recognize the inefficiencies. Technologies such as blockchain and artificial intelligence can enhance the transparency of the supply chain via storing, tracking and provision of real time information [10]. The whole supply chain will be visible starting from finding of raw materials to end consumer. There will be perfect streamlining of processes with high visibility throughout the entire supply chain with the aid of digital transformation techniques such as cloud-based software and Internet of Things. The supply chain risks of businesses can be effectively managed and operated perfectly via transparency [5].

* **Geopolitical Conflict**

A key risk to world supply chains is geopolitical conflict. This can result in shortage of global raw materials and energy which afterwards influence the supply chain logistics and planning. Typical cases are the political conflicts in the Middle East, North Africa and Ukraine which has powerfully interrupted with the supply chains. Trade restrictions such as sanctions and tariffs can be imposed by the government to put an end to goods flow across borders which increase the cost additionally [15]. Uncertainty that disrupts perfect operations can be created via geopolitical conflict causing serious delays and having to re-route the resources. The supply chain efficiency and security can be impacted through the alterations. Geopolitical risks can be controlled via supplier’s diversification; forecasting the worst scenarios happening; reliable connectivity with logistics partners; and exposure monitoring, mapping and measuring of the events. The influence of the geopolitical risks on supply chain can be drastically ameliorated [7].

* **Operational Incapability**

Issues relating to costs, delays and quality in the supply chain can be linked with operational incapability which may affect the supply chain. For instance, inadequate management of inventory may result into stockouts and affect the general performance of the supply chain. Selection of wrong product and mislabeled packages are the major operational errors which are peculiar origins of incapability [16]. To address this, it very imperative to optimize and manage the processes involved with the managing supply chain risks inclusive. Logistics optimization, reduction of packaging material usage and streamlining of inventory management are important points needed to improve the efficiency of supply chain. The general performance and supply chain resilience can be improved if the operational risks are adequately addressed [17].

* **Transport and Logistics**

A substantial disturbance of the supply chain can emanate from transport and logistics. Failures in transport mode, closures of ports and shipping bottlenecks will surely increase the impacts of supplier relationships and freight costs. The implementation of automated and dynamic freight management will assist in alleviating logistics risks [12]. Distribution, warehousing and delivery can be adequately and effectively managed by the incorporation of AI driven planning attributes in logistics software. This ascertains error free and timely product delivery and thus makes supply chains to be more efficient. The use of standardized freight documents, automated processes and real time information is suggested to ameliorate disruptions of supply chain caused by logistics risks [11].

* **Reliability and Supplier Dependence**

Reliability and supplier dependence are essential factors to flexibility of supply chain. Supply shortages as a result of political instability or natural disasters can result from over dependence on a single supplier. The supplier base should be diversified while sourcing from numerous locations in order to mitigate these kinds of accorded risks. Knowing the suppliers is vital in taking strategic decisions on services and external products. Also, for suppliers to meet the standard, it is recommended to have the supplier performance monitoring systems intact. This gives room for the smooth supply of raw materials and products during interferences. Establishing robust relationships via collaborative planning, consistent communication and shared risk management will yield long term resilience and stability [13].

* **Cybersecurity Threats Linkage with Supply Chain**

The advent and rise of IoT networks and cloud connected supply chains has catalyzed cybersecurity threats. In 2023, the ransomware attacks have risen by more than 70% with possibility of further increase. The SolarWinds attack and MOVEit hack in 2020 and 2023 respectively have greatly contributed to the high rise in profile incidents of the supply chain [12]. It is essential to invest in the robust cybersecurity procedures to address the threats which include constant cybersecurity awareness programs and training for both the suppliers and the employees; steady detection and monitoring of tools; and vendor contracts involving cybersecurity necessities like regular audits and data breach notifications. Strong framework such as the NIST Cybersecurity Framework is crucial for cyber risks management in the supply chain [18].

2.1 cases of supply chain attack

Numerous problems arising from supply chain attack have been recorded. The reported cases were not just imaginary scenarios. The case of SolarWinds Orion network management software being hijacked by attackers in 2020 was reported [19]. This impacted Fortune 500 companies and government agencies. The devastating ripple effect was exemplified by this attack such that a digital domino chain can be toppled by one compromised vendor. In 2021, the Bash Uploader tool from Codecov, which was a security firm, was infiltrated by attackers [13]. Thousands of software projects were jeopardized because of this attack. This describes how security providers can even be unconscious traders in supply chain attacks game. Furthermore, pre-installed malware was discovered in 2022 by researchers on some ASUS laptops. The insidious attribute of hardware attacks was revealed by this case showing how hidden threats can be harbored by seemingly harmless devices [6].

**3.0 SOLUTIONS TO SUPPLY CHAIN ATTACKS**

Different suggested solutions to curb supply chain attacks have been in existence. These include but not limited to the following:

* **Risk management, Logistics and Criminology**

The risk management, logistics and criminology work together with security and crime prevention to tackle supply chain attacks. The fundamental principle is that risk management and security are useful with reference to the ethical point of view due to the fact that they enhance crime reduction [14]. This ascertains crime reduction because better risk management and security are put into places. However, the major challenge is that crime is defined by a law based on the principle of “there is no crime without a law”. Also, there is no philosophical attachment to law with reference to risk management or security. Thus, there can be better risk management and security for people on both sides of the law [19].

* **Prevention of Incident Occurrence**

The improvement of terminal security has greatly increased theft incidents linking terminals. Under development has been previously noticed with freight transport security. From the perspective of a supply chain, this development is also applicable. The remaining chain exists in the absence of security while security in manufacturing facilities is usually targeted and adequately managed. Security in the process of transportation is essential in preventing unplanned negative interference in goods flow [12]. Transport security entails interconnectivity between humans’ intervention and physical obstructing artifacts which are Closed Circuit Television (CCTV), fences, locks and so on. This is purposely to reduce sabotage, theft and other forms of illegal activity. There is rapid improvement in the technological innovations of adopting complex post theft systems and anti-theft devices. There are various preventive techniques that can be adopted in minimizing accorded risks of a cargo theft incident. The correct use of physical security counter procedures is identified as the main method such as guards, locks, fences, seals and so on. The principal objectives of adopting these kinds of counter measures are to ensure that the theft both is riskier and harder to commit. The employees’ trust and control in the company is also another counter measure that can be adopted. With this technique, the internal theft problem is targeted and can be subdivided into new employee reference checks and present employees’ supervision [17].

* **Opportunity, Perpetrator and Security**

The interconnectivity between opportunity and security is the principal understanding of security in various contexts. The ideology depends on having the belief that security only can repel or deter a motivated perpetrator from committing a crime via the limitation of the opportunities for a particular crime. The principal thing to take note with crime opportunities is that an opportunity alone cannot describe the reason a crime happens because it requires an opportunity and a motivated perpetrator to occur [21]. Opportunity plays a key role in making a crime to exist and these opportunities are extremely concentrated and specific in time and place [20]. Also, opportunity is a function of everyday movements. These opportunities can be minimized and targeted opportunity minimization can generate broader declines in crime. This is an established principle behind security. The major challenge happens when the security capability of an organization is less than the potential perpetrator’s capability. Ethics, determinism, vindication from morality and altruism can be the driving force within each potential perpetrator [12]. Thus, it is important to understand the connectivity between opportunity and security on the basis that the engaged parties (actors, stakeholders and humans) have various individual incentives to utilize opportunity that security requires to address. Therefore, security should be viewed as incentive limiting and opportunity limiting which makes security a preventive variable on both sides of the post- and pre-events [22].

* **Mixing of Criminology into Logistics via Interdisciplinary Research**

The tradition of using criminology theories to fortify logistics field is adopted making criminology to be interdisciplinary research combining future of crimes and history together. The principal research technique in logistics connected to influence on a smaller extent or human intervention and tangible artefacts are challenged by the mixture of theories. The purpose of this technique is to ensure that law violation is accepted as part of human attributes [9]. The three crime elements present in all forms of crime are distinguished by criminology and this ranges from occasional violence to complex and advance economic crimes. These elements include appropriate object, motivated perpetrator and deficiency in capable guardian.

* **Crime Displacement**

The assumption of crime displacement is based on the principle that crime is inelastic which strongly indicates the insignificance of preventive efforts on crime demand. However, this is untrue because all crimes are more or less elastic. Opportunistic criminals are more elastic while professional criminals are more inelastic. The crime displacement theory states that prevention of crime in a location may have unintentional penalty in other locations. Thus, crime prevention may not result into an absolute decrease in crime. Crime displacement theory is based on rational choice theory using the previously mentioned assumptions regarding the target and potential perpetrator [13]. The perpetrators have mobility because of their flexibility relative to place, crime type, time, and method. In the real sense, there are limitations by perpetrators to their adaptability, mobility and flexibility relative to a certain crime, time, place and method. Numerous counts of optional targets are already in existence. The perpetrators have unconstrained numbers and kinds of possible targets to pick from. However, in reality in one way or another, the targets number is constrained.

3.1 Linking Supply to National Security: United state as a case study

The supply chain security in United State is progressively under threat. This present moment has been described by the National Security Strategy of the White House as an inflection point. The principle of supply chain security has been heightened by numerous federal agencies to a subject matter expertise with severe national security inferences. The supply chain professionals are presently working on the front lines of United State national security in numerous ways. Some of these include cybersecurity controls, personnel security controls and physical security controls [23].

* Reports of cyber threats have been made with enormous frequency which resulted in fixing them in the national consciousness. The Transportation Security Administration (TSA) and the United State Cybersecurity and Infrastructure Agency (CISA) are the two federal agencies that have improved attention on this susceptibility in supply chains. These efforts’ theme includes activities reporting by potential threat actors and steadfast awareness necessity.
* Another long-standing risk that is receiving serious attention in the entire supply chain is the personnel threats. These extend excellently past screenings for who may have access to particular facilities. These include some particular domestic technologies like deemed export restrictions and TWIC cards. The personnel security question is observed in constraints around who may hold certain responsibility and roles for some essential functions having great impact significance for national security and supply chain security.
* Although physical threats remain significant, they are more conventional in their risk profile. More attention has been given to cargoes protection, transportation movements and facilities. National security threats of theft, espionage and terrorism are substantial in the entire supply chain. Regulatory requirements and programs have long been maintained by a broad range of federal agencies to curb risk exposure from physical threats. New efforts are evolving for particular geopolitical worries.

4. Conclusion

Supply chain attacks have become serious threat, at both private and state companies, to various organizations around the globe. Records of continuous exploitation by attackers have been on rampage necessitating the need to take proactive steps and strategic techniques in securing the supply chain network. It is imperative to build a resilient defense which neutralizes and anticipates risks before causing harms. The worldwide supply chain system will enhance prosperity and innovation via reliably, securely and expeditiously moving goods and services within domestic borders and across the globe. This review article has examined the strategic threat of supply chain attacks considering national security and economic perspective using published articles indexed in scholarly journals. The fundamental principles behind the connective web involved in supply chain have been discussed. The general threats characterized with supply chain together with suggestions on how they can be ameliorated are examined. Some of these include environmental and climate risks; fluctuations in the economy, geopolitical conflict; transport and logistics and many more. Suggestion solutions to tackle threats from supply chain attacks include risk management, logistics and criminology; prevention of incident occurrence; opportunity, perpetrator and security; crime displacement and so on. In conclusion, the defense of supply chain attacks imperative for uninterrupted and smooth linkage between the manufacturer, supplier and end-users.

**Disclaimer (Artificial intelligence)**

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

References

1. Ram, J. and Zhang, Z., 2020. Belt and Road Initiative (BRI) Supply Chain Risks: Propositions and Model Development. The International Journal of Logistics Management, 31(4), pp. 777-799.

2. Tyagi, P., Grima, S., Sood, K., Balamurugan, B., Özen, E., Thalassinos, E.I. (Eds.). 2023. Smart analytics, artificial intelligence and sustainable performance management in a global digitalised economy. Emerald Publishing Limited.

3. Oral, F. and Paker, S., 2023. Risk Assessment for Maritime Container Transportation Security. Journal of ETA Maritime Science, 11(4).

4. Pérez-Morón, J., 2021. Eleven Years of Cyberattacks on Chinese Supply Chains in an Era of Cyber Warfare: A review and future research agenda. Journal of Asia Business Studies, 16(2), pp. 371-395.

5. Grima, S., Thalassinos, E., Cristea, M., Kadłubek, M., Maditinos, D., Peiseniece, L. (Eds.). 2023. Digital transformation, strategic resilience, cyber security and risk management. Emerald Publishing Limited.

6. Iakovakis, G., Xarhoulacos, C.-G., Giovas, K., and Gritzalis, D., 2021. Analysis and Classification of Mitigation Tools against Cyberattacks in COVID-19 Era. Hindawi Security and Communication Networks, Volume 2021, Article ID 3187205.

7. Auzina, I., Volkova, T., Norena-Chavez, D., Kadłubek, M., Thalassinos, E. 2023. Cyber Incident Response Managerial Approaches for Enhancing Small–Medium-Size Enterprise's Cyber Maturity. In Digital Transformation, Strategic Resilience, Cyber Security and Risk Management (pp. 175-190). Emerald Publishing Limited.

8. Etemadi, N., Van Gelder, P., and Strozzi, F., 2021. An ISM Modeling of Barriers for Blockchain/Distributed Ledger Technology Adoption in Supply Chains Towards Cybersecurity. Sustainability, 13(9), p. 4672.

9. Creazza, A., Colicchia, C., Spiezia, S., and Dallari, F., 2022. Who cares? Supply Chain Managers' Perceptions Regarding Cyber Supply Chain Risk Management in the Digital Transformation Era. Supply Chain Management - An International Journal, 27(1).

10. Azab, M., Alhyari, S., Awajan, A., and Abdallah, A.B., 2021. Blockchain Technology in Supply Chain Management: an Empirical Study of the Factors Affecting User Adoption/acceptance. Cluster Computing, 24(1), pp. 83-101.

11. Manuj, I. and Mentzer, J.T., 2008. Strategies for Managing Risk in Gobal Supply Chains. International Journal of Physical Distribution & Logistics Management, 38(3), pp. 192-223.

12. Naz, F., Kumar, A., Agrawal, R., Garza-Reyes, J.A., Majumdar, A. and Chokshi, H., 2023. Artificial Intelligence as an Enabler of Quick and Effective Production Repurposing: An Exploratory Review and Future Research Propositions. Production Planning & Control, 23, 67-76.

13. Noja, G.G., Cristea, M., Thalassinos, E., Kadłubek, M. 2021. Interlinkages between government resources management, environmental support, and good public governance. Advanced Insights from the European Union. Resources, 10(5), 41.

14. Pournader, M., Shi, Y., Seuring, S. and Kh, S., 2019. Blockchain Applications in Supply Chains, Transport and Logistics: a Systematic Review of the Literature. Special Issue: Blockchain in Transport and Logistics, pp. 2063-2081.

15. Gourisetti, S.N.G., Mylrea, M., and Patangia, H., 2019. Evaluation and Demonstration of Blockchain Applicability Framework. IEEE Transactions on Engineering Management, 67(4), pp. 1142-1156.

16. Ekwall, D. 2012. Supply Chain Security – Threats and Solutions. Chapter 8: Risk Management – Current Issues and Challenges, Intech Open, 157 – 184.

17. Ekwall, D. 2009. The Displacement effect in cargo theft”. *International Journal of Physical Distribution and Logistics Management,* Vol. 39, No. 1, pp. 47-62.

18. Sampson, R., Eck, J.E. and Dunham, J. 2010. Super controllers and crime prevention: A routine activity explanation of crime prevention success and failure”. *Security Journal,* Vol. 23, No 1, pp. 37–51.

19. Johnston, R. B. and Nedelescu, O. M. 2006. The impact of terrorism on financial markets”. *Journal of Financial Crime*, Vol. 13, No. 1, pp. 7-25.

20. Arlbjörn, J.S. and Halldorsson, A. 2002. Logistics knowledge creation: reflections on content, context and processes”. *International journal of physical distribution & logistics* *management*, Vol. 32, No. 1, pp. 22-40.

21. Mmaduekwe, U. 2024. Bias and fairness issues in artificial intelligence-driven cybersecurity. *Current Journal of Applied Science and Technology*, 43, 6, 109-119.

22. Mmaduekwe, U. and Mmaduekwe, E. 2024. Cybersecurity and Cryptoy: The New Era of Quantum Computing. *Current Journal of Applied Science and Technology*, 43, 5, 41-51.

23. U.S. Department of Commerce, 2023. Cyberattacks in Poland Occur Every 9 Minutes. Trade.gov. (Online) Available at: <https://www.trade.gov/market-intelligence/poland-ict-cyberattacks-poland-take-place-every-9-minutes>