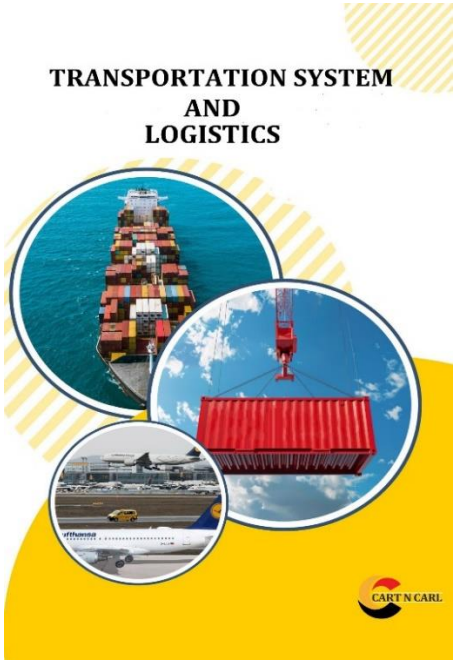
Original Research

Transportation System and Logistics
https://cartcarl.com/journal/transportation-system-and-logistics

E-ISSN: 0331-846X



Cyber Security Measures and Operational Efficiency of Seaports in Eastern Nigeria

Authors
[a] Nkitma, A. N., [ab] Wizor, C. H.

[a] Centre for Logistics and Transport Studies, Faculty of Social Sciences, University of Port Harcourt, PMB, 5323, Choba, Rivers State, Nigeria.
[b]Department of Geography and Environmental Management, Faculty of Social Sciences, University of Port Harcourt, PMB, 5323, Choba, Rivers State, Nigeria.

Corresponding Author
Nkitma, A. N.
(atimnkitma@yahoo.com)

Received: 26 November, 2025
Accepted: 06 December, 2025
Published: 10 December, 2025

Citation
Nkitma, A. N. and Wizor, C. H. (2025). Cyber security measures and operational efficiency of seaports in Eastern Nigeria. *Transportation System and Logistics, 2* (1), 49 - 57. https://doi.org/10.70726/tsl.202514957

Abstract

This study examined the relationship between cybersecurity measures and operational efficiency in the Eastern Nigeria seaports. The study adopted an explanatory research design; and surveyed one hundred and twenty respondents of 4 seaports in Eastern Nigeria. However, 114 copies were considered fit for the study. The Pearson Product Moment correlation was used to analyze data retrieved from respondents. The results indicate that cybersecurity measures have a very strong positive and significant relationship with the measures of operational efficiency (cargo dwell time, ship turnaround time and cargo throughput) in the Eastern Nigeria seaports. Therefore, we concluded that the seaports in Eastern Nigeria should adopt cybersecurity measures in order to maintain operational efficiency in the long run. It was recommended that ports managers and stakeholders should implement comprehensive cyber defense strategies, including regular vulnerability assessments, data encryption, and real-time monitoring of networks in order to achieve operational efficiency in terms of cargo dwell time, ship turnaround time and cargo throughout.

Keywords : Emerging Technologies, Operational Efficiency, Nigerian Navy, Logistics Management, Artificial Intelligence

Introduction

In response to new regulations and economic factors, the seaports in Eastern Nigeria are digitizing their systems to enhance efficiency. They are compelled to incorporate cyber technologies into port operations, including process design, cargo handling, navigation, environmental protection, pollution prevention, risk management, and port safety and security, while adhering to the international and national standards set forth by the SOLAS Conventions (IMO, 2019a, 2019b, 2019c), the MARPOL Conventions, and the ISPS Codes (Homeland Security, 2018). Simultaneously, attackers have identified these technologies as a means to infiltrate vital infrastructures and compromise their security. Cyberattacks attacking digital systems are becoming prevalent. The weaknesses of various cyber technologies and digital systems might result in cyber-attacks that incur substantial financial losses due to company interruptions and system recovery efforts. Ports serve as essential connections in global supply networks, making them attractive targets for cyberattacks (Ahokas et al., 2017; Heilig & Voß, 2017). Shipping and port operators may be susceptible to five kinds of cyber threats: hacktivism, cybercrime, cyber espionage, cyber terrorism, and cyber warfare (Ahokas et al. 2017). Consequently, port managers and policymakers of Eastern

Nigeria's seaports must comprehend the many cyber risks that jeopardize port cybersecurity.

Ports are essential nodes in the global transportation system that need robust security against cyber-attacks (Akpan et al, 2022). Securing networks and information systems has become paramount due to the vast volume of data and the rapid technological advancements in the ports and maritime sector (Bunyamin, Gizem & Pelin, 2021). Maritime cybersecurity involves safeguarding shipborne systems, shore-based operations, and communication networks from cyber threats (Melnyk et al., 2023). Effective cybersecurity in the marine sector requires a comprehensive strategy, including technical, organizational, and regulatory initiatives (Farah et al., 2023). Technological solutions, like encryption, intrusion detection systems, and secure communication protocols, are vital for improving cybersecurity in marine systems (Walid et al., 2017). Organizational methods include educating workers on cybersecurity best practices and establishing incident response plans (Chowdhury et al., 2022). Regulatory frameworks at both national and international levels are essential for standardizing and enforcing cybersecurity activities (Faria, 2020).

As digitalization in the maritime sector escalates, cybersecurity has become a crucial area impacting the safety of ship operations and port services. Cybersecurity enhances the productivity and efficiency of port operations along the whole logistical chain. In this context, sea transport provides the most advantageous cost-benefit ratio for managing substantial cargo quantities across extensive distances, characterized by cheap costs and efficient services, making it the predominant option for international commodities transportation. The contemporary globalization scenario necessitates that ports provide services that enhance transport with agility, safety, and efficiency to sustain market competitiveness (Sanchez-Gonzalez et al. 2019). Efficient operations result in diminished turnaround times for vessels, decreased operating expenses for shipping firms, and enhanced client satisfaction owing to dependable schedules (Hart, 2019). The effectiveness of port operations, including ship-to-shore gantry cranes, terminal area activities from container stacks to berth-side, and the patterns of container arrival and departure at entry gates, may impact vessel turnaround time. Operational interruptions may result in delays in production timelines and product delivery, adversely affecting customer satisfaction and operational efficiency.

The aim of this research is to objectively investigate the correlation between cybersecurity measures and the operational efficiency of seaports in Eastern Nigeria. This study examines a significant gap in comprehending the correlation between cyber security measures and three indicators of operational efficiency cargo dwell time, ship turnaround time, and throughput of seaports in Eastern Nigeria through the following research objectives: evaluate the relationship between cyber security measures and cargo dwell time at seaports in Eastern Nigeria; investigate the relationship between cyber security measures and ship turnaround time at seaports in Eastern Nigeria and valuate the correlation between cybersecurity protocols and cargo throughput at seaports located in Eastern Nigeria.

Cyber Security Measures

Cybersecurity measures include digital protections, including firewalls, data encryption, and secure networks (Fettermann & Eltayeb, 2020). The ongoing advancement of technology has resulted in the absence of a globally accepted definition of cyber security. General definitions, however, underscore that the term include defensive strategies to identify and thwart unauthorized third parties. The US National Institute of Standards and Technology (NIST) defines cyber security as the capacity of cyberspace to safeguard and defend itself from cyber-attack activities (NIST, 2019). Cybersecurity encompasses a comprehensive array of rules and practices designed to manage personal data, ensuring its confidentiality and integrity to mitigate cyber-attacks. Organizations with strong data security measures are more effectively positioned to manage risks associated with cyber-attacks (Alzighaibi, 2021). Cybersecurity measures are essential for mitigating organizational risk by protecting information systems from dangers such as data breaches and cyber-attacks. These include firewalls, encryption, and multi-factor authentication, which assist in preventing data loss, data leakage, and ensuring data accessibility.

Although digital transformation in ports can enhance operational and managerial efficiency, the quest for competitive advantage frequently leads to the neglect of critical security concerns, particularly cyber risks, thereby disrupting the equilibrium between the advantages and hazards of this process (Marques-Guedes 2018). An insecure cyberspace, characterized by inadequate cybersecurity measures, is susceptible to various cyber-attacks (Ahokas et al. 2017). Cyberthreats are a significant

risk for global logistics and transportation security within the marine sector. As shipping increasingly relies on digital technology such as automated vessel traffic management, IT systems, and electronic data transmission, it becomes more susceptible to cyberattacks. A cyberattack is an offensive action aimed against information technology (IT) and operational technology (OT) systems, computer networks, and personal computing devices, with the intent to compromise, damage, or access organizational and maritime systems and data. Digitalization is crucial for port efficiency and competitiveness, including automated trucks, stacking cranes, gate automation, optical character recognition, license plate identification, automated teller machines, e-tracking services, and wireless gadgets. Confronting the cybersecurity difficulties encountered by marine ports requires a comprehensive strategy that integrates technical, procedural, and human factors (Fenton, 2024). Implementing modern technical solutions is a crucial part of enhancing cybersecurity in the marine industry.

Cybersecurity measures are activities implemented to safeguard a device or its system against assaults and unauthorized access, aiming to provide a steady state of security in cyberspace, characterized by protection and reliability (Ahokas et al. 2017). Essential cybersecurity duties include safeguarding information, networks, and data against unauthorized access, preserving data integrity, and ensuring access is restricted to authorized persons only. In the realm of cyber security, tools used to safeguard against malware, computer and network assaults, identify unauthorized access, and mitigate infections are included. As ports adopt digitalization, they encounter an increasing number of cyber events that interrupt operations and cause significant economic harm, highlighting the need for robust cybersecurity measures. Port cybersecurity is of paramount significance for guaranteeing safety and security by implementing effective security protocols and disseminating them to shipping lines and other pertinent operators. The inadequacy of cybersecurity and port policies increases vulnerability in safeguarding digital assets and infrastructure (Moerel & Dezeure, 2017).

Operational Efficiency

Operational efficiency refers to how effectively the port manages its resources such as berths, cranes, labour, and equipment to minimize delays and maximize the throughput of ships (Stephen, 2024). High operational efficiency at the port would mean that ships are processed quickly, with minimal waiting time, ensuring that cargo is loaded and unloaded swiftly. This would involve optimizing processes such as berth allocation, crane operations, and coordination between different port services. Efficiency is defined as the result of input divided by output. There has been minimal progress in enhancing effectiveness and efficiency in the management of Nigeria's ports to meet the International Maritime Organization's regulations regarding cargo clearance. Furthermore, when comparing the operating data of the port in question with that of neighboring ports, it becomes evident that the operational reliability of the surrounding ports is more resilient and stronger. Hence, it is imperative to reassess Nigeria's port operations in order to enhance the ports' competitive standing in both the global and regional marketplaces.

The performance of seaport operations is inextricably tied to the efficiency of terminal operators, the availability of cargo handling equipment, and the logistics dynamics of cargo dwell time. Notably, industries engaged in non-time-sensitive cargo tend to experience smoother trade facilitation compared to time-sensitive sectors, which are frequently constrained by inefficiencies in port operations (Kin, 2002). The ability of terminal operators to procure and deploy the appropriate cargo handling equipment demanded by shippers not only enhances their throughput capacity but also serves as a significant attraction for cargo traffic to their facilities. Steenken et al. (2004) offer a practical framework for measuring port performance through the lens of terminal operations. Their simulation-based models link key variables such as: Berth occupancy rate, Cargo handling time, ship turnaround, Storage yard congestion. These metrics collectively define the efficiency of port operations and highlight the need for real-time system feedback loops to prevent operational bottlenecks. Thus, the measures of operational efficiency employed in this study were; ship turnaround time, cargo dwell time and throughput.

Ship Turnaround Time

The entire amount of time it takes for a ship to do all the port-related tasks from the moment it arrives until it leaves is known as the ship turnaround time (Nnwaogbe et al. 2023; Mensah et al. 2023). According to Nze et al. (2018), the operational indicator of productivity that measures the time at which a vessel entirely departs the port is the idea of ship turnaround time (STRT), defined in

hours or days. This is the period that elapses between when a vessel enters the port and when it leaves. Since STRT shows how efficiently the port's superstructures and cargo handling equipment are being used, it is a big component that impacts the ports that ship owners and operators choose, according to Nwokedi et al. (2021). The time it takes for a ship to dock, unload its cargo, and leave the port is called its turn-around time. One indicator of a port's efficiency and trade competitiveness is the amount of time vessels spend there (UNCTAD, 2019). Shipowners benefit most from the fastest ship turnaround time since the amount of time a ship spends in port has a significant impact on its profitability. Therefore, the shorter the time ships spend in ports, the more money they make.

Cargo Dwell Time

Cargo dwell time, as defined in the Nigeria Ports Authority (NPA, 2016) handbook, is the amount of time that a consignment of goods waits to be transported by ship for export or evacuated by rail or road for import. Cargo dwell time (CDT) is the amount of time a cargo or ship spends within a port. It measures the total time cargo spends at the terminal from unloading to final evacuation and serves as a proxy for gauging port efficiency, competitiveness, and logistics fluidity (Nze, Ejem, & Nze, 2020). The time spent between the time the cargo arrived in the port and the moment the consignee or his representative picked it up from the port's premises after all permits, customs clearances, and other formalities have taken place is known as the cargo dwell time. It is a critical performance indicator in port operations, reflecting the efficiency of cargo handling, customs clearance, and logistical processes. The longer the dwell time, the more inefficient the port operation, leading to higher costs, congestion, and delays. Reducing dwell time is a primary objective for many ports worldwide, as it directly impacts the speed at which goods can be processed and transported. For ports in emerging economies like Nigeria, minimizing dwell time is key to boosting their trade capacity, attracting investment, and ensuring a seamless connection to global supply chains.

Cargo Throughput

El Imran and Babounia (2018) state that cargo throughput is defined as the total amount of cargo handled during a certain time, expressed in TEUs or metric tonnes. A port's cargo throughput is the total tonnage of cargo it handles or facilitates, which includes export and import cargo of different categories. National economic growth, trade facilitation, and sustainable urban development are all influenced by port cargo throughput, which is an important metric for evaluating port operational activity and levels of regional economic development (Cong et al., 2020; Xiao et al., 2024). The port may be experiencing low revenue production and deteriorating performance when the cargo throughput value is low. Since port cargo throughput is based on vessel traffic statistics and size, stronger performance in this area is suggestive of better port operations and, by extension, higher revenue profits, since cargo and ship charges are the primary sources of income. A port city's economic status and degree of growth may be reflected in its cargo throughput.

Empirical Review

Aderinto and Adeniran (2025) looked at how cybersecurity risks affected the bottom lines of Nigeria's publicly traded commercial banks. An ex-post facto research design was used in the study. This study's population includes all fourteen (14) commercial banks that are listed on the Nigerian Exchange Limited. Ten (10) named commercial banks were chosen at random from this pool of participants using a judgmental sampling approach. We used robust least square regression to evaluate our hypotheses. Earnings per share of listed commercial banks in Nigeria are negatively impacted by financial losses caused by cybersecurity vulnerabilities, according to the report. Cybersecurity risks are significant financial worries that have an immediate impact on profits, in addition to being technical or operational hurdles. Another research that looked at how cybersecurity procedures affected supply chain performance in the banking industry of Jordan was Al-Khatib, Ibrahim, and Alnadi (2025). Results were obtained from 250 digital banking customers' surveys and 40 managers' surveys; 220 of these were deemed legitimate for analysis using IBM SPSS V26 and PLS-SEM V4; 30. The results of this research show that cybersecurity policies have a favourable effect on the efficiency of the supply chain in Jordanian banks. A other research that looked at the impact of cybersecurity and data protection methods on risk reduction for a corporation was Ali et al. (2025). The authors used a quantitative research paradigm to survey data protection officers, cybersecurity experts, and IT managers from a variety of industries. Using regression analysis, this study looks at the connection between cybersecurity measures, data security, and the consequent decrease in risk. The survey found that organizations may

lower their risk levels with the use of cybersecurity solutions and clear data protection policies. In their study, Ren et al. (2024) looked at how digital progress affects the resilience of port security. Using provincial panel data collected between 2010 and 2019, this research empirically examined how digital growth affected the resilience of port security in 16 provinces along China's coast and in the Yangtze River Economic Belt. There is substantial variety and long-term impacts, but overall, the data show that digital growth makes port security more resilient. Listed Nigerian food and beverage firms' financial performance was studied by Aminu (2024) in relation to cybersecurity measures. The study evaluated the effectiveness of cybersecurity measures using multiple regression analysis and an ex post facto research approach. The findings showed that cybersecurity expenditures increase shareholder value and that cybersecurity measures and regulatory compliance greatly improve financial performance. Up until now, researchers have used several proxies to study the correlation between cybersecurity measures and operational efficiency. However, fundamental research on how cybersecurity measures might enhance seaport operating efficiency is lacking. To fill this knowledge vacuum, this study analyses how seaports in Eastern Nigeria's cybersecurity measures affect their operating performance.

Theoretical Background

This paper is grounded on the High Reliability Theory (HRT). High reliability theory (HRT) is concerned with how complex organizations operating in high-risk environments maintain consistent and error-free performance (Roberts, 1990). Ports are critical infrastructures where lapses in security can result in significant economic and safety consequences suggests that achieving operational efficiency under high-risk conditions requires a strong culture of safety, real-time monitoring, redundancy, and continuous learning. This is echoed by Fettermann and Eltayeb (2020), who stress the integration of physical and cyber defense mechanisms to safeguard digital port operations. HRT supports the argument for proactive risk management and institutional learning as foundations for improving port security and efficiency. The study is thus guided by the following hypotheses:

H_{01}: There is no significant relationship between cybersecurity measures and operational efficiency of seaport in Eastern Nigeria.

H_{02}: There is no significant relationship between cybersecurity measures and operational efficiency of seaport in Eastern Nigeria.

H_{03}: There is no significant relationship between cybersecurity measures and operational efficiency of seaport in Eastern Nigeria.

Method and Materials

The study adopted an explanatory research design to examine the relationship between cybersecurity measures and operational efficiency of seaports in Eastern Nigeria. The examination of this study was done at the organizational level. Four (4) seaports operating in the Eastern Nigeria constitute the population of the study. The study took a census, and surveyed a total of 120 respondents on a sample frame of 30 respondents per seaport. 114 copies were considered fit for the study. The questionnaire appeared in the form of 5- point Likert scale and data gathered were analyzed using mean, standard deviation, frequency distribution and percentage for the univariate analysis; and the Pearson Product Moment Correlation (PPMC) for bivariate analysis. The SPSS aided all the analyses.

Results and Discussion

Univariate Analysis

The data distribution for the properties of cybersecurity measures as revealed on Table 1 shows that majority of the participants affirm to these items and indicators as substantially characterizing their behavior and the management of the interventionist agencies in Eastern Nigeria. Results indicate that most of the participants identify with cybersecurity measures as substantially expressed. Result from the analysis indicates that the indicator substantially reflected within the context of leadership in the target organizations, thus shaping and characterizing the organizations of interest.

Operational Efficiency

Analysis on the measures of organizational efficiency, as depicted on Table 2, affirm to the capacity of the ports in Eastern Nigeria for turnaround time, dwell time, and throughput. The result reflects the substantiality of the properties of operational efficiency, demonstrating its correspondence and relationship with the various elements and constituents of its environment. This is as the

outcome of the analysis reveals all mean distributions for the indicators to be above the adopted benchmark of x = 2; suggesting a general or average position that can be considered as agreeing to the variables of interest.

Table 1: Univariate Distribution for Indicators of Part Security Strategies

Dimensions	Indicators	N	Mean	Std. Deviation
Cybersecurity measures	The port utilizes secure digital systems for documentation and cargo tracking.	114	3.1228	1.31795
	Cybersecurity protocols such as firewalls and encryption are implemented in port operations.	114	2.9474	1.45640
	The port's ICT systems are regularly audited for security vulnerabilities.	114	3.1579	1.16421
	Cybersecurity breaches have negatively impacted stakeholder satisfaction in the past.	114	3.0351	1.34316
	Improved digital security has enhanced trust and satisfaction among port users.	114	3.1667	1.17433
	Valid N (listwise)	114		

Table 2: Univariate Distribution for Indicators of Operational Efficiency

Measures	Indicators	N	Mean	Std. Deviation
Turnaround Time	Ships berth and depart within scheduled time without unnecessary delays.	114	3.1316	1.32714
	Security screening of vessels is completed efficiently and without bottlenecks.	114	2.9737	1.48420
	Improved port security has positively affected vessel turnaround time.	114	3.2193	1.21027
	Delays in vessel handling are mostly due to poor coordination among agencies.	114	3.0614	1.37155
	Vessel turnaround is faster in ports with well-integrated security protocols.	114	3.1404	1.14349
Dwell time	Cargo is cleared within a reasonable time after arrival.	114	3.3246	1.34029
	Delays in cargo release are often caused by repeated security checks.	114	3.2105	1.22275
	Efficient security procedures reduce the time cargo spends in the terminal.	114	3.0000	1.30350
	Security agencies coordinate well to reduce cargo dwell time.	114	3.3070	1.32456
	Automated cargo clearance processes have helped reduce dwell time.	114	3.1491	1.15393
Throughput	The volume of cargo handled at the port has increased in recent years.	114	3.0263	1.37268
	Security measures in place facilitate faster handling of cargo and containers.	114	2.9474	1.49833
	The port is capable of processing large cargo volumes without significant delays.	114	3.1140	1.30864
	Throughput is negatively affected by inefficient security processes.	114	2.9386	1.51853
	Well-trained security personnel contribute to higher port throughput	114	3.1930	1.24714
	Valid N (listwise)	114		

Bivariate Analysis

Cybersecurity Measures and Operational Efficiency

The test for the significance of the relationship between cybersecurity and the measures of operational efficiency is examined and presented in Table 3. Result from the analysis shows that cybersecurity measures is an antecedent of all three measures of operational efficiency. This is as the outcome of the tests show that cybersecurity, significantly influences turnaround time (R= 0.998 and P = 0.000), dwell time (R= 0.986 and P = 0.000), and throughput (R= 0.987 and P = 0.000). The test shows that cybersecurity contributes significantly to the operational efficiency of the Ports in Eastern Nigeria. Thus, following the outcome of the analysis, and the evidence of significance in the relationship between the variables, all related null hypotheses are therefore rejected.

Table 3: Cybersecurity and the Dimensions of Operational Efficiency

		Cybersecurity Measures	Turnaround Time	Dwell Time	Throughput
Cybersecurity Measures	Pearson Correlation	1	0.998**	0.986**	0.987**
	Sig. (2-tailed)		0.000	0.000	0.000
	N	114	114	114	114
Turnaround Time	Pearson Correlation	0.998**	1	0.982**	0.989**
	Sig. (2-tailed)	0.000		0.000	0.000
	N	114	114	114	114
Dwell Time	Pearson Correlation	0.986**	0.982**	1	0.971**
	Sig. (2-tailed)	0.000	0.000		0.000
	N	114	114	114	114
Throughput	Pearson Correlation	0.987**	0.989**	0.971**	1
	Sig. (2-tailed)	0.000	0.000	0.000	
	N	114	114	114	114

Seaports in Eastern Nigeria were the subject of this research, which aimed to evaluate the relationship between cybersecurity measures and operational efficiency. Statistical analysis revealed a very favourable and statistically significant relationship between cybersecurity measures and operational efficiency as measured by cargo dwell time, ship turnaround time, and cargo throughput. The results of this study support the empirical stance taken by Al-Khatib, Ibrahim, and Alnadi (2025), who investigated the effect of cybersecurity practices on the efficiency of the supply chain in the banking sector of Jordan and concluded that such practices do, in fact, affect the efficiency of the supply chain in that sector. Ship turnaround times are decreased, operating expenses are lowered, and customer satisfaction is raised owing to predictable schedules as a result of efficient operations (Hart, 2019). The current results back up the claims that clear data protection policies and cybersecurity measures help lower an organization's risk levels (Ali, et al., 2025); and that cybersecurity measures, along with regulatory compliance, greatly improve financial performance, and that cybersecurity investments increase shareholder value (Aminu, 2024). Although there is considerable variety and long-term impacts, our results corroborate the claim that digital growth improves port security. In 2024, Ren and colleagues worked on

Conclusion and Recommendations

This study finds that cyber security measures are highly correlated with the operational efficiency of seaports in Eastern Nigeria, based on its findings and their coherence with comparable research. This conclusion emphasizes cyber security measures as a port security plan that monitors cyber risks inside a port and may progressively create an active environment for effective port operations. The study advised that port managers and stakeholders implement robust cyber defence strategies, encompassing regular vulnerability assessments, data encryption, and real-time network monitoring to enhance operational efficiency regarding cargo dwell time, ship turnaround time, and cargo throughput.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Credit Authorship Contribution Statement

Nkitma, A. N.: Conceptualization, Methodology, Formal analysis, Investigation, Resources, Data curation, Visualisation, Project administration, Writing - original draft, Review & Editing. **Wizor, C. H.**: Supervision, Methodology, Validation, Formal analysis, Data curation, Visualisation.

References

Aderinto,, A. A., & Adeniran, C. F. (2025). Cybersecurity threats and financial performance of listed commercial banks in Nigeria. *Asian Journal of Advanced Research and Reports 19* (4), 381-94.

Ahokas, J., Kiiski, T., Malmsten, J., & Ojala, L. (2017) Cybersecurity in ports: A conceptual approach. In: *Proceedings of the Hamburg International Conference of Logistics (HICL),* Hamburg, October 2017. Hamburg: epubli, pp. 343-359. DOI: 10.15480/882.1448.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. *Network, 2*(1), 123-138.

Ali, A., Zulfiqar, N., Usama, M., & Ikraam, R.M. (2025). Impact of cyber security measures on risk Mitigation, with the mediating role of data protection. *Indus Journal of Social Sciences, 3*(1), 356- 372

Al-Khatib, S. F., Ibrahim, Y. Y., & Alnadi, M. (2025). Cybersecurity practices and supply chain performance: The case of Jordanian banks. *Administrative Sciences, 15*(1), 1-27

Alzighaibi, A. R. (2021). Cybersecurity attacks on academic data and personal information: The mediating role of education and employment. *Journal of Computer and Communications, 9*(11), 77-90.

Aminu, M. A. (2024). Effect of cyber security measures on financial performance in listed food and beverage companies in Nigeria. *ANUK College of Private Sector Accounting Journal, 1*(2), 232-242.

Bunyamin, G., Gizem, K., & Pelin, B. (2021). Cyber security risk assessment for seaports: A case study of a Container port. *Cyber and Security Journal*. doi: 10.1016/j.cose.2021.102196

Chowdhury, N., Nystad, E., Reegård, K., & Gkioulos, V. (2022). Cybersecurity training in Norwegian critical infrastructure companies. *International Journal of Safety and Security Engineering.*

Cong, L. Z., Zhang, D., Wang, M. L., Xu, H. F., and Li, L. (2020). The role of ports in the economic development of port cities: Panel evidence from China. *Transportation Policy 90*, 13-21

El Imran, O., & Babounia, A. (2018). Benchmark and competitive analysis of port performances model: Algeciras Bay, Rotterdam, New York-New Jersey and Tangier Med. *European Journal of Logistics, Purchasing and Supply Chain Management, 6,* 28–48.

Farah, M. B., Al-Kadri, M., Ahmed, Y., Abouzariba, R., Benfarah, M., Alkadri, O., Ahmed, Y., & Bellekens, X. (2023). Cyber incident scenarios in the maritime industry: Risk assessment and mitigation strategies. *2023 IEEE International Conference on Cyber Security and Resilience* (CSR), 194-199.

Faria, D. L. (2020). The impact of cybersecurity on the regulatory legal framework for maritime security. Janus.net. Retrieved from https://www.researchgate.net/publication/347113237_The_impact_of_cybersecurity_on_the_regulatory_legal_framework_for_maritime_security

Fenton, A.J. (2024). Preventing catastrophic cyber-physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the straits of Malacca and Singapore. *Journal of Marine Science and Engineering, 12*(3), 510.

Fettermann, D., & Eltayeb, T. K. (2020). Port security in the age of digital transformation. *Journal of Marine Science and Engineering*, 8(9), 696.

Hart, K. (2019). *An analysis on cargo handling performance and its effect on turnaround time of liner ships (a case of Tema port).* Unpublished. Retreived 10th November, 2025 from; https://doi.org/10.13140/RG.2.2.12226.73922

Heilig, L., & Voß, S. (2017) Information systems in seaports: A categorization and overview. *Information Technology and Management, 18*(3), 179-201.

Homeland Security. (2018). *Examining physical security and cybersecurity at our nation's ports*. Washington: U.S. Government Publishing Office.

IMO (2019a). Air pollution, energy efficiency and greenhouse gas emissions. Retrieved from http://www.imo.org/en/OurWork/Environment/PollutionPrevention/AirPollution/Pages/Default.aspx.

IMO (2019b). AIS transponders. Retrieved from; http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx.

IMO (2019c). SOLAS XI-2 and the ISPS code. Retrieved from The International Ship and Port Facility (ISPS) Code: http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/ Pages/SOLAS-XI 2%20ISPS%20Code.aspx

Marques-Guedes A (2018) Cibersegurança no setor marítimo. *Revista de Marinha: marinha de comércio 1004*, 30–32.

Melnyk, O., Onyshchenko, S., Onishchenko, O.A., Lohinov, O.V., & Ocheretna, V. (2023). Integral approach to vulnerability assessment of ship's critical equipment and systems. *Transactions on Maritime Science*. Retrieved from https://www.researchgate.net/publication/371220089_Intergral_Approach_to_Vulnerability_Asse ssment_of_Ship%27s_Critical_Equipment_and_Systems.

Mensah, E. A., Nani, G., Akoto, L. S., & Anlesinya, A. (2023). Seaport security strategies and performance: Insights from emerging economies. *Journal of Marine Science and Engineering, 13*(119), 1–21. https://doi.org/10.3390/jmse13010119

Moerel, L., & Dezeure, F. (2017). *Cyber security in ports: Business as usual? Vlaams Nederlandse Delta.* Retrieved 15th November, 2025 from; http:// www.vndelta.eu/files/3215/1125/0649/Cyber_Security_in_Ports_Whitepaper_VND_vonference_ november_2017.pdf.

NIST. (2019). *Framework for improving critical infrastructure cybersecurity*. Retrieved 24th November, 2025, 2024, from https:// nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

Nnwaogbe, O. R., et al. (2023). Comparative study of Eastern Port operational performance. *Journal of Strategic Development Studies and Law*, 8(2), 153–163.

NPA (2016). Handbook. Retreived 12th November, 2025 from; www.nigerianports.org

Nwokedi, T. C., Ndikom, O. B., Okoroji, L. I., & Nwaorgu, J. (2021). Determinant port-related factors affecting the flow of shipping trade and logistics in Nigerian seaports. *LOGI – Scientific Journal on Transport and Logistics,12*(1), 261-270.

Nze, O. N., Ejem, A. E., & Nze, I. C. (2020). Benchmarking technical efficiency of Nigerian seaports. *Journal of Sustainable Development of Transport and Logistics, 5*(1), 77-95.

Ren, X., Shen, J., Feng, Z., Wang, X., & An, K. (2024). The Impact of digital development on port security resilience-An empirical study from Chinese provinces. *Sustainability, 16*, 1-17.

Roberts, K. H. (1990). Some characteristics of one type of high reliability organization. *Organization Science*, 1(2), 160–176.

Septian,E., T. Wibawa,T., Sularto, R.B., Endah,A.M., & Astuti, S. (2016). Kebijakan Non-Penal Penerapan Isps Code Dalam Pencegahan Tindak Kejahatan Di Pelabuhan Tanjung Priok. *Diponegoro Law Rev., 5*(2), 1-15.

UNCTAD (2019). United Nations Convention on Trade and Development, Maritime Transport Review, 2019 edition. Retrieved 15th November, 2025 from: http//www.unctad.org/maritime-transport/.

Walid, E., Newe, T., Ó. Eoin, & Gerard, D. (2017). Trust security mechanism for maritime wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*. Retrieved from;https://www.researchgate.net/publication/308274768_Trust_security_mechanism_for_maritime_ wireless_sensor_networks

Xiao, G.N., Wang, Y.Q., Wu, R.J., Li, J.P., & Cai, Z.Y. (2024). Sustainable maritime transport: A review of intelligent shipping technology and green port construction applications. *Journal of Maritime Science and Engineering 12* (10), 1728.