International Journal of Scientific Engineering and Science
Volume 10, Issue 9, pp. 47-55, September 2026. ISSN (Online): 2456-7361

Maritime Security Risks and Operational Performance of Nigerian Seaports: An Integrative Review and Quantitative Evidence Synthesis

Adeyemi Adetunji Samsideen[1], Oladosu Jubril Oloruntoba[2]*, Sonde Dimeji Rotimi[3], Babatunde Olasunkanmi Folasayo[4]
[1, 2, 4]Department of Transport Management, Ladoke Akintola University of Technology, Ogbomoso, Oyo State Nigeria
asadeyemi49@lautech.edu.ng, jooladosu@lautech.edu.ng, ofbabatunde@lautech.edu.ng
[3]Department of Transport Management, Olabisi Onabanjo University, Ago-Iwoye, Ogun State, Nigeria
sonde.dimeji@oouagoiwoye.edu.ng

***Abstract*—*Maritime insecurity is an operational issue for Nigerian seaports as seaborne attacks and poor port-security governance and enforcement can disrupt ship traffic, cargo processing, insurance risk and service quality. The existing studies have focused on piracy, port reform, regulatory compliance and supply-chain risk individually, with the relationship between security risk and port performance being not consolidated. This study is an integrative review with quantitative evidence synthesis of peer-reviewed studies published between 2011 and July 2026. Following a structured screening process, 22 studies were identified that had a direct connection to seaport or maritime-logistics performance, and a direct link to Nigeria or the Gulf of Guinea. The studies were coded in terms of year, method, geographic focus, threat category, operational consequence and mitigation response. The pattern of evidence was explored using frequencies, ages, cross-tabulations and exact significance tests. A total of 17 studies were on piracy and armed robbery, and five were on port security and governance. In 77.3% of the studies safety and human harm were mentioned, as well as trade or throughput effects. Cost escalation came in at 68.2% and delay at 63.6% and service-reliability at 63.6%. The most common mitigation response was governance coordination (72.7%), followed by legal enforcement (68.2%) and technology/operational visibility (63.6%). The evidence does not lend itself to a simple conclusion that an increase in security technology is directly correlated to an increase in port performance. Enforcement authority, use of information, operational risk routines and coordination between agencies and port stakeholders are crucial for effective outcomes. The study establishes a security-performance pathway connecting threats, exposure points, operational disruptions and measurable port outcomes, and it identifies priorities for future empirical research in Nigerian seaports.*

***Keywords*—** *Maritime security; seaport performance; piracy; port governance; supply-chain risk; Nigeria.*

I. INTRODUCTION

Maritime transport is essential for the transport of Nigeria's international trade and links importers, exporters, inland transport operators and industrial supply chains. The importance of a seaport is thus not restricted to the amount of cargo that passes through the docks. It also relies on the ability of ships to approach safely, the ability to process cargo without unnecessary exposure, and the ability of port users to anticipate the time and expense of transiting through the port. The studies on the reform of the Nigerian port have revealed that the institutional setup and terminal management can significantly affect the efficiency of the port, but the efficiency is limited by congestion and clearance delays and regulatory coordination problems (Akinyemi, 2016; Nwanosike et al., 2016). The security risk has an additional dimension as it affects the conditions in which shipping lines, terminal operators and cargo owners plan their operations.

Moreover, the maritime insecurity in the Nigerian coast has been studied primarily by focusing on piracy, armed robbery at sea, kidnapping of crews, oil related crime and poor enforcement across the Gulf of Guinea. The political economy literature does not view these threats as standalone attacks on ships, but as part of onshore criminal networks and illicit markets and institutional weakness (Perouse de Montclos, 2012; Peters, 2020). More recent research has also demonstrated that there are economic impacts beyond loss. Shipping firms could be required to make further security investments, insurance costs could increase, port calls could be delayed, and trade planning could be uncertain, and coastal states could lose investments and port competitiveness (Okafor-Yarwood and Pigeon, 2021; Yercan et al., 2026). These consequences establish a direct connection between maritime security and logistics performance.

However, the conditions within the port system also influence port security. Compliance to the International Ship and Port Facility Security framework is dependent on leadership, communication and enforcement (Okoroji and Ukpere, 2011) and the framework gives a standard for the protection of facilities, access control and security planning. Studies of port governance show that the formal reform does not necessarily eliminate the fragmentation of responsibilities or informal practices (Onwuegbuchunam, 2018). On the practical side, a ship can arrive safely in Nigerian waters and yet still be delayed due to anchorage controls, access restrictions, documentation issues or sub-optimal inspections. Maritime security is thus a continuum from approaches to terminals to cargo evacuation.

The evidence available is extensive but scattered. Piracy studies tend to focus on reasons and regional security measures, whereas port-performance studies focus on productivity, governance and infrastructure. Supply-chain risk

studies explore operational practice, and they are not often related to consistent measures like vessel waiting time, cargo dwell time, throughput variation, loss exposure or schedule reliability (Nsikan et al., 2023). This separation complicates the identification of the most operationally critical security risks and the extent to which security mitigation measures have been assessed and recommended.

Therefore, this study seeks to redress this by examining one defined relationship; maritime security risks and operational performance of Nigerian Seaports. It incorporates evidence on piracy, armed robbery, port security and governance, and only studies which demonstrate a clear Nigerian component and an operational maritime and/or port implication. The contribution is threefold: It offers a clear picture of the existing evidence, quantifies the incidence of operationally reported consequences and mitigation, and outlines a security-performance pathway that could be used to inform future measurement. Not all recommendations are considered to be proven interventions in the review. Instead, it differentiates between measures that are often recommended and outcomes for which there is empirical evidence.

II. 2LITERATURE REVIEW

2.1 Maritime security risk

Maritime security risk is the likelihood and impact of intentionally or governance-related events that pose a threat to ships, crews, cargo, port infrastructure and maritime services. In the Nigerian context, piracy and armed robbery has received the most attention, with incidents involving violent boarding, crew kidnapping, cargo theft and attacks connected with the overall criminal activity of the Niger Delta. The literature reveals that the risk is organised through both offshore and onshore means, such as access to weapons, intelligence, illegal markets, and local protection networks (Nwalozie, 2020; Jacobsen and Rasmussen, 2024). This broader structure helps to account for the fact that the presence of patrols alone does not necessarily lead to a decrease in opportunity in one place without a decrease in the conditions that support attacks at another.

There are also risks in port governance. Facility access, cargo documentation, gate operations, anchorage control and regulatory inspection can be exposure points caused by overlapping responsibilities or due to lax security procedures. Improvement in attention to formal security planning was achieved by the implementation of the ISPS Code in Nigeria, whereas the quality of compliance is subject to management commitment and communication (Okoroji and Ukpere, 2011). Institutional analysis of governance also reveals that port reforms redefine port functions without necessarily addressing coordination problems (Onwuegbuchunam, 2018). Security risk in ports is thus a physical and institutional problem.

2.2 Operational performance of seaports

The operational performance is the capacity of a port to accommodate ships and goods within reasonable time, cost, safety and reliability. Typical examples are cargo volumes, shipping vessel turnaround time, berth productivity, cargo dwell time, truck turnaround time, service reliability and the cost of port use. Much of the Nigerian port research has focused on the reform of the port, its physical dimensions and terminal productivity. The post-reform productivity analysis indicated efficiency improvement; however, technical progress and operational coordination was not uniform (Nwanosike et al., 2016). The berth characteristics have been recently investigated, and their significance for the operational results has been reinforced, including depth, quay length, number of berths and cargo specific areas (Dere et al., 2025).

Security impacts these indicators both directly and indirectly. An attack that results in an injury, the loss of cargo, diversion or the suspension of operations is a direct pathway. Indirect pathway is where perceived risk results in extra inspections, security charges, change of schedules, anchorage or no call at the port. Even if the incident numbers are down, the indirect effects may linger, as insurance pricing and internal company rules and risk perceptions may take a while to catch up. Any assessment of port performance needs to be considered in the light of the actual incidents as well as the preventive measures implemented in response to them.

2.3 Security-Performance Pathways

The first pathway is the increase in costs. Exposure to piracy may lead to higher security spending, crew-protection costs, insurance premiums and cost of compliance measures. These costs can be passed on as freight charges, terminal charges or cargo handling charges. The second pathway is time disruption, such as late arrivals, rerouting, extra clearance processes and longer anchorage or terminal stays. The third is the loss of reliability, when shipping lines, freight forwarders and cargo owners are unable to predict schedules or service completion. The fourth pathway is throughput and trade effect, which involves the reduction of port calls, investment or competitiveness of maritime trade due to sustained insecurity (Okafor-Yarwood and Pigeon, 2021; Ehizuelen, 2025).

There is another pathway related to safety and human harm. Personal consequences of kidnapping, assault and fatal attacks cannot be reduced to a monetary indicator. They also influence the decisions on crewings, voyage planning and the seafarers' interest in accepting crewings in high-risk waters. Anele (2016) highlighted the contribution of seafarers in combating piracy, and incident datasets have enhanced the capacity to study the spatial and temporal dimension of piracy attacks (Moura et al., 2023; Liang et al., 2024). However, better incident data do not necessarily result in port-performance measures unless they are tied to vessel movement, cargo and terminal records.

2.4 Institutional coordination and resilience

Resilience is about being able to prepare for disruption, to continue to deliver critical services, to recover and adapt. This capability is different from resistance, as a system might not be able to prevent all events, but it can minimize the impact they have on the system (Ponomarov and Holcomb, 2009; Tukamuhabwa et al., 2015). Resilience in maritime logistics can include surveillance, sharing intelligence, law enforcement, plans for facilities, contingency routing, incident reporting, cargo visibility and coordinating stakeholders.

However, the effectiveness of these measures hinges on their ability to decrease response time, reduce recurrence or ensure continuity of service.

Regional coordination is a key requirement highlighted in the literature of the Gulf of Guinea. There is a lack of national enforcement if the attacks cross jurisdictions or information is not shared promptly. Ukeje (2015), Oyewole (2016) and Schandorf (2024) all indicate that the effectiveness of regional security arrangements is influenced by institutional capacities and information infrastructure. The importance of legal measures is also significant as it undermines deterrence if there is no real prosecution of arrests. Technology can enhance detection, but needs to be coupled with authority, trained people and procedures. This combination provides the basis for the evidence synthesis in the present review.

2.5 Empirical Gap

While many good security countermeasures are proposed in the literature, and many theories are advanced on the causes of piracy, fewer studies report on the impact of insecurity on port operations using consistent metrics. Some quantitative studies rely upon incident data or institutional variables, whereas port studies rely upon productivity and governance measures. A small fraction of the evidence is directly related to security incidents and vessel delay, cargo throughput, insurance spending or service reliability. This gap makes it difficult to make causal interpretation and makes the comparison across Nigerian seaports difficult. This is addressed by the present study using quantitative content analysis. It is not possible to transform heterogeneous studies into a common effect size because their design and results are not sufficiently comparable. It does not, however, indicate which operational implications and mitigation measures are reported, how the evidence is spread by method and threat category, and where evidence is lacking. The method offers a more structured framework for empirical studies in the future.

III. MATERIALS AND METHODS

3.1 Research Design

An integrative review with quantitative content analysis was adopted in this study. Integrative reviews are appropriate when the evidence consists of both qualitative and quantitative studies, mixed-method studies and data-oriented studies, as long as the search, selection, and synthesis procedures are clearly described (Whittemore and Knafl, 2005; Torraco, 2016). The reporting structure also reflected the transparency of PRISMA and PRISMA-ScR, but instead of meta-analysis, it was used to evidence integrate (Tricco et al., 2018; Page et al., 2021). The f analysis was a peer-reviewed journal article. Each article included was coded once based on the predominant method, most prominent threat category, primary geographic focus, and operational implications and mitigation measures reported. Multiple outcome and mitigation codes assigned to a study were possible due to the design which enabled more than one consequence or recommendation to be reported in a single article.

3.2 Search strategy and eligibility

Academic publisher platforms, journal websites and scholarly search services (ScienceDirect, SpringerLink, Taylor and Francis Online, Wiley Online Library, Emerald Insight, Crossref-linked records, and Google Scholar) were searched. The principle query was a combination of location, security and performance terms: (Nigeria OR "Gulf of Guinea") AND (port OR seaport OR maritime OR shipping) AND (security OR piracy OR "armed robbery" OR governance OR ISPS OR risk) AND (performance OR throughput OR delay OR reliability OR logistics OR "supply chain"). Relevant studies were also listed and checked back to identify earlier articles. Articles were considered where they were published in English between January 2011 and 24 July 2026 and were peer reviewed with a clear Nigerian element or a Gulf of Guinea analysis with material relevant to Nigeria and maritime security/port-security governance was linked to an operational, trade, safety or logistics outcome. Conference abstracts, theses, news reports, institutional commentary and studies without a clear method were excluded. Port-performance studies were only kept if their governance or operational conclusions helped to interpret security-related performance.

3.3 Screening and data extraction

A more general search yielded 53 candidate records. Four duplicates were removed and 49 titles and abstracts were screened. At that stage, 7 records were excluded and 42 full-texts were evaluated. Five full texts were excluded because they did not meet the methodological and/or geographic requirements, resulting in 37 logistics-security studies. A second scope filter excluded 15 studies primarily focused on logistics of roads, energy or health. There were 22 studies in the final maritime and port evidence set. The publication year, study method, geographical focus, primary threat category, operational consequences and mitigation responses were recorded on a structured coding sheet. Operational consequences were coded as cost escalation, delay or variation in lead-time, safety and human harm, and trade or throughput effect and service-reliability effect. Mitigation responses were categorized as governance coordination, legal enforcement, technology and visibility, operational risk-management routines, community engagement and infrastructure resilience. Where the article reported or commented on the item, a code was assigned.

3.4 Data Analysis

Frequencies and ages were used to describe the evidence base. The association between threat category and study method was analyzed through cross-tabulation. The quantitative and mixed-method studies were grouped together and the qualitative and review or data studies were grouped together as the comparison group. Pearson's chi-square, continuity correction and Fisher's exact test were reported. Fisher's exact result was accorded more interpretive weight, as one of the expected cell counts was less than five. The strength of association was described by Cramer's V. Meta-analysis was not performed due to differences in the units, outcomes and analysis designs used by the studies.

International Journal of Scientific Engineering and Science
Volume 10, Issue 9, pp. 47-55, September 2026. ISSN (Online): 2456-7361

IV. RESULTS

4.1 Study selection

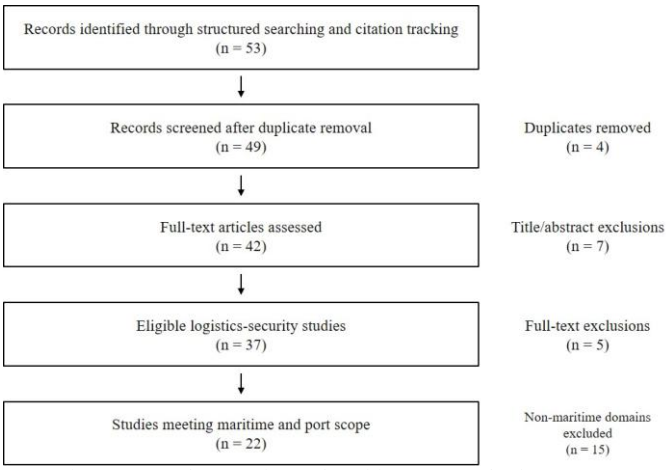

Figure 1. Search, screening and maritime-scope selection process.

The final set of 22 studies provides a focused record of Nigerian maritime and port-security research. The two-stage scope filter was necessary because the earlier evidence base combined maritime, road and energy logistics. Restricting the present article to maritime and port studies improved conceptual clarity and allowed the reported operational outcomes to be interpreted within one transport system.

4.2 Characteristics of the included studies

TABLE 1. Profile of included studies (n = 22)

Dimension	Category	Frequency	%
Method	Qualitative	12	54.5
Method	Quantitative	8	36.4
Method	Mixed methods	1	4.5
Method	Review/data	1	4.5
Geographic focus	Regional/Gulf of Guinea	11	50.0
Geographic focus	National	5	22.7
Geographic focus	South-South	4	18.2
Geographic focus	South-West	1	4.5
Geographic focus	Global with Gulf of Guinea	1	4.5
Primary threat	Piracy/armed robbery at sea	17	77.3
Primary threat	Port security/governance	5	22.7

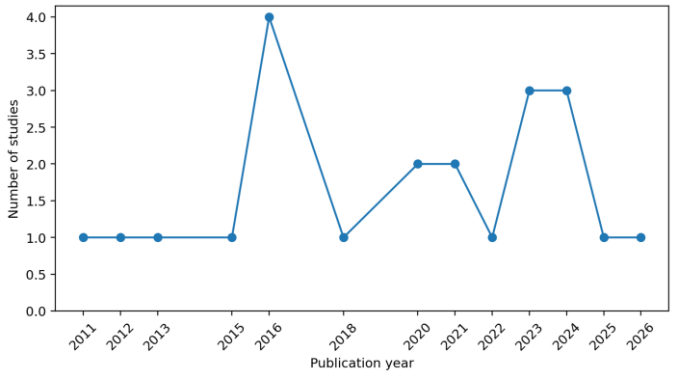

Figure 2. Publication trend of the included evidence, 2011-2026.

Qualitative studies formed the largest methodological group, accounting for 12 articles or 54.5 %. Eight studies were quantitative, one used mixed methods and one was a data article. The regional Gulf of Guinea perspective accounted for half of the evidence, while five studies used a national Nigerian focus and four concentrated on the South-South region. Seventeen studies examined piracy or armed robbery at sea, compared with five that centred on port security and governance. Publication activity was uneven, but the evidence became more frequent after 2020.

The distribution confirms that Nigerian maritime-security scholarship remains more developed in the explanation of piracy than in the direct measurement of port operations. Port-security and governance studies were fewer, although they were more likely to use quantitative measures. This difference becomes relevant when the method and threat categories are compared.

4.3 Reported operational consequences

TABLE 2. Frequency of reported operational consequences

Operational consequence	Frequency	% of studies
Safety and human harm	17	77.3
Trade or throughput effect	17	77.3
Cost escalation	15	68.2
Delay or lead-time variability	14	63.6
Service reliability effect	14	63.6

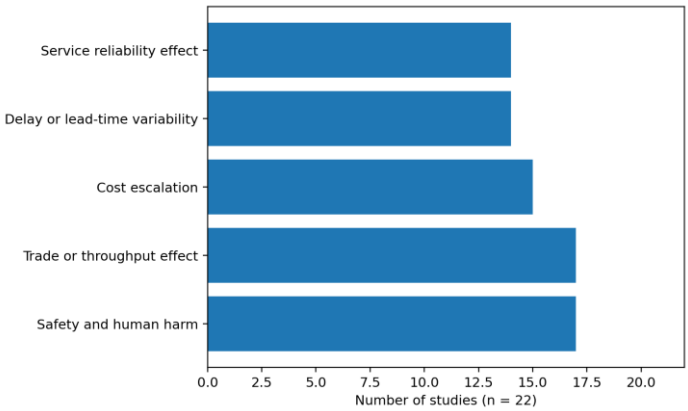

Figure 3. Reported operational consequences in the included studies.

TABLE 3. Operational consequences by primary threat category

Operational consequence	Piracy/armed robbery n (%)	Port security/governance n (%)	Total n	Total %
Safety and human harm	16 (94.1)	1 (20.0)	17	77.3
Trade or throughput effect	13 (76.5)	4 (80.0)	17	77.3
Cost escalation	12 (70.6)	3 (60.0)	15	68.2
Delay or lead-time variability	10 (58.8)	4 (80.0)	14	63.6
Service reliability effect	9 (52.9)	5 (100.0)	14	63.6

Safety and human harm were mentioned in 17 studies (77.3 % of the evidence). Trade or throughput effects were mentioned as often as were other effects. Cost escalation was reported in 15 studies and delay in 14 studies, and service-reliability effects in 14 studies. The findings show that maritime insecurity is not only viewed as threat to life and

property. The majority of studies also relate it to commercial and operational consequences.

However, the pattern varies depending on the threat. Often reported piracy studies included crew exposure, trade uncertainty and extra security cost. Delay, reliability, throughput and efficiency of terminal operations were given more attention in port-security and governance studies. Overlap is key, as security at sea can impact port calls and scheduling, and weaknesses in the port can compound the time and cost impacts of external maritime risk.

4.4 Relationship between threat category and study method

TABLE 4. Primary threat category by grouped study method

Primary threat	Quantitative or mixed	Qualitative or review	Total
Piracy/armed robbery at sea	5	12	17
Port security/governance	4	1	5
Total	9	13	22

TABLE 5. Tests of association

Test	Value	df	Asymptotic significance (2-sided)	Exact significance (2-sided)
Pearson chi-square	4.090	1	0.043	
Continuity correction	2.265	1	0.132	
Fisher's exact test				0.116
Cramer's V	0.431			

The Pearson chi-square result indicated that there was a relationship between threat category and grouped study method, but the expected-frequency condition was not completely met. The Fisher's exact test was not significant at the 5 % level ($p = 0.116$). Thus, the evidence does not provide an acceptable association between type of threat investigated and quantitative or qualitative approach. With a small sample, the moderate Cramer's V value should be interpreted only as descriptive.

The pattern in the cross-tabulation is still helpful. Quantitative methods were used in four of the five port-security and governance studies, while the majority of the piracy studies took the qualitative and review approach. This imbalance can be attributed to the fact that the literature offers detailed information on the drivers and institutional issues of piracy, while only a few directly comparable estimates of delay, cost and throughput effects are available.

4.5 Mitigation practices

TABLE 6. Frequency of reported mitigation practices

Mitigation practice	Frequency	% of studies
Governance and interagency coordination	16	72.7
Legal and regulatory enforcement	15	68.2
Technology and operational visibility	14	63.6
Operational risk-management routines	8	36.4
Community engagement and local intelligence	7	31.8
Infrastructure resilience investment	4	18.2

The most common mitigation theme was governance and interagency coordination (16 studies or 72.7%). Legal and regulatory enforcement was mentioned in 15 studies and technology and operational visibility was mentioned in 14 studies. Operational risk-management routines were identified in eight studies, community engagement in seven and infrastructure resilience in four.

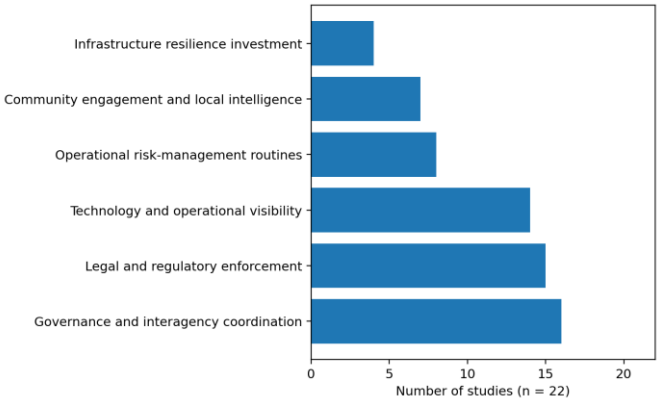

Figure 4. Mitigation practices reported in the included studies.

Based on the result it can be seen that the literature do not offer technology as a complete solution. Coordination, enforcement and operational response are typically addressed in connection with surveillance, tracking and information systems. Studies on the port supply chain are more visible in firm-level practices including risk assessment, disruption records, cargo-status updates and stakeholder relationship management, compared to the broader piracy literature (Nsikan et al., 2023). Community engagement is included largely in the context of piracy's relationship with onshore support networks and local economies.

V. DISCUSSION

The study clearly relates maritime security risk and seaport performance, and the evidence is more explanatory than causal in measuring. Safety harm, trade effects, cost escalation, and delay/reliability loss are most commonly identified in most studies, but operational indicators are not common among them. This is in line with the argument that Gulf of Guinea piracy has economic impacts, direct and indirect (Okafor-Yarwood and Pigeon, 2021; Yercan et al., 2026). It also illustrates the importance of not relying on the reduction of incidents as evidence of port performance. A port user can pay a higher security cost, and/or be subject to schedule precautions, for fewer attacks, even if the attacks occurred during a prior period of risk.

In the political economy of maritime crime in the Gulf of Guinea, Nigeria is the dominant country in studies of piracy. According to Perouse de Montclos (2012), Nwalozie (2020) and Peters (2020) piracy is an organised activity that is backed by other criminal and commercial networks. Jacobsen and Rasmussen (2024) provide an additional explanation in the form of the connection between piracy and the gun economy of the Niger Delta. Normally these studies do not correlate incident events to the arrival of a vessel, anchorage, berth or cargo records, but are important causal accounts. Thus the research field is better informed about the reasons for piracy

than what is known about the impact of piracy on the operations of specific ports, in terms of size and duration.

The port-governance evidence is less substantial and more closely related to operational performance. Akinyemi (2016) and Nwanosike et al. (2016) indicate that reform can enhance the efficiency, and Onwuegbuchunam (2018) indicates that the governance design is still relevant to the performance of terminals. Furthermore, Okoroji and Ukpere (2011) indicate that leadership and communication are crucial in formal security compliance. This indicates that security and efficiency must not be treated as distinct port functions. Security procedures that are poorly coordinated can cause delays, while inadequate security can result in a loss of confidence and expose cargo. So, the real operational question is not whether a control is in place or not, but how good and when does the security intervention occur?

A high frequency of trade and throughput effects is important. Maritime insecurity can deter port calls, change shipping practices and deter investments, especially when risk is added to congestion and unpredictable clearance. Ehizuelen (2025) correlates piracy with the trade goals of the African Continental Free Trade Area and Yercan et al. (2026) consider insurance, security spending and port inefficiency as broader economic costs. The impacts of these are likely to be manifested through multiple channels simultaneously for the Nigerian seaports. The performance loss can manifest itself as a drop in call frequency, extended buffers in shipping schedules, increased landed cost or decreased reliability as opposed to a loss per se.

Safety/human harm was the most common operational impact, in addition to trade and throughput. This finding validates the notion that the security policy can't be measured by cargo or financial metrics alone. Crew kidnapping and violent attacks have an impact on seafarer welfare, voyage acceptance and shipboard practices. The studies of Anele (2016) and Moura et al. (2023) and Liang et al. (2024) reveal that seafarers are not passive in prevention and that more systematic data on incidents can be useful. The next step in the analysis is to link the data with operational records to evaluate safety intervention in terms of response time and voyage disruption and recurrence.

The most prevalent mitigation practice was governance coordination. This finding aligns with regional research that has revealed that one of the major limitations is the existence of fragmented authority and poor information sharing (Ukeje, 2015; Oyewole, 2016). Schandorf (2024) suggests that information infrastructure is essential for counter-piracy coordination, and without it, there are no counter-piracy institutions. The discovery has a practical implication for Nigeria. Surveillance data must be disseminated to an agency with a clearly defined response mandate and port stakeholders must be aware of how security information impacts decisions regarding vessels, terminals and landside. But in the absence of this link, technology can generate more data, and more disruption.

Legal enforcement was also in the foreground. Deterrence is based on credible investigation, prosecution and consistent rules throughout the maritime area. Denton and Harris (2022) connect the piracy outcomes to military capacity and institutions, while Triantafillou et al. (2023) recognize the institutional and legal conditions as relevant determinants. So, legal reform should be assessed by operational indicators including the time to process cases, the rate of repeat incidents and how quickly security alerts are cleared. The number of arrests or legal provisions would not be a sufficient measurement if not considered in the light of their impact on maritime operations.

Nearly 2/3 of the evidence included references to technology and visibility. Tracking, surveillance and incident platforms help to detect and understand what is happening, and the effectiveness of these platforms requires good data, interoperability and timely responses. Nsikan et al. (2023) situate technology in the wider context of a range of port risk-management practices, such as disruption records, feedback mechanisms and stakeholder relationships. This helps to make a layered approach to the use of technology, where technology enables visibility, operational routines enable interpretation, and governance structures enable action.

Less commonly mentioned than governance, legal and technology responses, community engagement was nevertheless important where offshore attacks require onshore engagement. Political Economy studies show that maritime crime is affected by local networks, livelihoods and illicit markets. Community-based intelligence and grievance systems can thus enhance early warning, provided they are legitimate and protected for their participants. There is no evidence that community engagement can replace enforcement. It's best thought of as a piece of the puzzle in a greater security system.

The exact test should also be interpreted with caution if it's not significant. Does not indicate that method is independent of research focus in the broader universe of studies. It indicates that it is not possible to draw any statistically valid conclusions based on the current sample size. The descriptive trend holds true: port-governance studies are more quantitative; piracy studies are more qualitative. A full-fledged evidence base should integrate these strengths and connect explanatory accounts of criminal and institutional mechanisms with measurable port outcomes.

VI. Security-Performance Framework and Implications

6.1 Security-performance pathway

There are four stages of pathway supported by the evidence. The first stage is the threat source, such as piracy, armed robbery risk, cargo theft risk, weak access control and fragmented enforcement. The second phase is the exposure point, coastal approaches, anchorages, vessel boarding points, terminal yards and information systems. The third stage is operational disruption—diversion, delay, extra inspection, loss of cargo, security spending or interruption of service. The end result is the port measurable, like vessel waiting time, cargo dwell time, throughput, port call frequency, insurance cost, cargo claims and schedule reliability.

This pathway does not end up with recommendations being viewed as outcomes. A surveillance system is an

intervention, not evidence of performance improvement. It should be tested in changes of detection time, response time, event recurrence and operational loss. This is also true of legal reform, patrol activity, facility plans and community programmes. There must be a clear outcome and a time of comparison for each measure.

6.2 Managerial implications

A joint register of security-performance should be kept by port authorities and terminal operators. The register should be correlated with verified security incidents and security alerts with vessel, cargo and terminal information. It should at a minimum include information such as event time, location, operation affected, time to respond, time to delay, direct loss and recovery action. This would enable the cost of security to be evaluated as avoided delay and loss and not just as a compliance cost.

There is a need for shipping lines and port users to differentiate between structural and security-related delay. Congestion can happen along with the weather, and documentation and security intervention can happen at the same time, but they need different reactions. A standard delay code in port community systems would help to attribute and minimize the danger of putting the blame for all operational issues on insecurity. It also would enable more realistic negotiations on insurance and service terms.

6.3 Policy implications

National maritime agencies should establish information-sharing procedures, which include the list of who is alerted, who has authority to take action, and how the result is documented. National implementation is key to whether or not shared information will have an impact on operations, although regional arrangements in the Gulf of Guinea are still required. Legal enforcement should be linked to incident data to assess if enforcement and sanctions deter reoccurrence in specific sites and/or affect patterns. Moreover, there should also be independent evaluation of major security programmes, supported by policy. National incident totals alone should not be used to make an evaluation, as this could be due to displacement, under-reporting or regional trends. Programme indicators can be used to measure the extent to which a vessel's confidence is enhanced, waiting is reduced, loss exposure is decreased or service is stabilised as a result of a programme. It would enhance accountability and investment decisions if such evidence were available.

VII. Limitations

There are four limitations of the study. To begin with the evidence is heterogeneous and does not support a pooled effect size. Secondly, some papers mention operational implications without providing similar numerical results. Thirdly, where Nigeria was clearly a part of the analysis, the inclusion of Gulf of Guinea studies was necessary, but the results of the regions cannot always be solely attributed to the Nigerian seaports. Fourth, the coding does not indicate the magnitude or quality of the reported effect, just if an outcome or mitigation theme was reported. There are also few studies that have been conducted, which limits inferential analysis. Thus, the exact test was preferred to Pearson test and no causal claim was made on the cross tabulation. These restrictions do not detract from the usefulness of the study. They define exactly what are the measurement issues that future research needs to tackle.

VIII. Conclusion and Recommendations

Safety harm, trade uncertainty, cost escalation, delay and reduced service reliability are all maritime security risk factors that impact the performance of the Nigerian seaports. The evidence examined reveals that the literature is more focused on piracy and armed robbery and the direct analysis of port-security governance is less prevalent. The most common suggestions for addressing them are governance coordination, legal enforcement and technology, but these need to be integrated in operations and show measurable impacts. Furthermore, the main conclusion is that Nigeria is not lacking of maritime-security initiatives. The biggest weakness is the lack of linkage between security action and port-performance data. As such, security programmes should be measured by means of vessel waiting time, cargo dwell time, port-call reliability, response time, cargo loss, insurance cost and incident recurrence. The security-performance register should be common to all maritime agencies, port authorities and terminal operators. Standard codes for security related disruption should be included in port community systems. There is a need to conduct independent pre and post evaluations of major surveillance and enforcement programmes and to integrate community intelligence with formal response procedures. Future research should integrate the information on incidents with data on vessels and terminals in order to estimate the impact of maritime insecurity on Nigerian seaports.

References

[1] Akinyemi, Y. C. (2016). Port reform in Nigeria: Efficiency gains and challenges. *GeoJournal, 81*, 681-697. Retrieved from: https://doi.org/10.1007/s10708-015-9657-z

[2] Anele, K. K. (2016). A study of the role of seafarers in combating piracy off the coast of Nigeria. *WMU Journal of Maritime Affairs, 15*, 257-271. Retrieved from: https://doi.org/10.1007/s13437-016-0111-y

[3] Denton, G., & Harris, D. (2021). The impact of illegal fishing on maritime piracy: Evidence from West Africa. *Studies in Conflict and Terrorism, 44*(7), 593-614. Retrieved from: https://doi.org/10.1080/1057610X.2019.1594660

[4] Denton, G., & Harris, D. (2022). Maritime piracy, military capacity, and institutions in the Gulf of Guinea. *Terrorism and Political Violence, 34*(2), 405-425. Retrieved from: https://doi.org/10.1080/09546553.2019.1659783

[5] Dere, I. G., Ojekunle, J. A., & Sanni, L. M. (2025). Analysis of the effects of berth characteristics on operational performance of Nigerian seaports. *Journal of Shipping and Trade, 10*, 26. Retrieved from: https://doi.org/10.1186/s41072-025-00216-0

[6] Ehizuelen, M. M. O. (2023). Assessing the national and regional effectiveness of countering maritime piracy in the Gulf of Guinea. *GeoJournal, 88*, 3549-3574. Retrieved from: https://doi.org/10.1007/s10708-022-10823-0

[7] Ehizuelen, M. M. O. (2025). Assessing the possible influence of maritime piracy on the African Continental Free Trade Area in Nigeria. *Journal of Shipping and Trade, 10*, 30. Retrieved from: https://doi.org/10.1186/s41072-025-00215-1

[8] Hosseini, S., Ivanov, D., & Dolgui, A. (2019). Review of quantitative methods for supply chain resilience analysis. *Transportation Research Part E: Logistics and Transportation Review, 125*, 285-307. Retrieved from: https://doi.org/10.1016/j.tre.2019.03.001
[9] Ivanov, D., & Dolgui, A. (2020). Viability of intertwined supply networks: Extending the supply chain resilience angles towards survivability. *International Journal of Production Research, 58*(10), 2904-2915. Retrieved from: https://doi.org/10.1080/00207543.2020.1750727
[10] Jacobsen, K. L., & Rasmussen, J. J. (2024). Piracy and the broader gun business in the Niger Delta. *International Affairs, 100*(6), 2603-2620. Retrieved from: https://doi.org/10.1093/ia/iiae165
[11] Liang, M., Li, H., Liu, R. W., Lam, J. S. L., & Yang, Z. (2024). PiracyAnalyzer: Spatial-temporal patterns analysis of global piracy incidents. *Reliability Engineering and System Safety, 243*, 109877. Retrieved from: https://doi.org/10.1016/j.ress.2023.109877
[12] Moura, J. V. C., Kolden, L., & Yang, Z. (2023). A dataset of maritime piracy attacks in the Gulf of Guinea from 2010 to 2021. *Scientific Data, 10*, 770. Retrieved from: https://doi.org/10.1038/s41597-023-02706-x
[13] Nsikan, J., Rawlings, M., Ogbari, M., Ariyo, A., Briggs, I., & Inegbedion, D. (2023). Robust practices for managing maritime supply chain risks: A survey of Nigeria's seaports. *The Asian Journal of Shipping and Logistics, 39*(4), 1-7. Retrieved from: https://doi.org/10.1016/j.ajsl.2023.09.001
[14] Nwalozie, C. J. (2020). Exploring contemporary sea piracy in Nigeria, the Niger Delta and the Gulf of Guinea. *Journal of Transportation Security, 13*, 159-178. Retrieved from: https://doi.org/10.1007/s12198-020-00218-y
[15] Nwanosike, F. O., Tipi, N. S., & Warnock-Smith, D. (2016). Productivity change in Nigerian seaports after reform: A Malmquist productivity index decomposition approach. *Maritime Policy and Management, 43*(7), 798-811. Retrieved from: https://doi.org/10.1080/03088839.2016.1183827
[16] Okafor-Yarwood, I., & Pigeon, M. (2021). Stable seas, unstable ports: The impact of piracy on maritime trade in the Gulf of Guinea. *Maritime Economics and Logistics, 23*(4), 602-622. Retrieved from: https://doi.org/10.1057/s41278-021-00203-3
[17] Okoroji, L. I., & Ukpere, W. I. (2011). The International Ship and Port Facility Security Code: Its relevance and impact on port security in Nigeria. *African Journal of Business Management, 5*(31), 12313-12319. Retrieved from: https://doi.org/10.5897/AJBM10.1474
[18] Onuoha, F. C. (2013). Piracy and maritime security in the Gulf of Guinea: Nigeria as a microcosm. *Journal of the Middle East and Africa, 4*(3), 267-290. Retrieved from: https://doi.org/10.1080/21520844.2013.862767
[19] Onwuegbuchunam, D. E. (2018). Assessing port governance, devolution and terminal performance in Nigeria. *Logistics, 2*(1), 6. Retrieved from: https://doi.org/10.3390/logistics2010006
[20] Oyewole, S. (2016). Suppressing maritime piracy in the Gulf of Guinea: Prospects and challenges. *Australian Journal of Maritime and Ocean Affairs, 8*(4), 298-310. Retrieved from: https://doi.org/10.1080/18366503.2016.1217377
[21] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ, 372*, n71. Retrieved from: https://doi.org/10.1136/bmj.n71
[22] Perouse de Montclos, M.-A. (2012). Maritime piracy in Nigeria: Old wine in new bottles? *Studies in Conflict and Terrorism, 35*(7-8), 531-541. Retrieved from: https://doi.org/10.1080/1057610X.2012.684651
[23] Peters, B. C. (2020). Nigerian piracy: Articulating business models using crime script analysis. *International Journal of Law, Crime and Justice, 62*, 100410. Retrieved from: https://doi.org/10.1016/j.ijlcj.2020.100410
[24] Ponomarov, S. Y., & Holcomb, M. C. (2009). Understanding the concept of supply chain resilience. *International Journal of Logistics Management, 20*(1), 124-143. Retrieved from: https://doi.org/10.1108/09574090910954873
[25] Schandorf, S. O. (2024). Reimagining counter-piracy efforts in the Gulf of Guinea: Lessons from the theory of infrastructure for coordination and information sharing. *African Security Review, 33*(4), 403-419. Retrieved from: https://doi.org/10.1080/10246029.2024.2373110
[26] Snyder, H. (2019). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-339. Retrieved from: https://doi.org/10.1016/j.jbusres.2019.07.039
[27] Torraco, R. J. (2016). Writing integrative literature reviews: Using the past and present to explore the future. *Human Resource Development Review, 15*(4), 404-428. Retrieved from: https://doi.org/10.1177/1534484316671606
[28] Triantafillou, A., Bardaka, I., Vrettakos, I., & Zombanakis, G. (2023). Maritime piracy: Determining factors and the role of deterrence. *African Security Review, 32*(2), 166-183. Retrieved from: https://doi.org/10.1080/10246029.2023.2179411
[29] Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac, D., et al. (2018). PRISMA extension for scoping reviews: Checklist and explanation. *Annals of Internal Medicine, 169*(7), 467-473. Retrieved from: https://doi.org/10.7326/M18-0850
[30] Tukamuhabwa, B. R., Stevenson, M., Busby, J., & Zorzini, M. (2015). Supply chain resilience: Definition, review and theoretical foundations for further study. *International Journal of Production Research, 53*(18), 5592-5623. Retrieved from: https://doi.org/10.1080/00207543.2015.1037934
[31] Ukeje, C. (2015). The Abuja Declaration and the challenge of implementing a maritime security strategy in the Gulf of Guinea and the South Atlantic. *Journal of the Indian Ocean Region, 11*(2), 220-235. Retrieved from: https://doi.org/10.1080/19480881.2015.1074784
[32] Whittemore, R., & Knafl, K. (2005). The integrative review: Updated methodology. *Journal of Advanced Nursing, 52*(5), 546-553. Retrieved from: https://doi.org/10.1111/j.1365-2648.2005.03621.x
[33] Yercan, F., Cetin, O., & Conguloglu, R. (2026). The economic impact of piracy: A critical assessment of maritime security and trade disruptions in the Gulf of Guinea. *Maritime Economics and Logistics, 28*, 163-187. Retrieved from: https://doi.org/10.1057/s41278-025-00344-1

APPENDIX A. INCLUDED-STUDY CODING MATRIX

TABLE A1. Study characteristics and principal analytical focus

Study	Year	Method	Geographic focus	Primary focus
Okoroji and Ukpere (2011)	2011	Qualitative	National	ISPS compliance and port security implementation
Perouse de Montclos (2012)	2012	Qualitative	South-South	Political economy of maritime piracy
Onuoha (2013)	2013	Qualitative	Regional/Gulf of Guinea	Piracy trends, oil theft and regional security
Ukeje (2015)	2015	Qualitative	Regional/Gulf of Guinea	Regional maritime-security strategy
Akinyemi (2016)	2016	Quantitative	National	Port reform and efficiency
Anele (2016)	2016	Qualitative	South-South	Seafarer roles in piracy prevention
Nwanosike et al. (2016)	2016	Quantitative	National	Port productivity after reform
Oyewole (2016)	2016	Qualitative	Regional/Gulf of Guinea	Regional anti-piracy arrangements
Onwuegbuchunam (2018)	2018	Quantitative	National	Port governance and terminal performance
Peters (2020)	2020	Qualitative	South-South	Piracy business models and crime scripts
Nwalozie (2020)	2020	Qualitative	Regional/Gulf of Guinea	Contemporary piracy in Nigeria and the Gulf of Guinea
Denton and Harris (2021)	2021	Quantitative	Regional/Gulf of Guinea	Illegal fishing and piracy relationship
Okafor-Yarwood and Pigeon (2021)	2021	Mixed methods	Regional/Gulf of Guinea	Piracy effects on trade and port stability
Denton and Harris (2022)	2022	Quantitative	Regional/Gulf of Guinea	Military capacity, institutions and piracy

Triantafillou et al. (2023)	2023	Quantitative	Regional/Gulf of Guinea	Institutional and legal determinants of piracy
Moura et al. (2023)	2023	Review/data	Regional/Gulf of Guinea	Gulf of Guinea piracy incident dataset
Nsikan et al. (2023)	2023	Quantitative	South-West	Seaport supply-chain risk practices
Liang et al. (2024)	2024	Quantitative	Global with Gulf of Guinea	Spatial-temporal piracy analysis
Jacobsen and Rasmussen (2024)	2024	Qualitative	South-South	Onshore gun economy and piracy networks
Schandorf (2024)	2024	Qualitative	Regional/Gulf of Guinea	Coordination and information-sharing infrastructure
Ehizuelen (2025)	2025	Qualitative	National	Piracy and continental trade prospects
Yercan et al. (2026)	2026	Qualitative	Regional/Gulf of Guinea	Economic effects of Gulf of Guinea piracy

APPENDIX B. CODING DEFINITIONS

TABLE B1. Operational and mitigation coding rules

Variable	Meaning	Examples of evidence
Cost escalation	Additional financial burden attributable to security risk or response.	Insurance, guards, escorts, compliance, freight or operating cost.
Delay or lead-time variability	Security-related change in time or schedule.	Diversion, anchorage delay, clearance delay, interrupted operation.
Safety and human harm	Threat to crew, workers or other maritime users.	Kidnapping, injury, fatality, trauma or violent boarding.
Trade or throughput effect	Effect on cargo flow, vessel calls, port use or investment.	Reduced trade confidence, lower port calls, throughput or market access.
Service reliability effect	Reduced predictability or continuity of maritime service.	Schedule uncertainty, cancellation, disruption or recovery problem.
Governance coordination	Institutional cooperation and defined responsibilities.	Joint operations, information sharing, regional coordination.
Legal enforcement	Rules, prosecution and regulatory compliance.	Anti-piracy law, ISPS enforcement, prosecution or sanctions.
Technology and visibility	Systems used to detect, track or communicate risk.	AIS, CCTV, surveillance, tracking or incident platforms.
Operational risk management	Firm or port routines for preparation and response.	Risk assessment, disruption records, contingency plans.
Community engagement	Use of local trust, participation or intelligence.	Early warning, grievance channels, local reporting.
Infrastructure resilience	Physical capacity intended to reduce vulnerability or recovery time.	Secure facilities, access systems, protected operational assets.