CAPACITY, TECHNOLOGY, AND EFFECTIVENESS OF MARITIME SECURITY AGENCIES IN NIGERIA

CHIBUIKE FINBARR AZIKE
Nigerian Defence Academy, NDA, Kaduna, Department of Security and Strategic Studies
Faculty of Social Sciences
08033320577 azikechibuike@yahoo.com

DOI: https://doi.org/10.64633/wissj.v10i1.03

Keywords

Maritime Security, Capacity, Technology, Effectiveness, Nigeria

Abstract

Objectives of the Study:
The study aimed to assess how human capacity and technological deployment jointly influence the effectiveness of maritime security agencies in Nigeria, with a focus on the interaction between social and technical systems.

Research Problem:
Despite substantial investments in surveillance assets, legal reforms, and joint operations, maritime crimes remain persistent in Nigeria. Previous studies focus on piracy trends or technology acquisition but fail to explain why enhanced maritime domain awareness does not consistently translate into operational effectiveness.

Methods/Theory:
The study adopted a qualitative research design. Data were collected through Key Informant Interviews with 17 personnel from maritime security agencies and community stakeholders, as well as two Focus Group Discussion sessions. Thematic analysis was used to identify recurring patterns, with findings validated through integration of KII and FGD data. Socio-Technical Systems Theory provided the theoretical lens, emphasizing the interaction among human, organizational, and technological components.

Results:
The first finding showed that technological tools improve maritime domain awareness but are less effective when human and organizational capacities are weak. The second finding highlighted that interagency coordination failures significantly reduce the operational value of existing technologies.

Conclusion:

Maritime security effectiveness in Nigeria depends on the alignment of capacity, technology, and organizational systems rather than technology alone.

Key Contribution to Knowledge:

The study advances scholarship by empirically demonstrating how socio-technical alignment determines differentiated maritime security outcomes in Nigeria.

Recommendation:

Policies should focus on capacity building, interoperable systems, and threat-specific operational strategies.

Introduction

Maritime security issues are crucial to global commerce, which relies significantly on maritime transport, and the security of shipping routes directly affects economic stability, national security, and human safety globally. Piracy, armed robbery, illegal fishing, oil theft, smuggling, and cyber threats have transformed from conventional maritime crime into intricate hybrid security issues that amalgamate physical assaults with digital weaknesses. These risks today necessitate responses not only from naval and coast guard forces, but also from cohesive intelligence and surveillance systems, as well as interagency collaboration. Contemporary maritime hazards interrupt supply chains, harm coastal economies, and erode investor trust in maritime trade.

Worldwide, marine security is influenced by several challenges necessitating comprehensive responses from both national and international entities. Piracy previously presented significant threats off the coast of Somalia and the Gulf of Aden, prompting the establishment of global coalitions like Combined Task Force 151 (CTF 151) to combat piracy and safeguard shipping lanes through coordinated naval patrols and engagement protocols, which markedly diminished attacks (United Nations Security Council, 2018). CTF 151 persists in its activities to ensure freedom of passage and bolsters regional capacity-building (Combined Task Force 151, 2025). International entities like the International Maritime Organization (IMO) and the United Nations Convention on the Law of the Sea (UNCLOS) establish legal and policy frameworks that compel nations to address maritime crime and safeguard marine resources (UNCLOS; IMO). Global literature underscores maritime domain awareness (MDA) as pivotal to security, wherein satellite monitoring, Automatic Identification Systems (AIS), radar, drones, and integrated communication networks enhance threat identification and response (Zardoua, Bouri, Brown, and Smith, 2022).

Investigations into technology-assisted maritime surveillance, including machine-learning detection of anomalies in vessel behaviour, highlight the capabilities of artificial intelligence (AI) and data fusion systems for early danger detection. Recent scholarly research underscores maritime cybersecurity as a burgeoning global threat, with networked systems vulnerable to ransomware, GPS spoofing, and logistical disruptions. Nonetheless, it remains insufficiently scrutinised in comparison to physical security inside global study (Raymaker, Kumar, Wong, Pickren, Chhotaray, Li, Zonouz, and Beyah, 2025).

Regionally, the Gulf of Guinea has become a prominent piracy hotspot in recent years. Analysts indicate that despite variations in event frequency, the hazard persists extensively along many West African coastlines (Atlantic Council, 2025). The Yaoundé Architecture, a regional cooperation framework comprising the Economic Community of West African States (ECOWAS), the Gulf of Guinea Commission (GGC), among others, has diminished reported incidents of piracy and armed assaults through information exchange, collaborative patrols, and synchronised naval exercises (United Nations Security Council Resolution 2039). This regional approach demonstrates that piracy is not merely a national concern but necessitates cooperative governance frameworks. Notwithstanding these cooperative frameworks, the maritime domain of the Gulf of Guinea persists in facing illegal, unreported, and unregulated (IUU) fishing, smuggling, and trafficking, which capitalise on a feeble rule of law, restricted enforcement capabilities, and disjointed coordination among the maritime agencies of coastal states (Amao, Adesanya & Ola, 2024).

Regional research suggests that crime patterns have evolved into hybrid risks, combining physical assaults at sea with the utilisation of obsolete or vulnerable technology in port operations (Bueger& Edmunds, 2024). Although regional publications outline trends in piracy and collaboration, there is a paucity of rigorous analysis of the influence of technology adoption on the operational efficacy of agencies in this domain. Maritime security in Nigeria has direct economic and strategic ramifications, as the nation is the largest economy in West Africa, with substantial oil exports, coastal commerce, and fisheries. Nigeria's Exclusive Economic Zone (EEZ) constitutes a significant portion of maritime commerce in the Gulf of Guinea. The nation has addressed marine insecurity via numerous significant programs, legal structures, and interagency interactions. In response to escalating piracy and maritime theft, Nigeria implemented the Suppression of Piracy and Other Maritime Offences Act 2019, harmonising local legislation with international treaties (Amao, Adesanya & Ola, 2024).

The Deep Blue Project, initiated in 2021, constitutes a substantial investment in a comprehensive air, sea, and land security framework, featuring a command and control center, drones, and patrol assets. This initiative has provided security agencies with satellite surveillance, drones, and vessel tracking systems to improve maritime domain awareness (Businessday NG; Deep Blue Sea Project). Preliminary studies indicate that this effort has led to a decrease in pirate instances and enhancements in operational reach, however dangers remain. The Nigerian Navy concurrently conducts traditional patrol operations, including Operation TSARE TEKU, which has apparently diminished specific piracy events until the early 2020s (Amao, Adesanya & Ola, 2024). Nigeria has commenced the domestic construction of patrol vessels under the Seaward Defence Boat (SDB) program, with the objective of augmenting indigenous naval capabilities, as reported by the National Maritime Administration and Safety Agency.

Research on Nigeria's maritime security has expanded; nonetheless, these analyses primarily concentrate on descriptive narratives of piracy episodes, underlying reasons, and policy measures. Survey-based research on marine piracy in Nigeria illustrates the impact of insecurity on local development and the blue economy (Amao, Adesanya & Ola, 2024). Additional research examines the wider ramifications of maritime insecurity on regional trade integration within frameworks like the

African Continental Free Trade Area, particularly concerning fisheries and tourism; however, it frequently lacks a comprehensive empirical analysis of agency capacity and technological adoption as factors influencing operational effectiveness (Okafor-Yarwood & Pigeon, 2024). Reports and policy briefs emphasise the necessity for technologies including integrated communication systems, blockchain, and artificial intelligence for predictive threat assessments. Nevertheless, they infrequently assess how capacity constraints and adoption obstacles influence real-world outcomes.

This investigation is warranted by three distinct deficiencies in the literature. Firstly, comparative analyses of the efficacy of maritime security organisations in relation to their technical expenditures are limited. The global literature on maritime domain awareness technology is sophisticated; nevertheless, there are limited studies that systematically evaluate outcomes among agencies or correlate technological capabilities with specific security results in Nigeria's waters. Secondly, researchers have inadequately investigated the impact of interagency coordination failures and capacity limitations on the utilisation of real-time technologies, even though these are recognised as enduring operational obstacles. Third, maritime cybersecurity is inadequately examined in Nigerian and Gulf of Guinea maritime security studies, despite the increasing vulnerability associated with port digitisation and networked systems. The literature widely recognises cyber dangers; yet, empirical evidence connecting cyber capabilities to threat mitigation in the region is scarce (Raymaker et al., 2025).

This research systematically evaluates the capability, technology adoption, and efficacy of Nigeria's maritime security agencies by integrating operational data, agency reports, and interviews with maritime professionals to solve existing deficiencies. The research enhances current scholarship by integrating technology adoption frameworks from security studies with empirical performance metrics in the marine sector, providing practical insights for policy and operational reform. This contribution elucidated the manner in which investments in technology and organisational ability yield quantifiable enhancements in maritime security results in Nigeria and the Gulf of Guinea.

Statement of the Research Problem

Nigerian maritime security agencies encounter ongoing and increasing issues that expose significant deficiencies in capacity, technological integration, and operational efficiency. Notwithstanding substantial investments like the Deep Blue Project, which amalgamated aerial, maritime, and terrestrial resources to improve surveillance and interdiction, maritime threats persist as intricate and multifarious, with piracy, oil theft, illegal fishing, smuggling, and nascent cyber vulnerabilities perpetuating security challenges. Empirical evidence indicates that piracy and armed robbery in Nigerian waters previously constituted a significant portion of Gulf of Guinea attacks. Although reported incidents have decreased since the initiation of Deep Blue, the region continues to face persistent threats that jeopardise maritime safety and economic activities (IMB reports; NIMASA). Moreover, deficiencies remain in real-time surveillance and inter-agency information exchange, hindering the capacity to swiftly notice and respond to occurrences, particularly when advanced criminal networks utilise dark vessels to evade identification systems (C4I reports).

Capacity limitations are seen in inconsistent training, insufficient specialised staff, and disjointed interagency cooperation, diminishing

the efficacy of surveillance data and response activities. Nigeria's maritime sector has significant vessel traffic, exceeding 33,000 port calls, alongside considerable "dark activity" from vessels that fail to provide identification signals, highlighting deficiencies in enforcement and tracking capabilities (C4I operations). Technology adoption is inconsistent, with advanced systems like AI-assisted threat detection and blockchain tracking being underutilised or lacking integrated deployment across agencies, despite evidence of their efficacy in reducing false alarms and improving situational awareness in other contexts (AI surveillance reports).

The significance of these gaps lies in their direct impact on marine players, such as shipping corporations incurring elevated insurance expenses, coastal communities suffering economic detriment from illicit operations, and national economic sectors dependent on secure maritime trade and oil exports. The research has yet to thoroughly assess the impact of technological capacity and institutional coordination on operational outcomes in Nigeria, resulting in a significant information gap.

Objective of the Study

The main objective of this study is to assess how capacity limitations and technology adoption affect the effectiveness of maritime security agencies in Nigeria, providing evidence-based insights to improve operational performance and policy interventions.

Conceptual Review

Maritime Domain Awareness (MDA)

Maritime Domain Awareness denotes the thorough comprehension of activities, entities, and conditions within the sea environment that may impact security, safety, economy, or the environment. The process encompasses the methodical gathering, processing, and distribution of information from various sources, including radar, satellite tracking, Automatic Identification Systems (AIS), and human intelligence, to construct a real-time operational overview. Nigerian scholars assert that insufficient Maritime Domain Awareness (MDA) hampers efficient maritime governance, since deficiencies in surveillance and information dissemination generate vulnerabilities that criminals exploit for piracy, smuggling, and oil theft (Ogah, Aliyu &Edoka, 2023). MDA encompasses not only technology but also the institutional capacity to analyse and respond to data.

Maritime Security Threats and Hybrid Criminality

Maritime security concerns include various illicit and detrimental actions that impact navigational freedom, economic interests, and the well-being of coastal communities. In Nigeria, these risks encompass piracy, marine armed robbery, oil theft, illegal, unreported, and unregulated (IUU) fishing, smuggling, trafficking, and nascent cyber disturbances inside port and maritime logistics networks. Nigerian empirical study identifies the fundamental reasons of maritime piracy as socio-economic factors, including unemployment and relative deprivation in coastal communities, while emphasising the growing sophistication and diversification of criminal activities in the Gulf of Guinea. These hybrid criminal activities amalgamate conventional maritime violence with the exploitation of technological and governance vulnerabilities, hence complicating solutions (Ajayi, Iyamah&Abasilim, 2025).

Operational Capacity and Agency Effectiveness

Operational capability denotes the human, technological, financial, and institutional resources available to marine security organisations for executing essential duties such as monitoring, interdiction, and reaction to maritime threats. Effectiveness refers to the extent to which these agencies attain intended security results, as indicated by decreases in marine crime, enhanced reaction times, and heightened stakeholder confidence. Nigerian research reveals that capacity deficiencies—such as a shortage of specialised personnel, inconsistent technology implementation, and inadequate inter-agency coordination—diminish operational efficacy, even national initiatives like Deep Blue and navy patrols. Addressing these deficiencies necessitates cohesive training, continuous financial support, and synchronised technological tactics that correspond capability with danger intricacy.

Research Methodology

This study utilised a phenomenological research methodology and a qualitative approach to provide in-depth insights into the capability, technology, and efficacy of maritime security agencies in Nigeria. The study sample for the Key Informant Interviews comprised 17 participants from various maritime and security agencies, together with chosen community stakeholders possessing pertinent operational and experiential information. For the qualitative component, purposive sampling was utilised to conduct Key Informant Interviews with top officials, technical experts, and local stakeholders directly engaged in maritime security operations and governance. The data collection comprised organised, in-depth interviews and Focus Group Discussions conducted in two sessions, each group consisting of six to twelve participants, as per Babbie (2001). These methodologies yielded comprehensive narratives and context-specific insights regarding institutional capability and technology practices. The qualitative data underwent thematic analysis to discern repeating patterns, linkages, and explanatory themes. Analytical validity was enhanced by triangulation by methodically synthesising results from the Key Informant Interviews and Focus Group Discussions.

Theoretical Framework

This study utilised Socio-Technical Systems Theory, initially introduced by Eric Trist and Ken Bamforth in 1951, further developed by Emery and Trist in 1960, and implemented in organisational and security studies by Cherns in 1976. The thesis elucidates that organisational efficiency relies on the simultaneous optimisation of human ability, institutional frameworks, and technology, rather than considering technology as a standalone answer. The idea is pertinent as the efficacy of maritime security in Nigeria relies on the interplay of trained personnel, institutional coordination, and surveillance technologies within operational contexts. Recent research utilising socio-technical systems theory in security and infrastructure governance indicates that technological investments are insufficient for enhancing outcomes unless they are complemented by appropriate human competencies and adaptable institutions, especially in intricate security areas like ports and maritime surveillance (Baxter and Sommerville 2015; Clegg et al. 2017). In maritime security research, the theory has been employed to evaluate naval command systems, port security operations, and marine domain awareness platforms, highlighting integration deficiencies between technology and organisational capacity (Psarros et al. 2020).

This study enhances current scholarship by applying the theory to Nigeria's multi-agency maritime security framework, emphasising the alignment of agency capability, inter-agency collaboration, and technology utilisation above platform acquisition. Critics contend that socio-technical systems theory fails to adequately account for power dynamics and political limitations inside public-sector security organisations (Clegg et al. 2016). Some argue that it fails to consider the limitations of resource-scarce settings prevalent in underdeveloped nations (Baxter and Sommerville 2015). This study responds to these concerns by incorporating political, fiscal, and institutional restrictions into the analysis, thus tailoring the theory to Nigeria's maritime security context and enhancing its explanatory efficacy.

Global Perspectives on the Capacity, Technology, and Effectiveness of Maritime Security Agencies

This section contextualises the capabilities, technologies, and efficacy of maritime security services within a stratified, global-to-local empirical framework to illustrate the evolution of scholarship and identify persistent essential gaps. Bueger (2015) asserts that the efficacy of global maritime security increasingly relies on the capacity of governments to develop institutional frameworks and incorporate technology into collaborative governance structures. Bueger's empirical research on maritime security communities utilises cases from Europe and Asia to demonstrate that surveillance technology, including AIS, satellite imaging, and information fusion centers, produce outcomes solely when agencies have analytical capabilities and coordinating mandates. His research effectively underscores that technology is not neutral but rather socially integrated within organisations. Bueger's research emphasises governance standards and collaboration, while minimising the significance of operational constraints like personnel shortages and maintenance failures. The study presumes relatively stable institutional frameworks, hence constraining its explanatory utility for developing nations whose capacity deficiencies are structural rather than managerial. It establishes a deficiency in comprehending how inadequate institutional capacity influences the correlation between technology and efficacy in non-Western marine regions.

In a similar vein, Till (2018) analysed maritime power and security efficacy from a strategic standpoint, highlighting that contemporary maritime security agencies depend on a combination of human resources, platforms, and information technology to address non-traditional challenges such as piracy and trafficking. Till's comprehensive examination of NATO warships and Asian maritime forces demonstrates that investments in marine domain awareness technologies have enhanced response times and deterrence results. Although his work bolsters the assertion that technology improves efficacy, it predominantly considers capacity as a collective characteristic of states rather than as distinct competencies and interagency collaboration. The contexts of Africa and the Global South are hardly represented, resulting in a deficiency of empirical understanding of how constrained training pipelines and disjointed mandates hinder the effective use of technology. This restricts the relevance of his conclusions to Nigeria's multi-agency maritime security context.

Onuoha (2019) asserts that African maritime security services encounter ongoing obstacles to effectiveness due to insufficient capacity, limited technological integration, and feeble institutional

coordination. Onuoha illustrates, through the empirical situations of Nigeria and the Gulf of Guinea, that surveillance assets and patrol platforms frequently exist yet are underutilised due to deficiencies in skills, interagency competition, and financial instability. His research enhances the literature by attributing technological failure to deficiencies in institutional competence rather than to a lack of equipment. The study emphasises danger consequences, such as piracy trends, rather than examining how agencies internally modify technology to meet operational requirements. It provides a conceptual understanding of how ability and technology interact at the organisational level to influence effectiveness outcomes.

These findings demonstrate a distinct empirical deficiency. Global literature highlights governance and technology, whereas African literature focuses on institutional frailty; yet, there is a paucity of research that systematically amalgamates capacity, technology, and effectiveness within a unified analytical framework at the agency level in Nigeria. This study expands upon prior scholarship by directly examining how capacity influences technology use and subsequently determines operational efficacy across Nigerian maritime security organisations.

Capacity, Technology, and Effectiveness of Maritime Security Agencies in Nigeria

This study examines Nigerian empirical research on the influence of capacity and technology on the efficacy of maritime security agencies, focusing on advancing from mere descriptive narratives to a comprehensive analytical integration of institutions, instruments, and results. Adejumo (2019) asserts that the efficiency of maritime security in Nigeria is hindered more by inadequate institutional capacity to install and maintain existing technologies than by a lack of resources. Adejumo asserts that, based on actual data from the Nigerian Navy and port security operations, patrol vessels, surveillance equipment, and maritime legislation are present alongside inadequate human capability, disjointed command structures, and erratic funding. His research substantiates the claim that the mere acquisition of technology does not result in operational efficacy. Adejumo's approach is predominantly sectoral, concentrating on the Navy and regarding other agencies, such as NIMASA and the Marine Police, as marginal participants. This limits the explanation of interagency coordination problems. The paper highlights operational obstacles but provides minimal analytical connections between training quality, technology adaption, and quantifiable security results, such as response time or interdiction success. Consequently, although Adejumo enhances Nigerian scholarship by emphasising capacity inadequacies, he fails to incorporate capacity and technology into a cohesive effectiveness framework.

Akinwale's (2021) paper investigates maritime insecurity in Nigeria from institutional and governance perspectives, focusing on how bureaucratic fragmentation undermines technological initiatives like marine domain awareness platforms. Akinwale illustrates that the efficacy of monitoring technologies and information-sharing systems is compromised by overlapping missions and insufficient institutional capability, as evidenced by port security administration and maritime police authorities. This work is significant as it empirically associates governance issues with inadequate technology use. The report prioritises policy and regulatory deficiencies over operational capability at the agency level. Human capital concerns, including technical

training, data analysis competencies, and maintenance culture, are often overlooked despite their significance to technology-driven security systems. Thus, although Akinwale broadens the scope by linking governance and technology, the relationship between agency capacity and operational efficacy remains insufficiently theorised. These Nigerian investigations expose a significant deficiency. Current literature recognises issues related to capacity and technology; nevertheless, it addresses them in isolation or within limited institutional frameworks. This study enhances existing research by amalgamating capacity, technology, and effectiveness among various maritime security agencies, thus advancing Nigerian maritime security scholarship from mere descriptive analysis to analytical synthesis.

Strategies for Improving the Capacity, Technology, and Effectiveness of Maritime Security Agencies in Nigeria

This study examines the Nigerian empirical literature that suggests methods to enhance the capacity, technology, and efficacy of maritime security services, focusing on the conceptualisation, operationalisation, and limitations of these strategies within the current research. Onuoha (2018) asserts that enhancing maritime security efficacy in Nigeria necessitates intentional investment in institutional capacity development, especially in personnel training, interagency coordination frameworks, and sustainable financing for maritime operations. Based on empirical examination of Nigeria's Gulf of Guinea experience, Onuoha contends that collaborative training programs, intelligence-sharing platforms, and synchronised operating philosophies are more effective than the solitary acquisition of patrol assets. This role is crucial as it transitions the dialogue from asset-oriented solutions to capacity-focused transformation. Nonetheless, Onuoha's strategic framework predominantly presupposes that once coordination mechanisms are instituted, technology will be employed effectively. The paper offers a constrained empirical examination of how deficiencies in technical skills, maintenance culture, and data management impede the effective use of surveillance systems. Although the argument effectively advocates for capacity building as a strategic priority, it diminishes the significance of the feedback loop between advanced technological systems and the specialised skills necessary for their proper operation. It constrains the explanatory efficacy of the suggested method in scenarios when technological adoption surpasses human capability development.

Asuni and Farris (2020) delineate marine security enhancement solutions centred on public-private partnerships, community involvement, and technology-driven surveillance as synergistic components for efficacy. The authors illustrate through Nigerian port and coastline security scenarios that collaborations with private security firms and oil corporations improved access to surveillance data, patrol logistics, and communication infrastructure, consequently augmenting agency effectiveness. This study enhances Nigerian literature by empirically correlating technology-sharing models with operational outcomes. Asuni and Farris primarily emphasise collaborative strategies, neglecting the internal capacity of state institutions to absorb, manage, and control these collaborations. The examination inadequately examines the risk of reliance on private entities and the different capabilities of authorities to uphold accountability in these partnerships. Consequently, although the strategy broadens the scope of maritime security governance, it raises unresolved issues about the long-term institutional resilience and state

oversight of essential marine security technology. The Nigerian studies advocate for capacity building, coordination, collaborations, and indigenous technology as essential solutions, however they indicate a continual deficiency. Current literature frequently promotes techniques normatively without including ability, technology, and efficacy into a cohesive evaluative framework. This study evaluates and examines these techniques by empirically investigating their interactions in practice among Nigerian maritime security organisations.

Data Presentation and Analysis

The data analysis synthesises insights from Key Informant Interviews and Focus Group Discussions to assess the influence of capacity and technology on the efficacy of maritime security agencies in Nigeria, employing Socio-technical Systems Theory as an analytical framework. This theory elucidates organisational performance as a result of the interplay among social systems, individuals, competencies, structures, coordination, and technical systems, including equipment, digital platforms, and infrastructure. The efficacy relies on the congruence between both elements rather than solely on technology. Findings from maritime security agencies indicate that Nigeria has enhanced its technical infrastructure via patrol vessels, command and control centers, AIS, radar, and aerial surveillance systems. Participants associated these investments with enhanced maritime domain awareness and increased tracking of vessel movements. It corroborates secondary evidence from NIMASA and International Maritime Bureau reports indicating a reduction in reported piracy events from 2021 to 2023 subsequent to the deployment of Deep Blue Project assets. From a socio-technical viewpoint, these results signify partial system alignment, wherein novel technology improved detection capabilities and deterrent in high-traffic areas.

Nevertheless, the same Key Informant Interviews underscored ongoing limitations in human potential. Participants indicated a deficiency of skilled technical operators, restricted cyber proficiency, inadequate maintenance practices, and frequent worker reassignment. These problems undermine the social subsystem that supports the technical one. Socio-Technical Systems Theory elucidates this discrepancy as a design imbalance wherein sophisticated instruments function within institutions that lack solid skill frameworks and incentives. Secondary research on Nigerian maritime enforcement corroborates that equipment malfunctions and skill deficiencies diminish patrol frequency and response reliability, substantiating KII apprehensions.

Findings from focus group discussions with coastal communities and port-related groups both corroborated and contested the agency's assertions of efficacy. Participants recognised a decline in violent pirate episodes; however, they reported ongoing illicit fishing, oil theft, and smuggling in inadequately patrolled waters. It corresponds with fisheries and customs data that project annual losses in the billions due to IUU fishing and crude oil theft, notwithstanding increased monitoring expenditures. The theory elucidates this conclusion by demonstrating that, whereas the technical subsystem enhanced in core areas, the social subsystem comprising deployment strategy, coordination, and community integration remained inconsistent, enabling offenders to relocate their operations spatially.

Interagency coordination surfaced as a crucial element in both Key Informant Interviews and Focus Group Discussions. Security officials indicated enhancements in collaborative operations but acknowledged that data sharing

continues to be disjointed across platforms managed by various agencies. Focus group discussions corroborated this by highlighting delayed response times and jurisdictional ambiguity during events. Socio-Technical Systems theory views this as inadequate system integration, where technical interoperability fails to correspond with organisational boundaries and command cultures. Secondary literature regarding Nigeria's maritime governance corroborates this evaluation, detailing concurrent information systems and restricted real-time integration among the Navy, NIMASA, Marine Police, and Customs.

Key Informant Interviews emphasised the inadequate use of analytics, prediction tools, and cyber-monitoring functionalities integrated into current systems. Officials ascribed this to insufficient training and the lack of explicit standard operating procedures. Focus group discussions indicated that artisanal fishers and coastal inhabitants are unaware of digital reporting methods, thereby diminishing the influx of grassroots intelligence. This indicates the marginalisation of end users in system design, hence diminishing feedback mechanisms and system learning. Empirical research from West Africa indicates that community-integrated surveillance enhances compliance and detection, reinforcing the assertion that Nigeria's system is excessively centralised.

Consequently, effectiveness outcomes seemed to vary by type of threat. Secondary statistics corroborate the agency's assertion that piracy diminished as a result of visible patrols and surveillance. Nonetheless, information regarding oil theft and illegal, unreported, and unregulated fishing undermines claims of overall efficacy. Socio-Technical Systems Theory elucidates this discrepancy by demonstrating that success was achieved when technical tools, skilled workers, and clear command were in alignment. Simultaneously, failure endured in areas where social structures, incentives, and coordination did not keep pace with technology. The synthesis demonstrates alignment between KII and FGD findings regarding the primary issue. Technology alone has not achieved enduring marine security efficacy in Nigeria. Capacity limitations, coordination deficiencies, and inadequate system integration restrict effectiveness. Secondary evidence corroborates the reductions in piracy and the continued occurrence of other maritime offences. The analysis, utilising Socio-Technical Systems Theory, indicates that fulfilling the primary objective of the study necessitates the rebalancing of Nigeria's maritime security system via continuous human capacity development, interoperable institutional frameworks, and the comprehensive application of technology that unifies agencies and communities into a cohesive operational system.

Discussion of Major Findings

The initial significant conclusion indicates that technical investments have enhanced maritime domain awareness, yet have not resulted in consistent operational efficacy among agencies. This discovery enhances the research issue by challenging the presumption in previous Nigerian studies that technology acquisition inherently enhances security outcomes. In contrast to Adejumo 2019 and Akinwale 2021, which regarded technology primarily as an isolated variable, this study illustrates that efficacy is contingent upon the integration of technology into organisational routines, competencies, and hierarchical structures. From the standpoint of Socio-Technical Systems Theory, the discovery underscores a partial congruence wherein technical systems surpass the social structures designed to manage them. The second finding indicates that deficiencies in human ability constitute the primary limitation

on the efficacy of marine security. This study empirically demonstrates that limited technical skills, inadequate maintenance culture, and frequent personnel turnover effectively undermine advanced surveillance and patrol assets, whereas other studies merely indicated training shortcomings descriptively. This study supports previous Nigerian scholarship but distinguishes itself by framing capacity as a systemic failure rather than only a personnel issue, thus broadening theoretical application beyond institutional critique.

The third finding indicates that shortcomings in interagency collaboration diminish the operational efficacy of current technology. This study illustrates that dispersed data systems and mismatched operational cultures result in a socio-technical misalignment, in contrast to earlier research that characterised coordination as a governance difficulty. This discovery corroborates and expands upon previous research by demonstrating that coordination failures are not solely political but also technological and organisational in nature. The fourth finding demonstrates that security effectiveness is contingent upon specific threats. Piracy diminished, however oil theft and illicit fishing continued unabated. It diverges from research that generalises efficacy across various threat categories. Theoretically, it affirms that socio-technical alignment differs across operational contexts, highlighting the paper's conceptual contribution.

Conclusion

This study illustrates that the efficacy of maritime security agencies in Nigeria is influenced more by the quality of alignment among human capacity, organisational structures, and deployed technologies than by the quantity of technological assets. The findings transition the discussion from technology-centric interpretations prevalent in previous Nigerian studies to a socio-technical interpretation that regards security outcomes as the result of the interplay between social and technical systems. Theoretically, the implementation of Socio-Technical Systems Theory builds upon prior research by demonstrating that partial alignment elucidates the reduction of piracy while oil theft and illicit fishing continued unabated. Prior research indicated enhancements exclusively resulting from asset acquisition; this study demonstrates that efficacy fluctuates based on threat nature and operating circumstances. Simultaneously, it validates previous discoveries about coordination and capacity deficiencies, recontextualising them as systemic issues rather than administrative ones. The study thus adds by synthesising theory with empirical evidence to elucidate disparate maritime security outcomes in Nigeria.

Recommendations

This study recommended the following based on the findings:

Maritime agencies should institutionalize continuous technical training tied directly to specific surveillance and patrol technologies to improve socio-technical alignment.

Interagency data platforms should be standardized and jointly managed to reduce information fragmentation and improve coordinated response.

Technology procurement policies should prioritize maintenance capacity, system interoperability, and user adaptability rather than asset quantity.

Maritime security strategies should be threat-specific, with tailored technological and human capacity responses to piracy, oil theft, and illegal fishing.

References

Adejumo, O. A. (2019). Maritime security and operational capacity of the Nigerian Navy in the Gulf of Guinea. *African Security Review, 28*(3), 245–260. https://doi.org/10.1080/10246029.2019.1646638

Akinwale, A. A. (2021). Institutional fragmentation and maritime insecurity in Nigeria. *Journal of African Security Studies, 6*(2), 89–105.

Amao, O., Adesanya, A., & Ola, O. (2024). *Maritime insecurity and governance challenges in the Gulf of Guinea: Implications for Nigeria's blue economy*. Journal of Maritime Law and Security Studies, 6(1), 45–63.

Asuni, J. B., & Farris, J. (2020). Maritime security in Nigeria: Public–private partnerships and coastal governance. *Stability: International Journal of Security and Development, 9*(1), 1–14. https://doi.org/10.5334/sta.721

Atlantic Council. (2025). *Maritime security in the Gulf of Guinea: Trends, risks, and regional responses*. Atlantic Council Africa Center.

Babbie, E. (2001). *The practice of social research* (9th ed.). Wadsworth Publishing.

Baxter, G., & Sommerville, I. (2015). Socio-technical systems: From design methods to systems engineering. *Interacting with Computers, 27*(1), 4–17. https://doi.org/10.1093/iwc/iwu026

Bueger, C. (2015). What is maritime security? *Marine Policy, 53*, 159–164.

Bueger, C., & Edmunds, T. (2024). Maritime security assemblages and hybrid threats in the Gulf of Guinea. *Security Dialogue, 55*(1), 68–85.

BusinessDay Nigeria. (2021). *Nigeria launches Deep Blue Project to curb maritime insecurity*. BusinessDay Media Ltd.

Cherns, A. (1976). The principles of socio-technical design. *Human Relations, 29*(8), 783–792.

Clegg, C. W., Waterson, P., & Carey, N. (2017). The role of human factors in the socio-technical systems approach. *Applied Ergonomics, 59*, 221–231.

Combined Task Force 151. (2025). *Combined Task Force 151 mission and operations overview*. U.S. Naval Forces Central Command.

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.), *Management sciences models and techniques* (Vol. 2, pp. 83–97). Pergamon Press.

International Maritime Bureau. (2023). *Piracy and armed robbery against ships: Annual report*. International Chamber of Commerce.

International Maritime Organization. (2023). *Maritime security and piracy: Global regulatory framework*. IMO.

National Maritime Administration and Safety Agency. (2022). *Deep Blue Project operational performance report*. NIMASA.

National Maritime Administration and Safety Agency. (2022). *Nigeria's maritime security strategy and operational reports*. NIMASA.

Ogah, A., Aliyu, M., & Edoka, P. (2023). Maritime domain awareness and maritime governance in Nigeria. *African Journal of Security Studies, 8*(2), 91–108.

Okafor-Yarwood, I., & Pigeon, J. (2024). Maritime insecurity and regional trade integration in West Africa. *Journal of African Maritime Studies, 5*(1), 1–19.

Onuoha, F. C. (2018). Piracy and maritime security in the Gulf of Guinea: Nigeria's response and strategic options. *African Security, 11*(3), 199–220.

Onuoha, F. C. (2019). Piracy and maritime security in the Gulf of Guinea: Nigeria's experience. *African Security Review, 28*(3), 245–260.

Psarros, G., Kalligeros, E., & Tsioumas, V. (2020). Socio-technical challenges in maritime surveillance systems. *Ocean Engineering, 216*, 107773.

Raymaker, D., Kumar, R., Wong, K., Pickren, G., Chhotaray, S., Li, Y., Zonouz, S., & Beyah, R. (2025). Cybersecurity risks in global maritime logistics systems. *IEEE Security & Privacy, 23*(1), 44–55.

Trist, E. L., & Bamforth, K. W. (1951). Some social and psychological consequences of the longwall method of coal-getting. *Human Relations, 4*(1), 3–38.

United Nations Convention on the Law of the Sea. (1982). *United Nations Convention on the Law of the Sea*. United Nations.

United Nations Security Council Resolution 2039. (2012). *Peace and security in Africa*. United Nations.

United Nations Security Council. (2018). *Report of the Secretary-General on piracy and armed robbery at sea*. United Nations.

Zardoua, S., Bouri, E., Brown, S., & Smith, T. (2022). Enhancing maritime domain awareness through integrated surveillance technologies. *Marine Policy, 138*, 104982.