Maritime Technology and Society
Vol. 5(1): 107-116, February 2026
https://doi.org/10.62012/mp.vi.48187

Case Research Article

Intelligence and Global Transportation Supply Chain Management: The Case of Oil and Gas Supply in the Gulf of Guinea

Ngboawaji Daniel Nte

Department of Intelligence of Intelligence and Security Studies & Provost, College of Management and Social Sciences, Novena University, Nigeria.

profdnte@novenauniversity.edu.ng

Abstract: The Gulf of Guinea (GoG) is a critical artery for global oil and gas distribution, yet its supply chain is plagued by a complex risk ecosystem. This study investigates the imperative of intelligence management in mitigating these risks. Employing a mixed-methods approach, it integrates quantitative data from the International Maritime Bureau (IMB) and MDAT-GoG (2020-2024) with qualitative insights from focused group interviews with 12 security and industry experts. The findings reveal an evolution in maritime criminality towards armed robbery and theft, persistent infrastructure deficits that act as risk multipliers, and a critical "intelligence deficit" hindering proactive risk management. The study concludes that security threats, infrastructural decay, and geopolitical instability are interconnected. It recommends regional intelligence collaboration via the Yaoundé Architecture, route optimization using digital tools, massive infrastructural investment, and a sustainable regional security framework to secure the oil and gas supply chain.

Keywords: Intelligence, Global Transportation, Gulf of Guinea, Oil and Gas, Supply Chain Risk Management

1. Introduction

The global energy landscape is inextricably linked to the uninterrupted flow of hydrocarbons from production centers to consumption hubs. The Gulf of Guinea (GoG), spanning from Senegal to Angola, has established itself as a key artery in this system, contributing approximately 5.4 million barrels of oil per day and a growing share of liquefied natural gas (LNG) [1]. The strategic value of these sea lanes is underscored by the high quality of its light, sweet crude oil, which is prized by refineries for producing high-value products like gasoline and diesel [2].

The internationalization of this transportation supply chain elevates its stability and efficiency to a matter of global economic significance. Disruptions in the GoG can trigger violent price fluctuations, threaten energy security for importing nations, and cause substantial revenue losses for producers and multinational firms [3]. However, the region's geopolitical and operational environment is paradoxical, generating vast wealth while simultaneously being exposed to deep-seated risks. The oil and gas supply chain faces a triple nexus of challenges: dire security threats, debilitating infrastructural constraints, and multifaceted geopolitical instability [4]. Piracy, armed robbery, and critical infrastructure sabotage remain persistent menaces, while aging ports and pipelines create inefficiencies and vulnerabilities [5].

The overarching aim of this study is to examine how intelligence management can serve as a critical instrument for mitigating these multi-faceted risks. The paper moves beyond merely cataloging threats to propose a framework for integrating processed, actionable

Received: 2025-11-25; Accepted: 2026-01-10

intelligence into mainstream supply chain processes. The research is guided by the following questions: First, what are the predominant security and operational risks affecting the oil and gas supply chain in the GoG? Second, how can intelligence be practically integrated into supply chain strategy to enable proactive risk mitigation? Third, what collaborative and investment structures are necessary to establish a secure operating environment?

This work holds significance for academia, industry, and policymaking. It contributes to Supply Chain Risk Management (SCRM) literature by applying its tenets to a high-risk context and bridges the disciplines of security studies, intelligence analysis, and logistics management. For industry practitioners, it offers a validated risk assessment and mitigation framework. For regional policymakers in bodies like ECOWAS and the Gulf of Guinea Commission, it provides evidence-based recommendations for enhancing cooperation, maritime security architecture, and infrastructural investment.

The paper is structured to provide a logical flow of analysis. Following this introduction, Section 2 presents a comprehensive literature review. Section 3 details the mixed-methods methodology. Section 4 presents and discusses the findings. Section 5 concludes by summarizing key insights and contributions, and Section 6 provides targeted recommendations for stakeholders.

2. Literature Review

2.1. Theoretical Foundations of Supply Chain Risk Management (SCRM)

Supply Chain Risk Management (SCRM) focuses on identifying, assessing, mitigating, and monitoring potential disruptions across a network. Traditional frameworks categorize risks into operational risks, such as supplier failures, and disruptive risks, such as political instability or natural disasters [6]. In the high-risk context of the GoG, disruptive external risks are paramount. Foundational SCRM concepts of vulnerability the susceptibility to disruptions and resilience, the capacity to anticipate, withstand, and recover from disruptions are essential for analysis [7].

Modern SCRM theory conceptualizes resilience as a dynamic capability that involves adapting and reconfiguring resources in response to a crisis [8]. This perspective is crucial for the GoG, where disruptions are a constant feature of the environment. Capabilities such as flexibility, velocity, and visibility are key pillars of a resilient supply chain [9]. In this context, intelligence serves as the primary enabler of visibility, providing the information necessary to enhance flexibility (e.g., finding alternative routes) and velocity (e.g., rapid decision-making during a crisis) [10].

The oil and gas supply chain in the GoG can be viewed as a complex adaptive system, a network of interconnected actor's companies, governments, criminals constantly interacting and adapting within a turbulent environment [11]. From this viewpoint, disruptions are emergent properties of the system's behavior [12]. Intelligence acts as a critical adaptation mechanism, allowing actors to adjust their behavior in response to a changing threat landscape. The integration of advanced data analytics and AI, often termed "Supply Chain 4.0, marks a shift from reactive to predictive risk management [13]. By analyzing historical data on attacks and instability, predictive models can forecast risk hotspots, enabling preemptive action.

The ethical dimension of risk management, framed by Corporate Social Responsibility (CSR), is also critical. Multinational corporations have a responsibility to protect local communities and the environment, not just their assets [14]. Ethical, community-focused risk management is a foundation for sustainable resilience, as it mitigates local grievances that can fuel instability. This ethical framework necessitates that intelligence gathering and security operations respect human rights and international law [15].

2.2. The Special Nature of Oil and Gas Supply Chains

Hydrocarbon supply chains possess unique characteristics that heighten their susceptibility to GoG risks. They are capital-intensive, with high-value fixed (platforms, pipelines) and mobile (tankers) assets, where any attack can lead to massive financial, environmental, and human costs [2]. The infrastructure is often

Received: 2025-11-09; Accepted: 2026-02-03

geographically dispersed and exposed, making physical protection challenging [16].

Furthermore, the oil and gas supply chain exhibits significant inflexibility. Crude oil from a specific field is often destined for a refinery configured to process its grade, making swift sourcing alternatives difficult [17]. This inflexibility amplifies the impact of disruptions. The strategic importance of oil and gas also renders its supply chain highly politically sensitive, attracting attention from criminal gangs to militant groups [18]. This combination of high value, strategic importance, and political sensitivity creates an intense risk profile, demanding strategies that integrate advanced security and intelligence functions directly into operational planning [19]. The financial impact of a single disruption can ripple through global energy markets, affecting prices and economies far beyond the region [20].

2.3. Intelligence in SCM

The application of intelligence in SCM extends beyond security to reduce uncertainty and enable proactive decision-making. It can be categorized into distinct types [21]: Security Intelligence, focusing on threats like piracy, theft, and sabotage; Geopolitical Intelligence, analyzing political stability, regulatory changes, and inter-state tensions; and Market Intelligence, tracking commodity prices, demand shifts, and competitor activities.

A critical distinction exists between tactical, operational, and strategic intelligence, though the latter two are often conflated. For clarity in the supply chain context, the following definitions are applied. Tactical Intelligence refers to real-time or near-real-time information used for immediate, localized decisions, such as a vessel captain rerouting based on a fresh pirate alert [22]. Operational Intelligence is information used to manage and optimize core business processes over short to medium terms, such as adjusting port schedules or deploying security escorts for a specific voyage [23]. Strategic Intelligence involves long-term analysis of trends used to inform high-level strategy, such as assessing investment in new port facilities or understanding the evolution of militant groups [20].

An effective SCRM framework requires the seamless integration of all three levels. Tactical intelligence enables immediate responses, operational intelligence optimizes ongoing processes, and strategic intelligence guides long-term investments and partnerships [19]. This creates a layered defense that is both responsive and forward-looking. The process involves a continuous feedback loop, where data from tactical and operational activities refines strategic models, ensuring the intelligence function remains relevant [24].

2.4. The Gulf of Guinea Context

The operational challenges in the GoG are rooted in a complex interplay of geopolitical, security, and infrastructural factors. While regional bodies like ECOWAS and ECCAS have established frameworks like the Yaoundé Architecture for maritime security cooperation, implementation is hampered by resource constraints and political will [25]. State fragility, characterized by governance deficits and corruption, fuels instability and creates permissive environments for maritime crime [5], [15].

The region's history as a global piracy hotspot is well-documented. While kidnappings for ransom declined in 2022-2023 due to international pressure, the underlying drivers remain, and the threat has evolved into armed robbery and theft [26], [27]. The endemic issue of oil bunkering finances criminal networks and causes extensive environmental damage [28]. Compounding these security issues are severe infrastructural deficits. Ports suffer from congestion and inefficiency, forcing vessels to wait at anchor for extended periods and increasing their vulnerability [14]. Pipeline networks are aging and poorly monitored, making them easy targets for sabotage and theft [16].

Table 1. Key Geopolitical and Security Actors in the GoG [5], [18], [25].

Actor	Role in the Security Landscape	Influence on Oil & Gas Supply Chain
ECOWAS/ECCAS	Regional security cooperation frameworks (e.g., Yaoundé Architecture).	Provides a legal and institutional basis for maritime security.

Received: 2025-11-09; Accepted: 2026-02-03

Actor	Role in the Security Landscape	Influence on Oil & Gas Supply Chain
National Navies	Patrolling, anti-piracy operations, asset protection.	Direct operational impact on security of vessels and infrastructure.
Criminal Gangs	Piracy, kidnappings for ransom, oil bunkering.	Direct, high-impact disruptive threat to operations and finances.
Militant Groups	Sabotage of infrastructure for political or economic leverage.	Major strategic threat to long-term operational stability.
International Navies	Provide security presence and support to national forces.	Deterrent effects but may face political and legal constraints.

Table 2. Key Infrastructural Challenges in the GoG [14], [16].

Infrastructural Challenge	Impact on Supply Chain Risk	Mitigation Strategy (Intelligence-led)
Port Inefficiency	Increased vessel idle time, higher vulnerability to attack.	Tactical intelligence on port security status; strategic intelligence for long-term investment planning.
Aging Pipelines	High risk of sabotage, oil bunkering, and spills.	Operational intelligence on pipeline monitoring; strategic intelligence on criminal network activities.
Limited Maritime Patrols	Large unguarded maritime zones, allowing criminal activity.	Strategic intelligence to lobby for increased regional cooperation and funding.
Data & Communication Gaps	Delays in information sharing, hindering response time.	Investment in secure and redundant communication networks.

Comparative insights from other maritime regions highlight the GoG's distinct challenges. The Strait of Malacca successfully combated piracy through coordinated international patrols and stringent law enforcement [29]. The Persian Gulf navigates state-sponsored threats and geopolitical tensions. In contrast, the GoG's combination of non-state actors, state fragility, and infrastructural decay creates a uniquely complex "perfect storm" for supply chain disruptions [2].

2.5. Gap in Literature

A review of extant literature reveals significant bodies of work on GoG security [5], [18] and general SCRM theory [6], [7]. However, a distinct gap exists in their integration. Studies on GoG security, such as those by Okafor-Yarwood (2020) and Onuoha (2020), often lack explicit linkage to supply chain operational processes and the specific mechanisms of intelligence integration. Conversely, SCRM literature tends to treat risks like piracy as generic disruptions without delving into the unique context and intelligence mechanisms required to manage them in regions like the GoG. This study fills this gap by conducting an integrated analysis that places intelligence management at the center of SCRM for the GoG's oil and gas sector. It investigates not just the "what" of the risks, but the "how" of intelligence gathering, analysis, and utilization for daily and strategic decision-making, which prior works do not fully address.

3. Methodology

3.1. Research Philosophy and Design

This research is grounded in pragmatism, a philosophy oriented towards solving real-world problems [30]. Consequently, a sequential explanatory mixed-methods design was employed. This approach leverages the complementary strengths of quantitative and qualitative data, providing a more comprehensive understanding than either method alone. The design involved two phases: first, collecting and analyzing quantitative secondary data to establish trends and patterns; second, gathering qualitative data through focused group interviews to explain and provide context for the quantitative findings. The two

Received: 2025-11-09; Accepted: 2026-02-03

datasets were integrated during the interpretation phase to derive robust conclusions.

3.2. Data Collection

Quantitative Data: Secondary data was collected from 2020 to 2024 to ensure currency. Key sources included annual reports from the ICC International Maritime Bureau (IMB) on piracy and armed robbery [26], situational reports from MDAT-GoG [27], energy statistics from the U.S. Energy Information Administration (EIA) [1], and reports from institutes like the Institute for Security Studies (ISS). This data provided objective metrics on incident trends, economic impacts, and the policy environment.

Qualitative Data: Primary data was gathered through virtual focus group interviews with 12 participants. A purposive sampling technique was used to ensure the selection of information-rich participants with direct expertise. The selection criteria required a minimum of 10 years of professional experience in maritime security or oil and gas logistics within the GoG region. Participants were divided into two cohorts: Cohort A (Security Personnel, n=6) comprised two former regional naval officers, two private maritime security contractors, and two security risk analysts from international firms. Cohort B (Industry Players, n=6) included two shipping company operations managers, two logistics managers from major oil and gas firms, and two officials from GoG port authorities. A semi-structured interview guide facilitated discussions on risk perception, intelligence practices, disruption experiences, and improvement suggestions. Sessions were recorded and transcribed verbatim.

3.3. Data Analysis and Validation

Qualitative Analysis: Thematic analysis was conducted on the interview transcripts following the iterative process of Braun and Clarke (2022) [31]. Using NVivo software, initial codes were generated (e.g., "port congestion," "intelligence sharing failure," "tactical rerouting"). These codes were then aggregated into broader themes, such as "Infrastructural Deficits as Risk Multipliers" and "The Intelligence Deficit." The use of NVivo ensured analytical transparency and rigor.

Quantitative Analysis: Content analysis and descriptive statistics were applied to the secondary data. IMB and MDAT-GoG reports were systematically reviewed to extract data on the number, type, and location of security incidents. This data was tabulated to visualize trends.

Triangulation and Validation: Data triangulation was achieved by systematically comparing the quantitative trend data with the qualitative experiential data from the interviews. For instance, statistical trends showing a decline in kidnappings (quantitative) were explained by interview data pointing to a tactical shift towards armed robbery (qualitative). To ensure reliability, a clear audit trail of the research process was maintained. For validity, member checking was performed by sharing a summary of the findings with a subset of participants to confirm accuracy.

Table 3. Integrated Analysis of GoG Security Incidents (2020-2024) and Interview Findings [26], [27].

Year	IMB/MDAT-GoG Incident Data (Piracy/Armed Robbery)	Corresponding Qualitative Insight from Interviews
2020	100+ incidents, 140+ kidnappings.	"Large-scale kidnappings were the primary business model; a state of crisis." (Security Contractor)
2021	50+ incidents, 80+ kidnappings.	"Increased naval patrols began to disrupt the kidnapping model, forcing adaptation." (Former Naval Officer)
2022	20+ incidents, 25+ kidnappings.	"We saw a noticeable drop in major incidents but started getting more reports of petty theft and attempted boardings." (Shipping Manager)
2023	15+ incidents, 10+ kidnappings.	"The gangs are still active. They've just switched to lower-risk, higher-frequency crimes like stealing ship stores." (Security Analyst)

Received: 2025-11-09; Accepted: 2026-02-03

Year	IMB/MDAT-GoG Incident Data (Piracy/Armed Robbery)	Corresponding Qualitative Insight from Interviews
2024 (Q1)	5+ incidents, 5+ kidnappings.	"The underlying threat ecosystem is intact. We cannot afford complacency." (Port Authority Official)

3.4. Ethical Considerations

The research adhered to strict ethical standards. Informed consent was obtained verbally and recorded from all participants. Given the sensitive nature of the discussions, anonymity and confidentiality were guaranteed. Transcripts were anonymized, and data is stored on encrypted servers, scheduled for deletion after five years. The research protocol was approved by an institutional review board.

4. Results and Discussion of Findings

The integration of primary and secondary data revealed a complex risk ecosystem defined by four interconnected themes.

4.1. Presentation of Findings

4.1.1. The Persistence and Evolution of Security Threats

Quantitative data confirms a tactical shift in maritime criminality. While successful kidnappings have decreased, attempted boardings and armed robberies persist, particularly near Nigeria, Ghana, and Angola [26], [27]. Qualitative data contextualizes this shift. A security analyst noted, "The large-scale kidnappings have been suppressed... but we now see a rise in lower-level armed robbery... The criminal networks are still there; they've just adapted their business model." This demonstrates significant adaptive resilience by criminal actors. The threat of onshore infrastructure sabotage, particularly in the Niger Delta, also remains severe, driven by complex local grievances and leading to production shut-ins and environmental damage [5].

4.1.2. Systemic Infrastructural Deficits as a Risk Multiplier

Participants unanimously identified port congestion and aging pipelines as critical concerns. A shipping manager stated, "The congestion outside [Anonymous Port X] is a security nightmare. Vessels waiting at anchor for weeks are sitting ducks." This directly links operational inefficiency to security vulnerability. Secondary data shows vessel waiting times in GoG ports can exceed global averages by 300% [32]. These prolonged stationary periods create predictable targets. Furthermore, aging pipelines are not just vulnerable to sabotage; their frequent failures cause environmental degradation, which in turn fuels local grievances and justifies further attacks, creating a vicious cycle [14]. Thus, infrastructure acts not as a passive constraint but as an active risk multiplier, directly escalating security exposure.

4.1.3. The Critical Intelligence Deficit

A central finding is the "Intelligence Deficit" the gap between the recognized value of intelligence and its effective use. The feedback loop between public and private entities is broken. A former naval officer stated, "Intelligence often flows one way: from companies to us. But actionable feedback is slow and often too generic." Industry participants expressed a need for highly specific, geolocated data rather than vague warnings, desiring intelligence that can be integrated into digital Voyage Management Systems for dynamic routing.

4.1.4. The Overarching Geopolitical Overlay

The broader context of political instability, corruption, and weak judicial capacity enables other risks. While frameworks like the Yaoundé Architecture exist, they are hampered by funding issues and a lack of integrated operations [25]. This fragility fosters a sense of impunity among criminals and deters long-term infrastructural investment, undermining corporate security efforts.

Received: 2025-11-09; Accepted: 2026-02-03

Table 4. Intelligence Gaps and Operational Consequences

Intelligence Gap	Description	Operational Consequence for SCM
Timeliness	Delays in receiving threat alerts; intelligence is often post-incident analysis.	Inability to perform proactive rerouting; vessels enter danger zones unaware.
Specificity	Warnings are too broad (e.g., "High Risk in Niger Delta") and not actionable.	Difficulty in justifying costly security measures or route changes to management.
Sharing Mechanisms	Lack of trusted, formalized platforms for public-private information exchange.	Siloed knowledge: companies rely on expensive private intelligence.
Geopolitical Analysis	Poor understanding of local political dynamics and their impact on criminality.	Inability to anticipate new threat vectors from political changes or grievances.
Infrastructure Monitoring	Lack of real-time data on the status of pipelines and ports.	Reactive response to sabotage instead of predictive maintenance.

4.2. Discussion of Findings

The findings depict a risk ecosystem that is complex, adaptive, and interconnected, with direct implications for SCRM theory and practice.

The evolution of security threats from kidnappings to armed robbery aligns with complex adaptive systems theory [11]. Criminal networks have recalibrated their operations in response to countermeasures, demonstrating that SCRM strategies must also be dynamic. A singular focus on preventing high-impact kidnappings is no longer sufficient; the cumulative damage of persistent, lower-level crime must be addressed.

The role of infrastructural deficits as an *active risk multiplier* significantly contributes to SCRM theory. It moves infrastructure from a peripheral operational issue to a core component of security vulnerability. Inefficient ports are not just a cost center but a critical security flaw that increases the exposure of assets, directly impacting the supply chain's overall vulnerability [7].

The "Intelligence Deficit" is the most critical finding. It reveals a failure to operate the theoretical link between intelligence and resilience. For resilience, defined by visibility, adaptability, and recovery speed [9], intelligence is the fundamental enabler. The current reactive use of intelligence means supply chains are not resilient but merely reactive. Closing this deficit is paramount for building a proactive security posture. Intelligence must become a central strategic capability that drives decision-making from the tactical to the strategic level. For example, real-time tactical intelligence enables vessel rerouting (adaptability), operational intelligence on port conditions prevents unnecessary exposure (visibility), and strategic intelligence on criminal networks informs long-term security investments (enhancing recovery capacity).

Finally, the geopolitical overlay confirms that technical solutions are insufficient without addressing root governance issues [5], [25]. Sustainable supply chain security in the GoG is contingent upon parallel investments in regional stability, judicial reform, and economic opportunity.

5. Conclusion

5.1. Summary of Key Findings

This research demonstrates that the oil and gas supply chain in the Gulf of Guinea operates within a complex system of pervasive security threats, severe infrastructural deficits, and deep-rooted geopolitical instability. These elements are interconnected and compound to one another. The most significant finding is the critical "intelligence deficit," which hinders the transition from reactive to proactive risk management. The study concludes that intelligence is a fundamental enabler for core SCM activities and that achieving a stable supply chain requires an integrated, intelligence-led

Received: 2025-11-09; Accepted: 2026-02-03

approach addressing security, infrastructure, and governance simultaneously.

5.2. Theoretical and Practical Contributions

Theoretically, this study bridges SCRM and security studies, providing an empirical model for how intelligence capabilities build resilience in complex environments. It strengthens the argument that resilience is underpinned by visibility and adaptability, which are products of effective intelligence.

Practically, the research offers an evidence-based action framework. For corporations, it validates investment in dedicated intelligence capabilities and digital tools for dynamic decision-making. For policymakers, it underscores the necessity of functional public-private intelligence sharing platforms and reframes port infrastructure modernization as a security imperative.

5.3. Limitations of the Study

This study has limitations. The qualitative sample size of 12 experts, while rich in expertise, is not statistically generalized. The research relied on open-source data and participant experiences, lacking access to classified intelligence reports, which might reveal different insights. Potential biases include the professional perspectives of the participants, who may prioritize operational and corporate viewpoints over local community concerns. The findings, while potentially transferable, are specific to the GoG context and require adaptation for other regions.

5.4. Policy and Practical Implications

The findings have significant policy relevance. For regional bodies like ECOWAS and ECCAS, operationalizing the Yaoundé Architecture with sustainable funding and an integrated command and control center is critical. Harmonizing legal frameworks to close the impunity gap for maritime criminals is equally important.

For oil and gas and shipping firms, practical and feasible steps include investing in in-house intelligence cells or specialized partners, integrating intelligence feeds into Voyage Management Systems for dynamic routing, and collaborating through industry bodies to create pooled intelligence resources. The implementation of digital tools like AI for predictive analytics of threat patterns and IoT sensors for real-time pipeline monitoring is both feasible and critical for enhancing maritime domain awareness.

5.5. Suggestions for Future Research

Future research should quantitatively model the economic ROI of intelligence-based routing. A detailed case study of the Yaoundé Architecture's implementation would identify specific bottlenecks. Exploring the application of AI, machine learning for threat prediction, and blockchain for secure information sharing is a promising avenue. Finally, research incorporating the perspectives of coastal communities is essential for developing holistic, sustainable solutions.

6. Recommendations

6.1. For Regional Governments and ECOWAS/ECCAS

Regional governments must fully operationalize the Yaoundé Architecture by establishing a permanently funded regional maritime security coordination center. They should create a standardized, secure platform for real-time information sharing between navies and private security actors and harmonize legal frameworks to ensure the prosecution of maritime criminals. Port infrastructure modernization must be treated as a national security priority, funded through public-private partnerships.

6.2. For Oil and Gas Companies and Shipping Firms

Corporations should invest in dedicated intelligence capabilities, either in-house or through vetted partners. This intelligence must be integrated directly into supply chain control towers and voyage management systems for dynamic decision-making. Companies should collaborate through industry bodies to create pooled intelligence resources and invest in technologies like drone surveillance and IoT monitoring for critical infrastructure.

6.3. For Multilateral Partnerships (e.g., UN, EU)

International partners should focus on sustainable capacity building for regional navies,

Received: 2025-11-09; Accepted: 2026-02-03

particularly in intelligence analysis and maritime interdiction. Funding and technical assistance should be directed toward critical infrastructure projects. Multilateral organizations can act as neutral brokers to facilitate trust-building dialogue between regional states and between the public and private sectors.

References

[1] U.S. Energy Information Administration (EIA), *Country Analysis Brief: Gulf of Guinea*, 2023.

[2] R. Villar and F. C. Onuoha, "The Gulf of Guinea: A Regional Sea under Siege," *South African Journal of International Affairs*, vol. 28, no. 2, pp. 195–216, 2021.

[3] Sani and C. Nwafor, "The economic impact of maritime insecurity on the Nigerian oil and gas industry," *Journal of Energy and Development*, vol. 49, no. 2, pp. 201–218, 2024.

[4] F. C. Onuoha, "Maritime security and the politics of piracy in the Gulf of Guinea: Trends, Concerns, and Prospects," *Journal of the Indian Ocean Region*, vol. 16, no. 1, pp. 89–107, 2020.

[5] I. Okafor-Yarwood, "Maritime insecurity in the Gulf of Guinea: A review of the causes and consequences," *Ocean & Coastal Management*, vol. 198, p. 105349, 2020.

[6] W. Ho, T. Zheng, and P. Dey, "A review of supply chain risk management from 2006 to 2019," *Computers & Industrial Engineering*, vol. 144, p. 106456, 2020.

[7] D. Ivanov, *Predictive Supply Chain Management: Using Data and Analytics to Foresee and Mitigate Disruption*. Springer, 2021.

[8] D. Ivanov and A. Dolgui, "A literature review on supply chain resilience: From disruptions to systemic risks," *International Journal of Production Research*, vol. 58, no. 12, pp. 3740–3761, 2020.

[9] T. J. Pettit, K. L. Croxton, and J. Fiksel, "The Evolution of Resilience in Supply Chain Management: A Retrospective on Ensuring Supply Chain Resilience," *Journal of Business Logistics*, vol. 40, no. 1, pp. 56–65, 2019.

[10] O. Adomako, K. Agyei, and A. Antwi, "Building supply chain resilience in a volatile environment: The role of intelligence and agility," *International Journal of Logistics Management*, vol. 34, no. 5, pp. 1120–1145, 2023.

[11] T. Choi, D. Wuttke, and M. Schotman, "A complex adaptive systems perspective on supply chain risk management," *Journal of Operations Management*, vol. 66, no. 6, pp. 680–705, 2020.

[12] W. Klibi and A. Martel, "Modeling and analyzing supply chain disruptions from a complex systems perspective," *European Journal of Operational Research*, vol. 280, no. 3, pp. 918–934, 2020.

[13] G. Baryannis, S. Dani, and G. Harindranath, "Risk Management in the era of Industry 4.0: A systematic review of frameworks," *Computers in Industry*, vol. 125, p. 103362, 2021.

[14] J. Eweje, O. Oguntuase, and E. Ndiva, "Infrastructure Deficit and Maritime Logistics Performance in West African Ports," *Maritime Economics & Logistics*, vol. 24, no. 2, pp. 289–310, 2022.

[15] I. Okafor-Yarwood and A. Adetula, "The human cost of maritime crime in the Gulf of Guinea," *Journal of Human Security*, vol. 17, no. 1, pp. 1–18, 2021.

[16] K. Ikeji and C. Ude, "Challenges of port infrastructure in the Gulf of Guinea and their effects on maritime security," *African Journal of Maritime Affairs*, vol. 19, no. 2, pp. 201–218, 2022.

[17] O. Abiola, *Energy and Geopolitics in the Gulf of Guinea*. Palgrave Macmillan, 2020.

[18] F. Onuoha, "Maritime security and the politics of piracy in the Gulf of Guinea," *Journal of the Nigerian Political Science Association*, vol. 3, no. 1, pp. 1–25, 2020.

[19] E. Edoho, "The role of intelligence in enhancing corporate security in the Nigerian oil and gas sector," *International Journal of Security and Intelligence*, vol. 10, no. 4, pp. 112–130, 2023.

[20] A. Sani and C. Nwafor, "The economic impact of maritime insecurity on the Nigerian oil and gas industry," *Journal of Energy and Development*, vol. 49, no. 2, pp. 201–218, 2024.

Received: 2025-11-09; Accepted: 2026-02-03

[21] S. M. Wagner and C. Bode, “An empirical investigation into supply chain vulnerability,” *Journal of Purchasing and Supply Management*, vol. 27, no. 4, p. 100701, 2021.
[22] M. Duru and S. Akintola, “Tactical intelligence and its application in maritime security operations in the Gulf of Guinea,” *Journal of Maritime Studies and Operations*, vol. 21, no. 3, pp. 345–360, 2024.
[23] Bueger and T. Edmunds, “Beyond seablindness: a new agenda for maritime security studies,” *International Affairs*, vol. 96, no. 4, pp. 887–909, 2020.
[24] S. Iwuanyanwu and J. Amadi, “The intelligence-led approach to combating maritime crime in the Gulf of Guinea,” *Journal of Security Studies*, vol. 25, no. 3, pp. 450–465, 2022.
[25] A. Adetula, “The challenges of maritime security cooperation in the Gulf of Guinea,” *Journal of African Security*, vol. 15, no. 1, pp. 45–62, 2022.
[26] ICC International Maritime Bureau (IMB), *Piracy and Armed Robbery Against Ships Report, First Quarter 2024*. ICC Publishing, 2024.
[27] Maritime Domain Awareness for the Gulf of Guinea (MDAT-GoG), *Quarterly Advisory Report: Q1 2024*, 2024.
[28] N. Bouchaib and A. Hlioui, “Security and risk management in oil and gas supply chains,” *Journal of Supply Chain Management*, vol. 58, no. 2, pp. 220–245, 2022.
[29] Bueger and T. Edmunds, “The politics of maritime security,” *Journal of Strategic Studies*, vol. 43, no. 1, pp. 1–26, 2020.
[30] J. W. Creswell and V. L. Plano Clark, *Designing and Conducting Mixed Methods Research*, 4th ed. SAGE Publications, 2023.
[31] V. Braun and V. Clarke, *Thematic Analysis: A Practical Guide*. SAGE Publications, 2022.
[32] Drewry, *Maritime Security and Global Shipping Risk Outlook 2023*. Drewry Shipping Consultants, 2023.

Received: 2025-11-09; Accepted: 2026-02-03