Int. j. adv. multidisc. res. stud. 2023; 3(6):1770-1779

Received: 11-11-2023
Accepted: 21-12-2023

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Marine Security Risk Management in High-Risk Zones: Lessons from West African LNG Terminals

Ayomipo Ewuola
Nigeria LNG Ltd., Nigeria

DOI: https://doi.org/10.62225/2583049X.2023.3.6.4387
Corresponding Author: **Ayomipo Ewuola**

Abstract
Marine security risk management in high-risk zones is critical for safeguarding vital energy infrastructure, particularly in regions like West Africa, where Liquefied Natural Gas (LNG) terminals face complex and evolving threats. This abstract presents an overview of marine security challenges associated with LNG terminals in West African high-risk maritime zones and distills lessons learned from recent security incidents and mitigation strategies. West African coastal waters are characterized by a heightened risk environment due to piracy, armed robbery at sea, smuggling, and maritime terrorism. LNG terminals, as strategic energy assets, are attractive targets for criminal and militant groups seeking to disrupt energy supply chains and extract economic or political leverage. The unique vulnerabilities of LNG terminals such as their fixed location, dependence on maritime logistics, and proximity to international shipping lanes require robust risk management approaches tailored to the maritime context. This study explores the framework for marine security risk management implemented at several West African LNG terminals, focusing on threat identification, risk assessment, security governance, and operational controls. Key elements include the integration of maritime domain awareness technologies, such as Automatic Identification Systems (AIS) and radar surveillance, coordinated security patrols, and collaboration with regional naval forces and international partners. The importance of stakeholder engagement spanning terminal operators, government agencies, private security firms, and local communities is underscored as a critical factor in sustaining security and resilience. Lessons from West African LNG terminals highlight the necessity of adaptive security strategies that combine technological innovation with intelligence-led operations and community cooperation. The challenges posed by jurisdictional complexities and resource constraints emphasize the need for comprehensive policy frameworks and capacity building at national and regional levels. The findings contribute to the broader discourse on marine security in high-risk zones by providing practical insights into effective risk mitigation tailored to energy infrastructure. These lessons offer valuable guidance for policymakers, industry stakeholders, and security practitioners seeking to protect critical maritime assets in similarly vulnerable regions worldwide.

Keywords: Marine Security, Risk Management, High-risk Zones, West African, LNG Terminals

1. Introduction

Marine security is a critical component in safeguarding energy infrastructure worldwide, particularly Liquefied Natural Gas (LNG) terminals, which serve as pivotal nodes in the global energy supply chain (Akpe *et al*., 2020 [9]; Eyeregba *et al*., 2020). LNG terminals are strategic assets facilitating the import, export, storage, and regasification of natural gas, thus playing a vital role in national energy security and economic stability (Mgbame *et al*., 2020; Ofori-Asenso *et al*., 2020) [54, 57]. Given their fixed coastal locations and reliance on maritime logistics, these terminals are inherently vulnerable to a range of security threats, including piracy, armed robbery, sabotage, and terrorism (Eyeregba *et al*., 2020; Kisina *et al*., 2021). The importance of marine security in this context cannot be overstated, as any disruption to LNG terminal operations can lead to significant economic losses, energy supply interruptions, and broader geopolitical ramifications.

West Africa is recognized as one of the world's most challenging maritime security environments. The region's coastal waters, including the Gulf of Guinea, have experienced a marked increase in high-risk activities such as piracy, maritime armed robbery, illegal fishing, smuggling, and militant attacks targeting shipping and offshore infrastructure (Omisola *et al*., 2020;

Onifade *et al*., 2020) [61, 63]. These threats have escalated due to a combination of socio-economic factors, including political instability, weak maritime governance, and limited naval capacity in many West African states. The Gulf of Guinea, in particular, has become a hotspot for kidnappings for ransom and hijackings, posing significant risks to vessels and offshore installations, including LNG terminals (Akinsooto *et al*., 2014; Iyabode, 2015) [8, 40].

The high concentration of LNG infrastructure in West Africa, driven by the region's abundant natural gas reserves and growing energy demand, further elevates the strategic importance of effective marine security risk management. As such, understanding the unique threat landscape and vulnerabilities faced by LNG terminals in this region is essential for developing tailored security frameworks that can enhance resilience and operational continuity (Ezeanochie *et al*., 2021 [27]; Abayomi *et al*., 2021).

This study aims to provide a comprehensive analysis of marine security risk management specific to LNG terminals operating within high-risk zones in West Africa. The primary objectives include identifying the key threats and vulnerabilities affecting LNG terminals, evaluating existing risk management practices, and distilling lessons learned from past security incidents and mitigation efforts. Furthermore, the study seeks to propose strategic recommendations for improving marine security frameworks by leveraging technological advancements, fostering stakeholder collaboration, and enhancing governance structures (Abayomi *et al*., 2021; Abisoye and Akerele, 2021) [4].

By focusing on West African LNG terminals as a case study, the research contributes to the broader discourse on protecting critical maritime infrastructure in high-risk environments (Afolabi and Akinsooto, 2021 [5]; Kisina *et al*., 2021). The insights derived from this study will be valuable not only to regional stakeholders but also to international energy companies, policymakers, and security practitioners engaged in maritime security operations worldwide. Ultimately, the study underscores the imperative of adopting adaptive, intelligence-driven, and collaborative approaches to marine security risk management to safeguard LNG terminals against evolving maritime threats in West Africa and similar high-risk zones globally.

2. Methodology

The PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) methodology was employed to ensure a structured, transparent, and replicable process for identifying and synthesizing existing literature on marine security risk management in high-risk zones, with specific attention to LNG terminals in West Africa. A comprehensive search was conducted across academic databases including Scopus, Web of Science, ScienceDirect, and JSTOR, as well as grey literature sources such as government reports, industry white papers, and publications from maritime security organizations. Search terms included combinations of "marine security," "LNG terminals," "West Africa," "piracy," "risk management," and "Gulf of Guinea."

The initial search yielded 783 articles and documents. After the removal of duplicates, 642 records remained. These were screened based on titles and abstracts, with 214 selected for full-text review. Inclusion criteria required that sources address marine or port security, risk management strategies in maritime environments, LNG infrastructure vulnerabilities, or case studies from West Africa. Exclusion criteria filtered out studies not related to maritime operations, those outside the regional scope, and articles lacking empirical or applied relevance. After full-text assessment, 87 studies met the eligibility requirements and were included in the final synthesis.

Data extraction focused on capturing key information such as threat typologies, security frameworks, technological and operational measures, stakeholder roles, and regional case studies. Thematic analysis was used to identify recurring patterns, risk factors, and strategic responses across the literature. Studies were appraised for methodological quality, relevance, and contribution to the understanding of security challenges and practices at LNG terminals in high-risk zones.

The PRISMA methodology provided a rigorous foundation for mapping the knowledge landscape and deriving lessons learned. It facilitated the development of evidence-based insights into marine security risk management, helping to shape a nuanced understanding of vulnerabilities, threats, and mitigation strategies applicable to West African LNG terminals.

2.1 Risk Environment in West African Maritime Zones

The maritime zones of West Africa, particularly the Gulf of Guinea, represent one of the most volatile and high-risk regions globally for maritime operations. This region has become synonymous with a complex risk environment characterized by piracy, armed robbery at sea, terrorism, smuggling, and other illicit maritime activities. These threats pose significant security concerns for critical maritime infrastructure, including Liquefied Natural Gas (LNG) terminals, which are especially vulnerable due to their coastal location, economic value, and strategic importance in global energy supply chains (Mgbame *et al*., 2021; Ogbuefi *et al*., 2021) [55, 58].

Piracy and armed robbery at sea are the most prevalent and persistent threats in the region. Unlike the Somali piracy model, West African maritime crime often involves violent boarding of vessels, hostage-taking, and cargo theft close to the coast, with many incidents occurring within national waters rather than in the high seas. The Gulf of Guinea accounted for the majority of global kidnappings of seafarers between 2015 and 2021, highlighting the acute danger posed by organized maritime crime syndicates. Armed groups, often well-equipped and operating from coastal hideouts, have adapted their tactics to exploit weak maritime governance, targeting commercial vessels, offshore platforms, and port facilities (Ogeawuchi *et al*., 2021; Ogundipe *et al*., 2021) [59, 60].

Terrorism also presents an emerging risk, with extremist organizations expanding their influence from the Sahel region towards coastal West African states. Though large-scale maritime terrorist attacks have not yet occurred, the risk remains elevated given the potential for LNG terminals to serve as high-impact targets due to their symbolic and economic significance (Onifade *et al*., 2021; Ajayi and Akanji, 2021 [6]). Furthermore, terrorist groups may engage in maritime smuggling to fund operations or destabilize coastal security frameworks.

Smuggling operations ranging from drugs and weapons to human trafficking flourish in areas where maritime and border enforcement capabilities are weak. These illegal networks not only erode state authority but also create

overlapping threats that challenge the ability of security forces to prioritize and respond effectively (Akinsooto, 2013 [7]; Akinsooto *et al*., 2021). The convergence of criminal and violent extremist networks adds a layer of complexity to threat identification and management in West African maritime zones.

Geopolitical and socio-economic factors further exacerbate the risk landscape. Chronic political instability, corruption, underfunded naval and coast guard units, and ineffective judicial systems create a permissive environment for maritime crime. Many West African nations struggle with limited maritime domain awareness (MDA) and lack the surveillance technologies and logistical infrastructure needed for continuous coastal monitoring (Eyeregba *et al*., 2021) [24]. In addition, widespread poverty and youth unemployment provide a recruitment base for piracy and smuggling operations, turning criminal activity into a perceived economic opportunity for disenfranchised communities.

LNG terminals, as vital nodes in the regional and international energy infrastructure, present unique vulnerabilities within this environment. These installations often feature large, fixed assets located in remote or lightly guarded coastal areas. They rely heavily on predictable shipping schedules, which can be exploited by adversaries for planning attacks. LNG terminals also handle highly combustible materials, making them attractive targets for sabotage or terrorism with potentially catastrophic consequences (Barnes *et al*., 2019; Marcus, 2019) [14, 53]. The reliance on maritime supply chains for inbound and outbound LNG cargoes further exposes terminal operations to disruptions caused by piracy or smuggling activities in adjacent waters.

The physical security of LNG terminals is frequently limited to perimeter defenses, CCTV systems, and private security forces, which may be insufficient against coordinated or high-magnitude threats. Additionally, the lack of regional harmonization in maritime security regulations and response protocols impedes effective incident coordination and information sharing across borders. Given these layered vulnerabilities, LNG operators must adopt comprehensive risk management strategies that integrate marine domain awareness, cross-sectoral intelligence collaboration, and robust emergency response mechanisms (Fornasiero *et al*., 2018; Cassotta *et al*., 2019) [28, 18].

The maritime risk environment in West Africa presents a dynamic and evolving threat matrix that significantly impacts the operational security of LNG terminals. Addressing these risks requires a multifaceted approach, incorporating regional cooperation, capacity-building, and targeted investment in security infrastructure tailored to the unique challenges of the regio.

2.2 Marine Security Risk Management Framework

Effective marine security risk management in high-risk zones, such as West Africa's Gulf of Guinea, requires a systematic and integrated framework. Liquefied Natural Gas (LNG) terminals, due to their critical role in global energy logistics and their inherent vulnerabilities, demand comprehensive approaches to threat identification, risk assessment, governance coordination, and compliance with regulatory standards. A well-structured marine security risk management framework enables LNG operators to anticipate, prevent, and respond to evolving threats while ensuring operational continuity and safety as shown in Fig 1 (Chiappetta, 2018; Uddin, 2019) [19, 73].

The cornerstone of marine security risk management lies in the accurate identification of threats and the systematic assessment of associated risks. Threat identification involves recognizing the range of malicious activities that may impact maritime operations, such as piracy, terrorism, armed robbery, and smuggling. This process utilizes intelligence inputs from national security agencies, maritime domain awareness (MDA) tools, automatic identification systems (AIS), and open-source intelligence (OSINT) to detect patterns and anomalies.

Risk assessment methodologies incorporate both qualitative and quantitative approaches to evaluate the likelihood and potential impact of identified threats (Eckhart *et al*., 2019; Allouch *et al*., 2019) [23, 10]. Commonly used models include Threat-Vulnerability-Consequence (TVC) analysis and the Risk Assessment Matrix, which categorize threats based on severity and probability. These models enable LNG terminal operators to prioritize risks, allocate resources efficiently, and design mitigation strategies proportional to risk exposure. Scenario-based simulations and red-teaming exercises further support dynamic risk assessments by exposing potential weaknesses in current security systems.

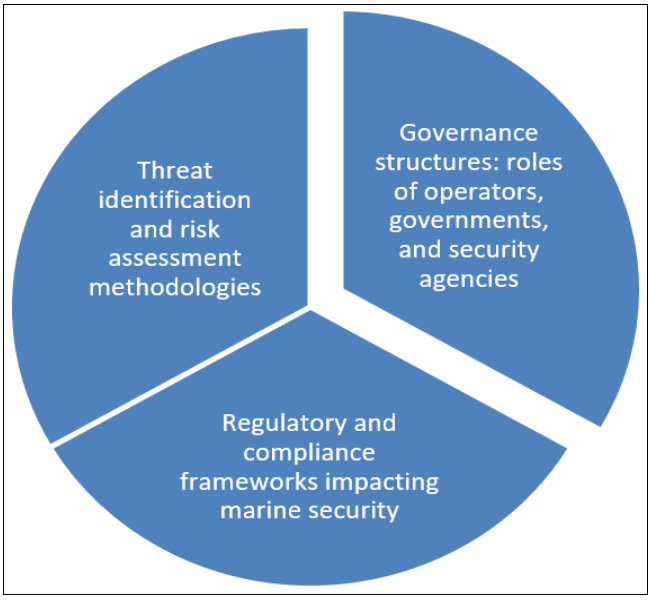

Fig 1: Marine Security Risk Management Framework

Marine security governance requires cohesive collaboration among LNG terminal operators, national governments, regional bodies, and international partners. Terminal operators bear primary responsibility for implementing on-site physical security, cybersecurity, and emergency response measures (Stellios *et al*., 2018; Schneider and Trotta, 2018) [70, 68]. Their role also includes conducting vulnerability assessments, training personnel, and developing standard operating procedures for potential maritime incidents.

Governments play a vital role in policy formulation, law enforcement, and resource allocation. National navies, coast guards, and port authorities are charged with maintaining maritime law and order, conducting patrols, and providing rapid response capabilities. Multilateral organizations, such as the Interregional Coordination Centre (ICC) under the Yaoundé Architecture for Maritime Safety and Security,

facilitate regional cooperation and capacity-building.

Effective governance requires the establishment of joint coordination centers and communication protocols that bridge the public-private divide. This ensures that intelligence sharing, situational awareness, and threat response actions are coherent and timely. Regular joint training exercises and security audits foster trust and build interoperability among stakeholders (Joiner and Tutty, 2018; Bellasio *et al*., 2018) [42, 15].

Marine security in high-risk zones is influenced by a diverse array of regulatory and compliance frameworks. At the international level, the International Ship and Port Facility Security (ISPS) Code, administered by the International Maritime Organization (IMO), sets minimum security requirements for ships and port facilities, including LNG terminals. Compliance with the ISPS Code involves the development of facility security plans, designation of security officers, and implementation of access control, surveillance, and incident reporting mechanisms.

Regionally, the African Union's Lomé Charter and the ECOWAS Integrated Maritime Strategy promote legal and institutional frameworks to combat maritime insecurity. These frameworks call for harmonized policies, coordinated patrols, and shared intelligence among West African nations. Nationally, governments establish regulations and guidelines that may include security certification, inspection regimes, and punitive measures for non-compliance (Havinga, 2018; Guo *et al*., 2019) [36, 35].

LNG terminal operators must navigate these layered regulatory environments while aligning their internal policies with both international standards and local requirements. This involves periodic compliance reviews, risk-based security enhancements, and active participation in policy dialogues. Achieving regulatory alignment not only reduces legal exposure but also enhances the credibility and resilience of LNG operations in high-risk zones.

A robust marine security risk management framework is essential for safeguarding LNG terminals operating in volatile maritime environments (John *et al*., 2018; Gritsenko, 2018) [41, 33]. By integrating structured threat assessments, collaborative governance, and regulatory compliance, operators and stakeholders can mitigate risks, ensure operational continuity, and contribute to regional maritime stability.

2.3 Security Technologies and Operational Controls

Securing Liquefied Natural Gas (LNG) terminals in high-risk maritime zones, such as West Africa's Gulf of Guinea, requires a multi-layered approach integrating advanced technologies and operational controls (Lloyd *et al*., 2019; Fulton, 2019) [50, 30]. Given the strategic and economic importance of LNG facilities, and the threats posed by piracy, armed robbery, and terrorism, robust security systems are essential. Key components include maritime domain awareness tools, physical security and access controls, and coordinated maritime patrols with rapid response capabilities as shown in Fig 2.

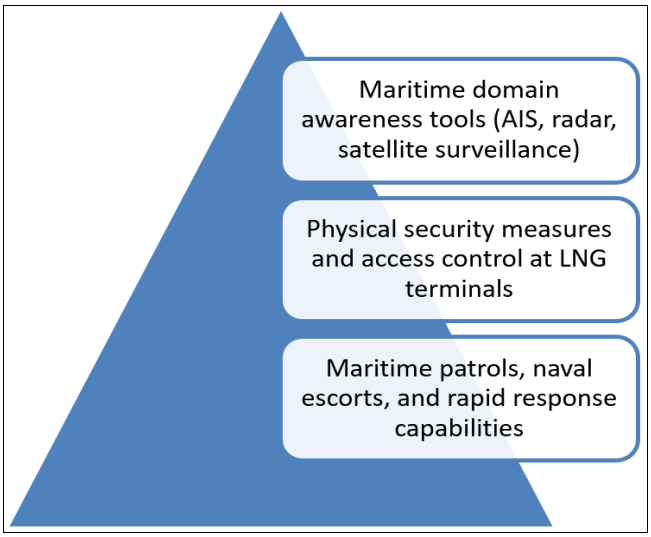

Fig 2: Security Technologies and Operational Controls

Maritime domain awareness (MDA) is foundational to identifying and tracking threats in real-time across vast and often unmonitored sea areas. Tools such as the Automatic Identification System (AIS), radar, and satellite surveillance provide critical situational awareness to LNG operators and maritime security agencies.

AIS transmits vessel identification, course, speed, and destination, enabling continuous monitoring of maritime traffic. While mandatory for commercial vessels under the International Maritime Organization (IMO) rules, AIS can be turned off by malicious actors. Therefore, its utility is augmented with radar systems that detect non-cooperative or non-compliant vessels based on signal reflections. Shore-based and ship-mounted radar units are employed to monitor vessel movement near LNG terminal.

Satellite-based surveillance further enhances coverage, particularly in remote or economically exclusive zones (EEZs). Platforms such as Synthetic Aperture Radar (SAR) and optical imaging satellites allow all-weather, day-and-night tracking of vessel activity. These systems can detect "dark" ships that disable AIS and facilitate early threat detection far beyond the visual horizon (Fournier *et al*., 2018; Kontopoulos *et al*., 2020) [29, 48]. Integration of these tools into central command centers enables predictive threat modeling and improves decision-making.

Physical security is the last line of defense at LNG terminals and involves the deployment of barriers, detection systems, and access controls to prevent unauthorized intrusion. Terminal perimeters are secured with fencing, motion sensors, and infrared cameras, providing 24/7 surveillance and intrusion detection. Secure mooring points, lighting systems, and patrol boats are deployed along waterfronts to deter and respond to unauthorized approach by sea.

Access control protocols regulate the movement of personnel, vehicles, and cargo within the terminal premises. This includes biometric verification, RFID-based ID cards, and multi-factor authentication systems at checkpoints. Visitors and contractors are subjected to background checks

and monitored through CCTV networks with AI-enabled video analytics that flag suspicious behavior in real-time.

Critical infrastructure, such as LNG storage tanks, compressors, and control rooms, are protected by layered security zones with increasing restrictions. Emergency response plans, evacuation drills, and on-site security personnel ensure rapid containment in case of a breach or attack. Physical security not only deters intrusions but also supports regulatory compliance with the International Ship and Port Facility Security (ISPS) Code (Gujar *et al*., 2018; Kopela, 2020) [34, 49].

Operational control in high-risk maritime zones is heavily dependent on mobile assets and coordinated response strategies. Maritime patrols conducted by navies, coast guards, and private security providers maintain a visible security presence, deter hostile actions, and provide real-time intelligence. These patrols are typically executed using fast-attack crafts, offshore patrol vessels, and aerial surveillance platforms such as drones and helicopters.

Naval escorts for LNG carriers transiting through piracy-prone areas are a critical preventive measure. Escort vessels shadow LNG tankers, maintain secure communication links, and are equipped to counter small boat attacks (Stöhs and Bruns, 2018; Dutton *et al*., 2020) [71, 22]. Their presence ensures safer passage from offshore terminals to international shipping lanes.

Rapid response capabilities are essential for neutralizing active threats. Quick Reaction Forces (QRFs) stationed near LNG facilities can deploy within minutes to intercept intruders or support ongoing engagements at sea. Joint operations between operators, security contractors, and national forces enhance response coordination and efficiency.

Inter-agency drills, incident simulations, and secure communication protocols improve interoperability between private and public security entities. Furthermore, intelligence sharing agreements among regional stakeholders, such as the Yaoundé Architecture, bolster coordinated responses to transnational threats.

The integration of advanced MDA tools, robust physical security infrastructures, and proactive operational controls is indispensable for protecting LNG terminals in high-risk maritime environments. A synergistic application of technology and human capabilities ensures the resilience of critical energy infrastructure and the safety of maritime operations in West Africa and beyond (Govindan and Al-Ansari, 2019; Rehak *et al*., 2020) [32, 66].

2.4 Stakeholder Collaboration and Community Engagement

Effective marine security risk management in high-risk maritime zones, such as those surrounding West African LNG terminals, is contingent upon robust stakeholder collaboration and proactive community engagement. Given the complexity of the threat landscape including piracy, terrorism, and smuggling no single entity can manage risks in isolation. Instead, partnerships between terminal operators, national authorities, security forces, private contractors, local communities, and international actors form the backbone of a resilient and adaptive security ecosystem (Koliousis, 2020; Biygautane *et al*., 2020) [47, 16].

One of the central pillars of marine security in LNG operations is the coordination between terminal operators and governmental agencies, particularly navies and maritime security institutions. Terminal operators bear the primary responsibility for securing their assets, yet their ability to address external threats such as offshore piracy or armed attacks depends heavily on the protective reach of state security forces. National navies and coast guards provide maritime patrols, naval escorts, and rapid intervention capabilities that supplement the static and technological measures deployed by operators.

Additionally, private maritime security companies (PMSCs) have become indispensable in zones where state capacity is limited or overstretched. These entities offer onboard armed security personnel, risk assessments, and surveillance expertise tailored to LNG vessels and terminals. A structured partnership between PMSCs and public entities ensures operational transparency, adherence to legal frameworks, and avoidance of jurisdictional conflicts. Memorandums of understanding (MoUs) and joint security committees have been used effectively to formalize such cooperation in West African contexts, particularly in Nigeria and Ghana (Desmidt, 2019; Mangan and Nowak, 2019) [21, 52].

Community engagement plays a critical but often underutilized role in maritime and terminal security. In coastal areas near LNG infrastructure, local populations frequently possess valuable knowledge regarding suspicious maritime activity, unfamiliar vessels, and smuggling networks. Integrating these communities into a broader security framework not only enhances real-time intelligence collection but also builds trust and mutual accountability.

Initiatives such as community policing forums, local security advisory councils, and employment opportunities within the security and logistics value chain have shown promise. By involving communities in the protection of energy assets, operators can reduce the risk of insider threats, sabotage, and local grievances that may be exploited by hostile actors. In Nigeria's Niger Delta, for instance, stakeholder mapping and structured engagement with youth organizations, fisherfolk unions, and traditional authorities have led to a notable reduction in attacks on critical infrastructure.

Moreover, community engagement supports early warning systems that rely on localized information and rapid reporting channels. Training community liaisons in security protocols and equipping them with communication tools allows for timely transmission of intelligence to both operators and government forces. This grassroots intelligence-gathering layer complements high-technology surveillance systems and enhances the accuracy of threat assessments.

The transnational nature of maritime threats necessitates regional and international cooperation. In the Gulf of Guinea, initiatives such as the Yaoundé Code of Conduct (YCC), which facilitates coordination among West and Central African states, have been instrumental in creating a collective security architecture. Through joint maritime centers, shared patrol zones, and real-time information-sharing platforms, countries can respond to threats more efficiently and foster a common operational picture (Androjna *et al*., 2020; Amjad *et al*., 2020) [12, 11].

International actors, including the International Maritime Organization (IMO), the European Union (EU), and the United States, have supported capacity-building programs, naval exercises, and technical assistance to improve regional preparedness. These efforts often include support for legal

harmonization, training of naval personnel, and investment in maritime domain awareness infrastructure.

Furthermore, LNG operators frequently collaborate with global industry groups such as the Oil Companies International Marine Forum (OCIMF) and the International Association of Oil & Gas Producers (IOGP) to establish best practices for terminal security. Participation in these forums ensures alignment with international standards and facilitates the exchange of lessons learned.

A holistic approach to marine security risk management in high-risk zones requires seamless collaboration among a diverse range of stakeholders. Strengthening the interplay between public and private actors, empowering local communities, and leveraging regional and international partnerships enhances the resilience of LNG terminals. Through such integrative strategies, the energy sector can safeguard its operations while contributing to broader maritime stability in West Africa (Voyer *et al*., 2018; García *et al*., 2019) [74, 31].

2.5 Lessons Learned from West African LNG Terminals

West African liquefied natural gas (LNG) terminals operate in a volatile and complex maritime security environment characterized by piracy, armed robbery, smuggling, and geopolitical instability (Siebels, 2020; Onditi, 2020) [69, 62]. Analysis of real-world security incidents at these terminals, and the strategies deployed in response, offers valuable insights into effective risk mitigation, crisis management, and the limitations that persist in operational security frameworks.

One of the most prominent examples is the 2021 hijacking of an LNG support vessel off the coast of Nigeria, near Bonny Island. The incident, attributed to a well-coordinated pirate group, highlighted the persistent vulnerability of LNG supply chains during maritime transit. Despite the deployment of private maritime security contractors onboard, the attackers overwhelmed the crew, resulting in hostages and cargo disruptions. A coordinated response involving the Nigerian Navy and international naval partners eventually resolved the crisis, but not without operational and reputational costs (Oyewole, 2018; Ibrahim, 2020) [65, 39].

Another instructive case occurred in 2018 at the Tema LNG terminal in Ghana, where credible threats of sabotage led to heightened security protocols. Intelligence gathered through local informants prompted a preemptive lockdown and increased naval surveillance. Although the threat was ultimately deemed non-imminent, the terminal's rapid activation of its crisis management protocol demonstrated the importance of proactive threat intelligence and inter-agency communication.

From these and other cases, several best practices have emerged. First is the integration of layered security architectures that combine physical protection (e.g., perimeter fencing, access controls), technological systems (e.g., radar, AIS, video surveillance), and personnel-based solutions (e.g., armed escorts, security patrols). These layers create a defense-in-depth strategy that deters threats before they can impact operations (Abdelghani, 2019; Huang and Zhu, 2020) [3, 38].

Second, the establishment of real-time communication channels between terminal operators, national security agencies, and international partners significantly improves response coordination. Additionally, the incorporation of simulation-based training has allowed security teams to rehearse scenarios involving both sea-based and insider threats (Tolk, 2019; Hermelin *et al*., 2020) [72, 37].

Third, stakeholder engagement with local communities has proven effective in improving early warning systems and intelligence gathering. Initiatives that offer local employment and involve community leaders in security dialogues contribute to a more secure and stable environment, reducing the risk of complicity in attacks (Warburton, 2018; MAHMOUD *et al*., 2018) [75, 51].

Despite progress, several challenges persist in marine security risk management at West African LNG terminals. Jurisdictional fragmentation is one such issue. The legal authority over maritime zones often overlaps between national and regional bodies, leading to confusion and delayed responses during crises. Disputes over who has the right to intervene whether it be the navy, coast guard, or regional coalitions can hinder decisive action (Morris, 2018; Roy, 2020) [56, 67].

Resource constraints also remain a significant hurdle. Many coastal nations in West Africa lack adequate naval assets, aerial surveillance equipment, and trained personnel to provide consistent security coverage. As a result, terminals often rely heavily on private contractors, which, while effective in the short term, may not be sustainable or fully integrated into national security frameworks (Kang *et al*., 2019; Kim and Bui, 2019) [43, 44].

Furthermore, threat actors are becoming more sophisticated, employing advanced tactics such as GPS spoofing, cyber infiltration of vessel navigation systems, and coordinated land-sea attacks. This evolution necessitates continuous investment in security technologies and threat intelligence capabilities. However, the high cost and complexity of such systems often place them beyond the reach of under-resourced states and smaller terminal operators (Derman and Jaeger, 2018; Cassidy *et al*., 2019) [20, 17].

The experience of West African LNG terminals underscores the importance of adaptive and collaborative security strategies. Case studies reveal that while effective responses and best practices are emerging, significant challenges especially those related to jurisdictional clarity, resource availability, and rapidly evolving threats must still be addressed. Strengthening legal coordination, investing in modern technology, and deepening multi-stakeholder collaboration will be essential to securing the future of LNG operations in high-risk maritime zones (Wilson *et al*., 2018; Ang, 2020) [76, 13].

2.6 Strategic Recommendations

The complex and evolving nature of threats in high-risk maritime zones such as West Africa necessitates a robust and forward-looking approach to marine security, particularly for critical infrastructure like liquefied natural gas (LNG) terminals. To ensure resilient and sustainable operations, strategic recommendations must focus on adaptive risk management, enhanced technological and intelligence capabilities, and strengthened institutional capacity at both national and regional levels.

Given the dynamic threat landscape including piracy, armed robbery, smuggling, and terrorism LNG terminals in high-risk maritime zones must adopt adaptive risk management strategies that are proactive, intelligence-driven, and scenario-based. Traditional static models of risk assessment are insufficient for rapidly changing maritime threats.

Instead, operators should implement continuous risk monitoring systems that integrate real-time threat intelligence with on-ground assessments.

Scenario planning and red-teaming exercises should be regularly conducted to test crisis response plans against a variety of potential security breaches, including multi-vector attacks that combine physical intrusion with cyber sabotage. Additionally, a layered security model that incorporates deterrence, detection, delay, and response should be standard. This includes the physical hardening of assets, the use of perimeter intrusion detection systems, and clear escalation protocols aligned with national security forces.

Risk assessments must also be localized, accounting for the socio-political conditions surrounding each terminal. For instance, the security needs of an offshore LNG facility differ from those of an onshore facility in a restive coastal region. Risk profiles should be revisited quarterly or following significant geopolitical events.

To stay ahead of increasingly sophisticated adversaries, the integration of advanced technologies is critical. Maritime domain awareness (MDA) tools such as Automatic Identification Systems (AIS), long-range radar, satellite imagery, and unmanned aerial vehicles (UAVs) should be linked with central command and control platforms for real-time decision-making.

Furthermore, LNG terminals must invest in interoperable technologies that enable intelligence sharing between public and private stakeholders. Developing regional threat intelligence platforms, similar to the Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG), can provide timely alerts and trend analyses. Such platforms should be expanded to allow LNG operators direct access to verified intelligence and allow them to contribute incident data in a secure and anonymized format.

Cybersecurity technologies must also be enhanced, as cyber-physical systems in LNG terminals such as SCADA networks are increasingly targeted. Investment in intrusion detection systems, endpoint protection, and cyber threat intelligence feeds should be aligned with national cyber defense strategies.

A critical enabler of sustainable marine security in high-risk zones is the development of institutional capacity. Governments must invest in training maritime law enforcement and naval personnel, with specialized units capable of responding to LNG-specific threats. Technical training in the use of surveillance equipment, secure communications, and rapid response tactics will significantly improve operational readiness.

At the policy level, national governments should establish standardized security requirements for LNG terminals, including baseline risk assessment methodologies, reporting protocols, and minimum technology benchmarks. These standards should be harmonized regionally through frameworks developed by the Economic Community of West African States (ECOWAS), the Gulf of Guinea Commission, and other regional organizations.

Public-private partnerships must also be formalized, ensuring that terminal operators, governments, and international bodies work collaboratively. Policy tools such as subsidies for security infrastructure, tax incentives for compliance with international best practices, and legal protections for intelligence-sharing initiatives can incentivize private sector engagement.

To secure LNG operations in high-risk West African maritime zones, strategic action must be multidimensional. Adaptive risk management, supported by advanced technologies and institutional collaboration, offers a viable pathway toward enhanced marine security. Ultimately, the integration of local knowledge, global best practices, and cooperative frameworks will be essential to navigating the complex and high-stakes environment of LNG terminal security.

3. Conclusion

The analysis of marine security risk management in high-risk zones, particularly in the context of West African LNG terminals, reveals the critical importance of integrated and resilient security frameworks. Key findings highlight that threats such as piracy, armed robbery, terrorism, and smuggling persist due to a complex interplay of geopolitical instability, socio-economic challenges, and limited maritime governance. LNG terminals, as vital nodes in the global energy supply chain, are especially vulnerable due to their strategic importance, reliance on secure maritime logistics, and exposure to both physical and cyber threats.

The study underscores the necessity of adopting adaptive risk management strategies that are intelligence-driven, technologically enabled, and context-sensitive. It also emphasizes the value of coordinated stakeholder engagement, where terminal operators, governments, security agencies, and local communities collaborate to enhance threat detection, response capabilities, and incident mitigation. Case studies demonstrate that while security breaches have posed significant challenges, they also provide important lessons in resilience-building, crisis management, and institutional learning.

Developing robust marine security frameworks is not merely a defensive measure but a strategic imperative for safeguarding energy infrastructure, ensuring operational continuity, and maintaining investor confidence. Technological integration, such as maritime domain awareness tools and cyber defense systems, alongside governance reforms and capacity-building efforts, are foundational to long-term success.

Looking ahead, the future of marine security risk management in West Africa and similar high-risk zones will depend on sustained political will, investment in human and technical resources, and regional cooperation. The evolution of threats necessitates a continuous adaptation of strategies, greater intelligence sharing, and harmonized regulatory environments. As LNG exports grow and maritime activities expand, ensuring resilient marine security will remain central to energy security and regional stability.

4. References

1. Abayomi AA, Mgbame AC, Akpe OEE, Ogbuefi E, Adeyelu OO. Advancing equity through technology: Inclusive design of BI platforms for small businesses. IRE Journals. 2021; 5(4):235-237. https://irejournals.com/paper-details/1708220
2. Abayomi AA, Ubanadu BC, Daraojimba AI, Agboola OA, Ogbuefi E, Owoade S. A conceptual framework for real-time data analytics and decision-making in cloud-optimized business intelligence systems. IRE Journals. 2021; 4(9):271-272. https://irejournals.com/paper-details/1708317

3. Abdelghani T. Implementation of defense in depth strategy to secure industrial control system in critical infrastructures. American Journal of Artificial Intelligence. 2019; 3(2):17-22.
4. Abisoye A, Akerele JI. High-Impact Data-Driven Decision-Making Model for Integrating Cutting-Edge Cybersecurity Strategies into Public Policy. Governance, and Organizational Frameworks, 2021.
5. Afolabi SO, Akinsooto O. Theoretical framework for dynamic mechanical analysis in material selection for high-performance engineering applications. Noûs, 2021, 3.
6. Ajayi SAO, Akanji OO. Impact of BMI and Menstrual Cycle Phases on Salivary Amylase: A Physiological and Biochemical Perspective, 2021.
7. Akinsooto O. Electrical energy savings calculation in single phase harmonic distorted systems. University of Johannesburg (South Africa), 2013.
8. Akinsooto O, De Canha D, Pretorius JHC. Energy savings reporting and uncertainty in Measurement & Verification. In 2014 Australasian Universities Power Engineering Conference (AUPEC) (pp. 1-5). IEEE, September, 2014.
9. Akpe OEE, Mgbame AC, Ogbuefi E, Abayomi AA, Adeyelu OO. Bridging the business intelligence gap in small enterprises: A conceptual framework for scalable adoption. IRE Journals. 2020; 4(2):159-161. https://irejournals.com/paper-details/1708222
10. Allouch A, Koubaa A, Khalgui M, Abbes T. Qualitative and quantitative risk analysis and safety assessment of unmanned aerial vehicles missions over the internet. Ieee Access. 2019; 7:53392-53410.
11. Amjad SOHAIL, Khan MI, Kanwel S, Ayub N. The Role of Regional Agreements in Enhancing Enforcement of Maritime Crime Laws. Asian Social Studies and Applied Research. 2020; 2:503-510.
12. Androjna A, Brcko T, Pavic I, Greidanus H. Assessing cyber challenges of maritime navigation. Journal of Marine Science and Engineering. 2020; 8(10):776.
13. Ang B. Singapore, ASEAN, and international cybersecurity. In Routledge handbook of international cybersecurity (pp. 218-226). Routledge, 2020.
14. Barnes P, Brabin-Smith R, Clark C, Coyne J, Crane M, Davis M, *et al*. North of 26 south and the security of Australia, 2019.
15. Bellasio J, Flint R, Ryan N, Sondergaard S, Monsalve CG, Meranto AS, *et al*. Developing Cybersecurity Capacity. RAND Europe corporation, 2018.
16. Biygautane M, Clegg S, Al-Yahya K. Institutional work and infrastructure public–private partnerships (PPPs): The roles of religious symbolic work and power in implementing PPP projects. Accounting, Auditing & Accountability Journal. 2020; 33(5):1077-1112.
17. Cassidy R, Singh NS, Schiratti PR, Semwanga A, Binyaruka P, Sachingongu N, *et al*. Mathematical modelling for health systems research: A systematic review of system dynamics and agent-based models. BMC Health Services Research. 2019; 19:1-24.
18. Cassotta S, Sidortsov R, Pursiainen C, Goodsite ME. Cyber Threats, Harsh Environment and the European High North (EHN) in a Human Security and Multi-Level Regulatory Global Dimension: Which Framework Applicable to Critical Infrastructures under. Exceptionally Critical Infrastructure Conditions. (ECIC)? Beijing L. Rev. 2019; 10:317.
19. Chiappetta A. Toward cyber ports: A geopolitical and global challenge, 2018.
20. Derman RJ, Jaeger FJ. Overcoming challenges to dissemination and implementation of research findings in under-resourced countries. Reproductive Health. 2018; 15:121-126.
21. Desmidt S. Conflict management and prevention under the African Peace and Security Architecture (APSA) of the African Union. Africa Journal of Management. 2019; 5(1):79-97.
22. Dutton PA, Kardon IB, Kennedy CM. China Maritime Report No. 6: Djibouti: China's First Overseas Strategic Strongpoint, 2020.
23. Eckhart M, Brenner B, Ekelhart A, Weippl E. Quantitative security risk assessment for industrial control systems: Research opportunities and challenges, 2019.
24. Eyeregba May Equitozia, Nneka Adaobi Ochuba, Omoniyi Onifade, Florence Sophia Ezeh. | IRE Journals | Volume 4 Issue 7 | ISSN: 2456-8880. IRE 1708072 Iconic Research and Engineering Journals 174. A Conceptual Model for Cross-Functional Collaboration Between Finance and Program Teams in Grant-Based Projects, January, 2021.
25. Eyeregba May Equitozia, Omoniyi Onifade, Florence Sophia Ezeh. | IRE Journals | Volume 3 Issue 8 | ISSN: 2456-8880. IRE 1708075 ICONIC RESEARCH AND ENGINEERING JOURNALS 236. Advances in Budgeting and Forecasting Models for Strategic Alignment in Financial and Nonprofit Organizations, February, 2020.
26. Eyeregba May Equitozia, Omoniyi Onifade, Florence Sophia Ezeh. | IRE Journals | Volume 3 Issue 7 | ISSN: 2456-8880. Systematic Review of Financial Operations and Oversight Mechanisms in Multi-Sectoral Organizational Structures, January, 2020.
27. Ezeanochie CC, Afolabi SO, Akinsooto O. A Conceptual Model for Industry 4.0 Integration to Drive Digital Transformation in Renewable Energy Manufacturing, 2021.
28. Fornasiero R, Zangiacomi A, Marchiori I, Barros AC, Pires K, Senna PP, *et al*. D3. 1: Technology Mapping and Scouting, 2018.
29. Fournier M, Casey Hilliard R, Rezaee S, Pelot R. Past, present, and future of the satellite-based automatic identification system: Areas of applications (2004–2016). WMU Journal of Maritime Affairs. 2018; 17(3):311-345.
30. Fulton J. China in the Gulf. About Energy, November, 4, 2019, 1-8.
31. García PQ, Sanabria JG, Ruiz JAC. The role of maritime spatial planning on the advance of blue energy in the European Union. Marine Policy. 2019; 99:123-131.
32. Govindan R, Al-Ansari T. Computational decision framework for enhancing resilience of the energy, water and food nexus in risky environments. Renewable and Sustainable Energy Reviews. 2019; 112:653-668.
33. Gritsenko D. Explaining choices in energy infrastructure development as a network of adjacent action situations: The case of LNG in the Baltic Sea region. Energy Policy. 2018; 112:74-83.
34. Gujar G, Ng AK, Yang Z. Contemporary container

security. Palgrave Macmillan, 2018.
35. Guo Z, Bai L, Gong S. Government regulations and voluntary certifications in food safety in China: A review. Trends in Food Science & Technology. 2019; 90:160-165.
36. Havinga T. The Integration of Private Certification in Governmental Food Controls. Nijmegen Sociology of Law Working Papers Series. 2018; 1.
37. Hermelin J, Bengtsson K, Woltjer R, Trnka J, Thorstensson M, Pettersson J, *et al*. Operationalising resilience for disaster medicine practitioners: Capability development through training, simulation and reflection. Cognition, Technology & Work. 2020; 22(3):667-683.
38. Huang L, Zhu Q. A dynamic games approach to proactive defense strategies against advanced persistent threats in cyber-physical systems. Computers & Security. 2020; 89:101660.
39. Ibrahim HB. Maritime search & rescue services in Nigeria: Examining the Regional Maritime Rescue Coordination Centre Lagos, Nigeria, 2020.
40. Iyabode LC. Career Development and Talent Management in Banking Sector. Texila International Journal, 2015.
41. John A, Yang Z, Riahi R, Wang J. A decision support system for the assessment of seaports' security under fuzzy environment. Modeling, computing and data handling methodologies for maritime transportation, 2018, 145-177.
42. Joiner KF, Tutty MG. A tale of two allied defence departments: New assurance initiatives for managing increasing system complexity, interconnectedness and vulnerability. Australian Journal of Multi-Disciplinary Engineering, 2018.
43. Kang S, Mulaphong D, Hwang E, Chang CK. Public-private partnerships in developing countries: Factors for successful adoption and implementation. International Journal of Public Sector Management. 2019; 32(4):334-351.
44. Kim K, Bui L. Learning from Hurricane Maria: Island ports and supply chain resilience. International Journal of Disaster Risk Reduction. 2019; 39:101244.
45. Kisina D, Akpe OEE, Ochuba NA, Ubanadu BC, Daraojimba AI, Adanigbo OS. Advances in backend optimization techniques using caching, load distribution, and response time reduction. IRE Journals. 2021; 5(1):467-472. https://irejournals.com/paper-details/1708127
46. Kisina D, Akpe OEE, Owoade S, Ubanadu BC, Gbenle TP, Adanigbo OS. A conceptual framework for full-stack observability in modern distributed software systems. IRE Journals. 2021; 4(10):293-298. https://irejournals.com/paper-details/1708126
47. Koliousis I. A conceptual framework that monitors port facility access through integrated Port Community Systems and improves port and terminal security performance. International Journal of Shipping and Transport Logistics. 2020; 12(4):251-283.
48. Kontopoulos I, Chatzikokolakis K, Zissis D, Tserpes K, Spiliopoulos G. Real-time maritime anomaly detection: Detecting intentional AIS switch-off. International Journal of Big Data Intelligence. 2020; 7(2):85-96.
49. Kopela S. Tackling maritime security threats from a port state's perspective. In Maritime Security and the Law of the Sea (pp. 180-201). Edward Elgar Publishing, 2020.
50. Lloyd C, Onyeabor E, Nwafor N, Alozie OJ, Nwafor M, Mahakweabba U, *et al*. Maritime transportation and the Nigerian economy: Matters arising. Commonwealth Law Bulletin. 2019; 45(3):390-410.
51. Mahmoud Y, Connolly L, Mechoulan D. Sustaining Peace in Practice: Building on What Works, 2018.
52. Mangan F, Nowak M. The WesT AfricA–sAhel connecTion. Mapping Cross-border Arms, 2019.
53. Marcus AA. Strategies for managing uncertainty: Booms and busts in the energy industry. Cambridge University Press, 2019.
54. Mgbame AC, Akpe OEE, Abayomi AA, Ogbuefi E, Adeyelu OO. Barriers and enablers of BI tool implementation in underserved SME communities. IRE Journals. 2020; 3(7):211-213. https://irejournals.com/paper-details/1708221
55. Mgbame AC, Akpe OEE, Abayomi AA, Ogbuefi E, Adeyelu OO. Building data-driven resilience in small businesses: A framework for operational intelligence. IRE Journals., 2021; 4(9):253-257. https://irejournals.com/paper-details/1708218
56. Morris LJ. Crossing Interagency Lines: Enhancing Navy-Coast Guard Cooperation to Combat Gray Zone Conflicts of East Asia. Asia-Pacific Journal of Ocean Law and Policy. 2018; 3(2):274-304.
57. Ofori-Asenso R, Ogundipe O, Agyeman AA, Chin KL, Mazidi M, Ademi Z, *et al*. Cancer is associated with severe disease in COVID-19 patients: A systematic review and meta-analysis. Ecancermedicalscience. 2020; 14:1047.
58. Ogbuefi E, Mgbame AC, Akpe OEE, Abayomi AA, Adeyelu OO. Affordable automation: Leveraging cloud-based BI systems for SME sustainability. IRE Journals. 2021; 4(12):393-397. https://irejournals.com/paper-details/1708219
59. Ogeawuchi JC, Akpe OEE, Abayomi AA, Agboola OA, Ogbuefi E, Owoade S. Systematic review of advanced data governance strategies for securing cloud-based data warehouses and pipelines. IRE Journals. 2021; 5(1):476-478. https://irejournals.com/paper-details/1708318
60. Ogundipe O, Mazidi M, Chin KL, Gor D, McGovern A, Sahle BW, *et al*. Real-world adherence, persistence, and in-class switching during use of dipeptidyl peptidase-4 inhibitors: A systematic review and meta-analysis involving 594,138 patients with type 2 diabetes. Acta Diabetologica. 2021; 58:39-46.
61. Omisola JO, Etukudoh EA, Okenwa OK, Tokunbo GI. Innovating Project Delivery and Piping Design for Sustainability in the Oil and Gas Industry: A Conceptual Framework. Perception. 2020; 24:28-35.
62. Onditi F. Conflictology: Systems, institutions, and mechanisms in Africa. Rowman & Littlefield, 2020.
63. Onifade Omoniyi, May Equitozia Eyeregba, Florence Sophia Ezeh. | IRE Journals | Volume 3 Issue 9 | ISSN: 2456-8880. A Conceptual Framework for Enhancing Grant Compliance through Digital Process Mapping and Visual Reporting Tools, March, 2020.
64. Onifade Omoniyi, Nneka Adaobi Ochuba, May Equitozia Eyeregba, Florence Sophia Ezeh. International Journal of Multidisciplinary Research and Growth Evaluation ISSN: 2582-7138. Received: 01-01-

2021; Accepted: 03-02-2021.Volume 2; Issue 1; January-February 2021; Page No. 902-908. DOI: https://doi.org/10.54660/.IJMRGE.2021.2.1.902-908. Systematic Review of Requirements Gathering and Budget Governance in Public Sector and Nonprofit Project Management.
65. Oyewole S. Flying and bombing: The contributions of air power to security and crisis management in the Niger Delta region of Nigeria. Defence Studies. 2018; 18(4):514-537.
66. Rehak D, Hromada M, Lovecek T. Personnel threats in the electric power critical infrastructure sector and their effect on dependent sectors: Overview in the Czech Republic. Safety science. 2020; 127:104698.
67. Roy D. China won't achieve regional hegemony. The Washington Quarterly. 2020; 43(1):101-117.
68. Schneider J, Trotta J. What We Talk About When We Talk About Resilience. Energy LJ. 2018; 39:353.
69. Siebels DIRK. Maritime Security in East and West Africa (Vol. 13). Springer International Publishing, 2020.
70. Stellios I, Kotzanikolaou P, Psarakis M, Alcaraz C, Lopez J. A survey of iot-enabled cyberattacks: Assessing attack paths to critical infrastructures and services. IEEE Communications Surveys & Tutorials. 2018; 20(4):3453-3495.
71. Stöhs J, Bruns S. Maritime Security in the Eastern Mediterranean. Baden-Baden: Nomos, 2018.
72. Tolk A. December. Tutorial on the engineering principles of combat modeling and distributed simulation. In *2019* Winter Simulation Conference (WSC) (pp. 18-32). IEEE, 2019.
73. Uddin SS. Belt and Road Initiative and the Geopolitics of energy. Bangledesh Institute of International and Strategic Studies (BIISS). 2019; 40(2):203-225.
74. Voyer M, Schofield C, Azmi K, Warner R, McIlgorm A, Quirk G. Maritime security and the Blue Economy: intersections and interdependencies in the Indian Ocean. Journal of the Indian Ocean Region. 2018; 14(1):28-48.
75. Warburton D. A passionate dialogue: Community and sustainable development. In Community and sustainable development (pp. 1-39). Routledge, 2018.
76. Wilson CE, Morrison TH, Everingham JA, McCarthy J. Capture and crush: Gas companies in the fracking dispute and deliberative depoliticization. Geoforum. 2018; 92:106-116.