VOL. 09 NO. 9,
AUGUST, 2025
E-ISSN 3026-958X
P-ISSN 3027-1169

African Scholar Publications & Research International
www.africanscholarpub.com

Journal of Science Innovation & Technology Research (JSITR)

Leveraging Technology for Enhanced Operational Effectiveness in the Nigerian Navy

Ali O. Barnabas[1]; & Obembe O. Elijah[2]

[1]International Transportation Management, SUNY Maritime College, Bronx New York.
[2]Department of Marine Science and Technology, School of Earth and Mineral Science, Federal University of Technology, Akure, Nigeria.
Corresponding Author: ochogwuali@yahoo.com
DOI: https://doi.org/10.70382/ajsitr.v9i9.035

Abstract

Nigeria possesses a spacious maritime space that is an important economic aspect and exposed to a complex network of criminal actions. The paper critically examines these security challenges, and they are widespread piracy, advanced kidnapping-for-ransom cases, mass oil piracy, and high economic and environmental cost of illegal, unreported and unregulated (IUU) fishing. According to this report, the historical issue and the incapacity of the states to respond to these endemic menaces adequately, has exacerbated the problem, and thus obstructed the effectiveness of traditional security strategies. The Nigerian Navy must win the battle by transcending the conventional ways of operation and employing modern technology tactically as a force multiplier. The solutions that are presented in this paper are recommended to enhance Maritime Domain Awareness (MDA). This is through the use of a multi-layered system of satellite surveillance (SAR and AIS), shore-based radar, unmanned aerial vehicles (UAVs), and safe data networks to provide real-time and overall intelligence. Additionally, it dwells on the necessity to streamline navy platforms and inject the usage of advanced cybersecurity as a way of protecting digital infrastructure. Lastly, the document presumes that technology is not an enabler, but it is fundamental in improving the efficiency and effectiveness of the operations of the Nigerian Navy. With these strategic investments into these technological pillars, and the challenges that accompany it; financing and human capacity, Nigeria can significantly improve its maritime security, protect its economic interests and stability in the valuable Gulf of Guinea area.

Keywords: Maritime Security, Nigerian Navy, Gulf of Guinea, Maritime Domain Awareness (MDA), Technology Integration.

INTRODUCTION

As the world continues to rely on the oceans as a food source, source of energy, trade and employment, the question of maritime security has become central in the international discourse. The seas, however, are not simply open highways for commerce. They are contested spaces where multiple and intensifying threats converge: overfishing, often through illegal, unreported, and unregulated (IUU) practices; piracy and armed robbery; oil theft and bunkering; toxic waste dumping; and the smuggling of drugs and people. Since the Cold War, these threats have grown sharper. Naval forces in many states were downsized, while surplus weapons and vessels filtered into the hands of criminal networks and non-state actors (Chijioke, 2020).

While global initiatives have tried to mitigate the risks, the African coastline—especially the Gulf of Guinea (GoG)—remains one of the most volatile maritime zones. IUU fishing, piracy, and oil theft continue to flourish, in part because regional states lack the resources to monitor and control their waters effectively. The roots of this problem are not only economic but historical. The colonial partition of Africa left unclear maritime borders and weak state capacity, and post-independence governments often focused resources on preventing civil wars rather than building effective navies (Ukoji & Okolie, 2016). Debt and underfunding have further limited maritime enforcement.

Conventional thinking has long equated maritime security with the mere absence of incidents. Yet this narrow view overlooks the central role of maritime domain awareness (MDA). Boraz (2009) observed that many policymakers assumed navies had always practiced MDA. In reality, MDA as a deliberate, technology-driven strategy is relatively new. Radar and the Automatic Identification System (AIS) have been around for decades, but they cannot explain a vessel's intentions or place its movements in context. As Thomas (2021) argues, what matters is not only surveillance but interpretation—turning data into usable knowledge.

The Gulf of Guinea highlights the costs of neglecting this. Regional strategies have been overwhelmingly "land-centric," focused on internal unrest, leaving states poorly equipped to deal with maritime threats (Gilpin, 2009). International and regional partners have therefore sought to build capacity around MDA, stressing information integration and situational awareness as prerequisites for sound decision-making. Doorey (2014) put it plainly: without knowing what is happening across inland waterways, territorial seas, Exclusive Economic Zones, and even the high seas, no policy or enforcement can succeed.

Technology has thus become a cornerstone of reform. The Yaoundé Code of Conduct (2013) and its associated Architecture created

a framework for regional cooperation, with mechanisms for information sharing, capacity building, and joint patrols (Murphy, 2010). These efforts have been endorsed by the UN Security Council through Resolutions 2018, 2039, and 2634, which urged states in the region to intensify collaboration against piracy and armed robbery.

Nigeria, with its vast hydrocarbon resources and fisheries in the Niger Delta, illustrates both the stakes and the difficulties. Despite the passage of the Suppression of Piracy and Other Maritime Offences (SPOMO) Act in 2019, insecurity persists. Piracy, kidnappings, and violent attacks regularly endanger coastal communities and international shipping (Brume-Eruagbere, 2017). Scholars such as Otto (2016) link these crimes to unresolved land-based conflicts that spill over into maritime zones.

The challenges are well known: too few patrol platforms, weak coordination between agencies, underdeveloped intelligence systems, and ineffective prosecution. Pranav (2016) reminds us that crime is spatial—it is bound to time, location, and process—which means effective monitoring requires predictive as well as reactive tools. Murphy (2010) adds that responsibility cannot rest solely with governments; shipping companies must adopt best practices, from additional lookouts to rapid distress protocols, to reduce their vulnerability.

Taken together, the evidence suggests that maritime insecurity in the Gulf of Guinea, and in Nigeria in particular, is not simply a matter of policing the seas. It is an expression of greater historical, institutional, and operational dis-junctions. The solution to these involves simultaneous technology-investment, particularly MDA systems, and governance, inter-agency collaborations, and community involvement. When used in the right way, MDA is not a luxury. It is based on it that all the other elements of maritime security are based.

In this paper, attention is drawn to the way in which technology can help the Nigerian Navy and other maritime security agencies to have a more efficient output and provide the Golf of Guinea with a more intensive security level. We will discuss the application of Synthetic Aperture Radar, Unmanned Vehicles, Autonomous Vehicles and some of the recent technology that will help the agencies to complete their assignment and ensure that the Nigerian waterways are safe and secured.

HISTORICAL INSIGHT OF MARITIME SECURITY AND TECHNOLOGY

This section, after having done a thorough historical analysis, shows the dynamic nature of the relationship between technological advancement and the multidimensional nature of the current issues of maritime security. It starts with such ancient civilizations as the adventurous Phoenicians and the seaward Greeks who survived piracy and stormy seas using primitive and yet revolutionary technologies such as oar-driven ships and sky-reading (Markoe, 2000; Oleson, 2008). Significant technological advances during the Industrial Revolution propelled the modernization of naval fleets and expanded maritime domain awareness (Lambert, 2010). The Age of Exploration introduced audacious European voyages, driving innovation through instruments like the astrolabe and compass, expanding the horizons of maritime endeavor (Jowitt, 2001; Turner, 1980). The rise of naval empires, epitomized by the formidable British

Royal Navy, underscored the geopolitical significance of maritime security and witnessed technological feats such as copper sheathing and precise chronometers (Bowers & Koh, 2017; Fuller, 1989).

The cataclysmic events of the World Wars ushered in submarines, mines, and long-range artillery as unprecedented threats, but also ignited a technological revolution with advancements like sonar, radar, and encryption technologies (Cunliffe, 2017). The contemporary era grapples with traditional challenges like piracy and smuggling, alongside emerging threats such as maritime terrorism and cyberattacks, met by cutting-edge solutions including satellite surveillance, unmanned underwater vehicles (UUVs), and advanced data analytics, all within the context of a globally connected and geopolitically complex world (Murphy, 2021).

Throughout history, technological progress and maritime security have maintained a symbiotic relationship. Technological innovations have not only empowered nations and civilizations to protect their maritime interests but have also been instrumental in driving the evolution of maritime challenges themselves. In the modern era, it is recognized that the relentless march of technology continuously shapes the landscape of maritime security, establishing a framework for the exploration of challenges and opportunities in subsequent chapters.

THE CONTEMPORARY MARITIME THREAT LANDSCAPE AND SOME REPORTED CASES IN NIGERIA

Navigating the contemporary maritime threat landscape reveals a complex web of challenges, each intertwined with global security, environmental sustainability, and legal boundaries. Such threats are piracy and maritime terrorism, human trafficking, and migrant smuggling, environmental degradation, and illicit trafficking that might pose serious risks not only to the safety and security of the maritime routes but to the global commerce and ecological balance (Murphy, 2021; UNODC, 2022). These are common and significant problems, which require a comprehensive and close analysis. The relevance of these threats, including centuries-old history of piracy, points to the necessity of the dynamic and changing way of considering maritime security (Hastings, 2009). These problems are also multidisciplinary in nature and are associated with security, legal frameworks and ethical, environmental, and political factors. This complexity demands a narrowed approach in order to have an in-depth comprehension, which is backed with well documented cases and practical considerations.

In order to have a complete understanding of the concept of maritime insecurity, then it is important to define security first. Ewetan and Ese (2014) define security as the state of peace and the lack of anxiety in order to develop the country. This way it is a state of order and unity that promotes growth of the society. Conversely, anything that disrupts this state can be considered insecurity. Big-Alabo and Ezugwu (2022) further define security as a “dynamic situation that helps in guarding against threats to its deep-rooted values and interests.”

Maritime insecurity, therefore, refers to the threats and attacks experienced within the maritime environment.

Nigeria's maritime domain is undeniably vital, serving as a cornerstone of its national economy, security, and regional influence across West Africa. This expansive domain spans its extensive coastline along the Gulf of Guinea and its intricate network of navigable inland waterways. However, this critical asset faces persistent and severe threats. Nigeria's waters are a hotspot for various maritime crimes, including piracy, kidnapping for ransom, widespread oil theft (illegal bunkering), illegal fishing, smuggling, and significant environmental damage (Adebayo & Ojo, 2020; International Maritime Bureau [IMB], 2021). These illicit activities gravely undermine the Nigerian economy, disrupt international trade, and inflict substantial harm on vulnerable coastal communities (Onuoha, 2012).

The persistence of these threats is fueled by a complex interplay of factors, such as pervasive poverty, weaknesses in law enforcement, insufficient surveillance capabilities, endemic corruption, and broader political and economic instability (Onuoha, 2018; Okafor-Yarwood, 2020). Though recent proactive efforts, including intensified operations by the Nigerian Navy and the enactment of the Suppression of Piracy and Other Maritime Offenses (SPOMO) Act, have yielded some positive results, leading to a notable decline in certain crimes, the challenge remains formidable (Akinwale, 2021). To Effectively secure Nigeria's maritime domain demands a comprehensive, integrated, and cooperative strategy involving enhanced surveillance, robust regional cooperation, and a dedicated focus on addressing the fundamental socio-economic issues that drive individuals towards these criminal enterprises.

Similarly, to comprehensively grasp the prevalent security landscape of Nigeria's vital maritime sector, a critical examination of its primary contributing factors is essential. The subsequent analysis delineates key elements that underpin the enduring threats and insecurities confronting the "Giant of Africa's" invaluable domain.

REPORTED THREAT CASES IN NIGERIA

1. Piracy and Armed Robbery at Sea

Piracy is arguably the most publicized maritime threat affecting Nigeria, particularly within the Gulf of Guinea. Attacks on vessels often involve theft, kidnapping, or siphoning of cargo, with Nigerian pirates frequently noted for their violence (Onuoha, 2013; Murphy, 2021). In recent years, kidnapping for ransom (K&R) has emerged as a dominant trend. Instead of merely stealing cargo, pirates increasingly abduct crew members, especially foreign seafarers, and hold them for ransom. The MV Mozart incident of January 2021 starkly illustrates this trend, where pirates killed one crew member and kidnapped fifteen others off Nigeria's coast (Al Jazeera, 2021). Similarly, the Bourbon Liberty 249 attack in October 2012 involved the abduction of seven crew members, underscoring the long-standing severity of this issue (Bourbon Offshore, 2012).

These incidents highlight the evolving tactics of pirates, the severe human costs involved, and the jurisdictional challenges of combating maritime crime in Nigeria. Cargo theft, often

referred to as petro-piracy, also remains prevalent. Product tankers are especially targeted for their refined petroleum cargo, with notable hijackings reported in 2012 off Benin, Togo, and Lagos (International Maritime Bureau, 2013).

2. Oil Theft and Illegal Bunkering

Illegal oil bunkering represents one of the largest economic and environmental crimes in Nigeria's maritime sector. Criminal groups routinely vandalize pipelines and establish illicit refining sites, leading to massive financial losses and severe ecological damage (Asuni, 2009; Obi, 2010). Operations typically involve "hot-tapping" into pipelines to siphon crude oil, which is then refined in makeshift facilities or shipped offshore for resale. The Nigerian Navy has reported frequent arrests of vessels engaged in illegal bunkering and the destruction of hundreds of illicit refineries (Nigerian Navy, 2023). These highly organized operations are often enabled by local complicity and, in some cases, corruption within security forces.

3. Illegal, Unreported, and Unregulated (IUU) Fishing

IUU fishing is another significant maritime threat, resulting in economic losses estimated at over $600 million annually (FAO, 2018; Agnew et al., 2009). Foreign industrial trawlers from China, the EU, Russia, and other nations frequently exploit Nigeria's Exclusive Economic Zone (EEZ), depleting vital fish stocks such as tuna, shrimp, and shark. This has devastated artisanal fishing communities, reduced Nigeria's domestic fleet, and contributed to an estimated loss of more than 300,000 jobs (Okafor-Yarwood, 2020). The long-term impact includes food insecurity, declining livelihoods, and ecological imbalance in Nigeria's coastal waters.

4. Smuggling and Human Trafficking

Nigeria's extensive coastline and porous borders provide fertile ground for smuggling and human trafficking via maritime routes. Illicit commodities such as drugs, poultry products, and textiles are trafficked through coastal communities, often facilitated by bribery and collusion with corrupt officials (Akinyemi, 2019). In parallel, human trafficking has escalated through Nigeria's waterways, with traffickers disguising victims as stowaways on vessels. Agencies such as the National Agency for the Prohibition of Trafficking in Persons (NAPTIP) have partnered with maritime authorities to disrupt these practices, though challenges remain (NAPTIP, 2021).

5. Maritime Terrorism and Militancy

Although large-scale maritime terrorism has declined compared to the height of Niger Delta militancy, the legacy of groups such as the Movement for the Emancipation of the Niger Delta (MEND) continues to shape Nigeria's security landscape. During the 2000s, MEND and similar groups carried out attacks on oil installations, kidnapped oil workers, and sabotaged pipelines, actions driven by political grievances and criminal enterprise (Ikelegbe, 2013).

While government amnesty programs significantly reduced overt militancy, underlying socio-economic grievances persist, and sporadic attacks still occur. International advisories, including those from the UK government, continue to warn of kidnapping risks and attacks on offshore oil and gas facilities in the Niger Delta (UK Foreign, Commonwealth & Development Office, 2023)

ROLES OF TECHNOLOGY TO ENSURE OPTIMAL SECURITY AND EFFICIENT NAVAL OPERATIONS IN NIGERIA

These multifaceted threats not only severely undermine Nigeria's economic stability and disrupt international trade but also inflict profound harm on vulnerable coastal communities and the delicate marine ecosystem.

Technology emerges not merely as an enabler, but as an indispensable force multiplier, critically vital for ensuring optimal security and enhancing the efficiency of naval operations within Nigeria's maritime domain. By leveraging advanced technological solutions, Nigeria can strengthen its capacity to monitor, detect, deter, and respond to maritime threats, thereby safeguarding its national interests and fostering sustainable development. This section focuses on some notable technologies that have the potential of enhancing and progressing the effort of the Nigerian Navy in combating the insecurity rampaging the maritime industry.

Maritime Domain Awareness (MDA) Systems

Technology plays a transformative role in building a resilient maritime security architecture. At the forefront is Maritime Domain Awareness (MDA), defined as the effective understanding of anything associated with the maritime domain that could impact security, safety, economy, or the environment (United States Department of Defense, 2013). Robust MDA systems integrate a variety of technologies, from satellites and radar to Automatic Identification Systems (AIS), enabling authorities to detect, track, and respond to maritime threats more effectively.

Understanding Synthetic Aperture Radar (SAR) for Maritime Security

Synthetic Aperture Radar (SAR) is a sophisticated form of radar that generates high-resolution images of the Earth’s surface. Unlike optical satellites that depend on sunlight, SAR is an “active” sensor that transmits its own radio waves and measures the reflected signals (Moreira et al., 2013). This feature enables SAR to cut through cloud, mist and darkness and provides a highly valued all-weather, day-night surveillance solution. In maritime use, SAR is especially useful in detection of vessels, patrolling of coastal activities, and enforcement of illegal operations.

Key Applications of SAR in Maritime Security

Combating Illegal, Unreported, and Unregulated (IUU) Fishing: IUU fishing is one of the

most urgent issues of maritime regulation. Numerous ships that are involved in this practice intentionally switch off their AIS transponders in order to escape. SAR addresses this by:
Detection of dark ships: When the SAR imagery is combined with AIS data, the authorities can detect the ships that do not transmit any signals (Park et al., 2020).
Vessel wake analysis: SAR is able to capture vessel wakes and movement patterns that can be used to verify the presence and direction of ships, despite them moving out of an area (Kanjir et al., 2018).

Piracy and Armed Robbery Prevention
SAR provides continuous monitoring of the high-risk waters and, thus, suspicious activities of vessels in the piracy-prone regions can be detected and addressed:
Surveillance of high-risk areas: SAR is able to give early notice of pirate activity by monitoring abnormal vessel congestion or abnormal routes (Kourti et al., 2005).
Assistance in emergency response: SARs are able to find distressed vessels in the case of poor visibility, which will assist in quicker rescue or intervention efforts (Ferraro et al., 2017).
Smuggling and Trafficking Interdictment.
Monitoring suspicious ships: Nighttime or covert operations can also be identified with the help of SAR images, particularly when the ships do not follow the regular traffic patterns (Greidanus and Alvarez, 2021).
Detecting the anomalies: SAR data can be differentiated by distinguishing small and fast-moving boats or debris associated with illegal activity (Kersten et al., 2016).

Advantages of SAR for Maritime Security
SAR is a superior maritime surveillance technology that is unparalleled due to the fact that it provides:

- All-weather operation: not affected by the cloud cover or storms.
- Day and night vision: not dependent on sunlight.
- Large ocean areas can be imaged in a single scan: wide-area coverage.
- Diversity in identifying vessels: can detect vessels of varying sizes and operation types (Moreira et al., 2013).

AUTOMATIC IDENTIFICATION SYSTEM (AIS) AND VESSEL MONITORING SYSTEM (VMS)

Although Synthetic Aperture Radar (SAR) offers an advanced technology of identifying dark vessels, the Automatic Identification System (AIS) and the Vessel Monitoring System (VMS) are the cornerstone technologies that ensure transparency in the sea. Together, these systems create a global surveillance network that enhances Maritime Domain Awareness (MDA) and strengthens enforcement mechanisms.

Automatic Identification System (AIS)

The Automatic Identification System (AIS) is an automated tracking system mandated on most commercial vessels and used by vessel traffic services (VTS). AIS transponders broadcast vessel information via VHF radio signals, allowing all AIS-equipped vessels and shore stations within range to receive real-time updates (IALA, 2016).

AIS data is typically divided into three categories:

- ***Static information***: vessel name, MMSI number, call sign, dimensions, and type.
- ***Dynamic information:*** position, course over ground, speed, and navigational status.
- ***Voyage-related information***: destination and estimated time of arrival.

Although AIS was originally designed to prevent collisions, it has become an essential security tool. For example:

- ***Traffic monitoring:*** Authorities use AIS to track commercial shipping, fishing vessels, and passenger ships, detecting anomalies in declared routes (Kourti et al., 2005).
- ***Search and rescue***: AIS assists in locating vessels in distress and coordinating emergency responses (IALA, 2016).
- ***Detecting suspicious behavior***: Deviations from shipping lanes or unexplained stoppages may trigger inspections.
- ***Interdiction of illicit activity***: AIS data can be cross-referenced with intelligence sources to identify smuggling, trafficking, or sanctions evasion (Balduzzi et al., 2014).

However, a key weakness of AIS is its reliance on voluntary transmission. Crews can disable AIS transponders to evade detection—a tactic often associated with illegal activities such as IUU fishing and oil smuggling (Tournadre, 2014).

Vessel Monitoring System (VMS)

The Vessel Monitoring System (VMS) is a satellite-based technology primarily designed to monitor commercial fishing vessels. VMS is not an open broadcast model like that of AIS, but sends data directly to central monitoring authority which is usually run by governments or regional fisheries management organizations (RMMOs) (FAO, 2007).

It can be used in the following ways:

- ***Imposing fishing zones:*** VMS is also useful to make sure that vessels are fishing within the authorized territory, and authorities are immediately notified when they venture into the protected areas (Natale et al., 2015).
- ***Fighting IUU fishing:*** Sustained reporting has a good data trail that can facilitate compliance and prosecution (Park et al., 2020).
- ***Quota management:*** The real time fleet tracking will allow fisheries managers to balance quotas and avoid overfishing (FAO, 2018).

VMS is therefore the key to sustainable fisheries management and maritime law enforcement.

Key Differences and Synergy of AIS and VMS

Table 1: Showing the differences and synergy of Automatic Identification System and Vessel Monitoring System.

Feature	Automatic Identification System (AIS)	Vessel Monitoring System (VMS)
Primary Purpose	Collision avoidance & traffic management	Fisheries management & enforcement
Transmission	VHF radio (broadcast to vessels/stations)	Satellite (direct to authority)
Data Recipient	Other vessels & coastal monitoring stations	Government authorities / RMFOs
Flexibility	Mandatory for most large commercial vessels	Mandatory for fishing fleets in regulated zones
Security Weakness	Easily turned off without immediate detection	Can be disabled, but alerts are triggered

While AIS and VMS have distinct functions, they complement each other to produce a fuller picture of maritime activity. AIS provides a real-time, decentralized view of global maritime traffic, while VMS delivers centralized oversight of regulated fishing activity. When either system shows anomalies—such as a vessel suddenly going "dark"—authorities often deploy advanced tools such as SAR to verify the situation (Greidanus & Alvarez, 2021). This synergy between AIS, VMS, and SAR constitutes a robust, multi-layered approach to maritime security and transparency.

COASTAL RADAR AND SURVEILLANCE SYSTEMS

In the layered approach to maritime security, Coastal Radar and Surveillance Systems represent the most immediate and tactical line of defense. Unlike satellite-based tools such as Synthetic Aperture Radar (SAR), the Automatic Identification System (AIS), and the Vessel Monitoring System (VMS), which provide broad oceanic coverage, coastal systems focus on littoral zones, ports, and territorial waters. They offer a high-resolution, real-time picture of vessel movements, forming the "eyes and ears" of coast guards and naval forces. By delivering ground-truth data to complement satellite intelligence, these systems strengthen the multi-layered shield needed to counter diverse maritime threats ranging from smuggling to piracy.

Components of a Coastal Surveillance System

Modern coastal surveillance networks are built on integrated sensors, communication systems, and command centers that fuse multiple data streams into a coherent maritime picture. Key components include:

1. Coastal Radar

Radar remains the cornerstone of coastal surveillance. Positioned at strategic intervals along coastlines, coastal radars use high-frequency electromagnetic waves to detect and track vessels within short-to-medium ranges, typically 0.5 – 40 nautical miles (Ray & Ghosh, 2015). Unlike AIS, radar can detect both compliant and non-compliant vessels, including small, wooden, or fiberglass boats often used in smuggling and illegal fishing. Their 24/7, all-weather capability ensures uninterrupted monitoring of surface activity (Berković et al., 2019).

2. Electro-Optical (EO) and Infrared (IR) Cameras

EO and IR imaging systems are used to complement radar as they allow visual classification of vessels. EO cameras offer high-resolution images in the daytime, whereas IR sensors can trace heat events, which is why they cannot do without night and low-visibility surveillance (Millefiori et al., 2016). In addition to detecting vessels, IR cameras can show signs of activity on the ship, e.g., running engines and allow identifying active and inactive ships (Chandra and Jain, 2019).

3. AIS Shore-Based Receivers

AIS receivers are also embedded in coastal surveillance stations to intercept signals sent by vessels that are in compliance (IALA, 2016). Crossover radar detections with AIS data can help the authorities detect so-called dark vessels, or vessels that do not transmit identification signals (Tournadre, 2014). This two-track approach improves the detection of anomalies and guarantees responses to interdiction processes in a shorter time.

4. VMS Data Integration

The use of VMS data streams to coastal surveillance systems is additional in monitoring fishing activities in an Exclusive Economic Zone (EEZ) of a given country. Through integrating VMS and radar as well as AIS feeds, authorities get a clear operational view of both commercial shipping and fishing activity (Natale et al., 2015). This surveillance mode assists in the enforcement of fisheries laws, inhibition of illegal fishing, as well as identification of illegal movements of vessels.

THE ROLE OF UNMANNED VEHICLES IN MARITIME SECURITY

Unmanned Surface Vehicles (USVs) and Unmanned Aerial Vehicles (UAVs) are also changing the way maritime security is conducted by extending its surveillance, minimizing risk to human life, and offering affordable, long-range, and continuous surveillance. These systems serve as effective force multipliers in the navies, coast guards, and law enforcement agencies at sea by automating activities that are dangerous, monotonous, or resource-intensive (O'Hanlon, 2020).

Unmanned Aerial Vehicles (UAVs)

UAVs are the eyes on the sky, which have high-resolution infrared and electro-optical cameras that provide real-time images of maritime activity (Cunningham and Roberts, 2020). They can best identify so-called dark vessels, which turn off their Automatic Identification System (AIS) transponders, and also observe hard-to-reach coastal and oceanic areas.

Unmanned aerial and surface systems are not merely experimental technologies, but it is clear that they are becoming part of the contemporary maritime security practice. The UAVs and USVs will be increasingly important in the protection of world maritime space as their endurance, autonomy, and sensor payloads keep increasing.

Search and rescue missions are also very essential in use of UAVs. They have the ability to assist in reducing response time and enhancing survival rates as they provide live video feeds that direct rescue boats to the people in distress by covering large areas of the ocean rapidly (Karjalainen et al., 2021). Besides optical sensors, UAVs may also be equipped with Synthetic Aperture Radar (SAR) that allows them to observe during the day and night, and the ability to break through clouds and unfavorable weather conditions (Clapperton, 2018). This renders them invaluable in the long-range Intelligence, Surveillance and Reconnaissance (ISR) operations.

Unmanned Surface Vehicles (USVs)

Persistent patrol and monitoring is being put into use by USVs. They can work continuously during days or weeks, keeping a constant guard on assets of high value like ports, oil installations, and vital sea ways (Manley, 2016).

In addition to patrols, USVs have environmental and oceanographic sensors that allow collecting data on the weather, currents, and pollutants and monitor oil spills and other criminal activities on the sea (Schmidt et al., 2020). Other hi-tech USVs also have non-lethal deterrents, which enable them to intercept suspicious vessels and hold on to them until manned patrols reach them (Mclaren & Jakobi, 2017).

Importance and Effectiveness of Unmanned Vehicles

UAVs and USVs can be successfully employed in the maritime security due to several strategic benefits:

- ***Cost-Efficiency***: Unmanned systems are much cheaper to develop, maintain, and run than manned vessels or aircraft and can be expanded to more resource-constrained agencies (Wright, 2021).
- ***Risk Reduction:*** Unmanned systems decrease risks to human life by putting them in high-risk situations, such as piracy interdictions, storm surveillance or hostile environments (O'Hanlon, 2020).
- ***Stability and Permanence:*** Contrary to human crews, unmanned systems have the ability to work 24-hour shifts in large parts of the sea, providing continuous coverage in large areas of the sea (Manley, 2016).

- ***Unobtrusiveness and Dexterity:*** Numerous unmanned systems are miniature, silent, and stealthy, so they can be used to obtain intelligence without notice (Schmidt et al., 2020).

The Strategic Input of AUVs

Where surface and aerial drones (USVs and UAVs) are surveying the seas and skies, the Autonomous Underwater Vehicles (AUVs) are bringing a revolution to the underwater security. These are self-driving, remotely controlled robots that are free to roam and carry out assignments on pre-programmed missions and gather information and complete tasks in a hostile and inaccessible environment. Their unique capabilities make them indispensable for a wide range of naval and maritime law enforcement operations (Bellingham & Rajan, 2007). The primary function of an AUV is to conduct missions that are too dangerous, too long, or too costly for manned submersibles or divers.

1. Underwater Surveillance and Reconnaissance

AUVs are ideal platforms for covert underwater surveillance. They are able to spy on the actions of foreign submersibles, follow underwater ships, and inspect the subsea structures like communication cables, offshore oil rigs, and pipelines (Strode and Hendrix, 2019). They are also very powerful tools in intelligence gathering since they can work silently and over long durations (Obembe and Ali, 2025).

2. Mine Countermeasures (MCM)

Mine warfare is a major naval threat and AUVs are becoming the focus of mine countermeasures (MCMs). AVU can search a pre-defined pattern of the seabed, identify, and categorize suspicious objects without putting human divers at risk (Manley, 2008; Rigby, 2019). This greatly minimizes the operational risks that were traditionally related to mining operation of clearing mines.

3. Port and Harbor Security

Smaller AUVs are used to improve the security of ports and harbours. They are able to check ship hulls to identify contraband or improvised explosive devices (IEDs) and regularly scan the seabed to identify unauthorized modifications or foreign objects (Baker and Westwood, 2018). They can be used in critical maritime infrastructure protection because they are flexible.

4. Anti-Submarine Warfare (ASW)

ASW has traditionally been manned, but today, AUVs are being used as distributed unmanned listening posts. Having passive acoustic sensors will enable them to offer continuous underwater coverage, which will facilitate the detection and tracking of adversary submarines over a larger area (Murphy, 2014; Schmidt, 2020).

Advantages and Strategic Importance

The strategic capability of AUVs in maritime security is based on a number of strengths:

Stealth and Surreptitiousness: Being underwater means being concealed by nature. In contrast to surface or aerial platforms, AUVs are able to conduct missions without being noticed and thus they are perfect in covert surveillance (Murphy, 2014).

Access to High-Risk Environments: AUVs can function in areas with strong currents, confined harbor spaces, or minefields where deploying humans would be prohibitively dangerous (Rigby, 2019).

Endurance and Autonomy: Many AUVs are designed for long-duration missions, allowing them to operate with minimal human supervision, freeing manned assets for higher-priority tasks (Strode & Hendrix, 2019).

Cost-Effectiveness: Although acquisition costs can be high, operational costs are significantly lower than those of manned submarines or patrol boats. This allows for persistent presence at reduced financial burden (Baker & Westwood, 2018).

Their combination of stealth, endurance, and cost-efficiency makes them an indispensable asset for modern navies and coast guards.

COMMUNICATION AND INFORMATION SHARING PLATFORMS IN MARITIME SECURITY

The effectiveness of maritime security hinges on the ability of stakeholders to communicate and share information securely and in real-time. In a domain as vast and dynamic as the ocean, threats can emerge from any direction and at any time. A delay in information transfer or a breach in data integrity can result in catastrophic consequences. To mitigate these risks, secure communication and information-sharing networks are indispensable.

The Importance of Secure Data Networks

Traditional maritime communication systems are often vulnerable to interception and manipulation. Open radio channels can be monitored by adversaries, while unencrypted internet-based communications can be compromised. Secure data networks address these vulnerabilities by ensuring the Confidentiality, Integrity, and Availability (CIA) of information (ITU, 2018).

Confidentiality: Sensitive data, such as vessel positions or interdiction plans, must be accessible only to authorized personnel. Encryption standards such as the Advanced Encryption Standard (AES) are widely adopted for ensuring military-grade protection (NIST, 2017).

Integrity: Communication systems must prevent tampering and spoofing attacks, in which adversaries impersonate trusted entities. Cryptographic verification protocols ensure that received data remains unchanged and authentic (Hasselbach & Kessler, 2019).

Availability: Data must remain accessible during operations, including in remote areas. Robust networks mitigate risks posed by jamming or ransomware attacks, guaranteeing operational continuity (Kassab, 2021).

Levels of Communication and Information Exchange

Secure maritime communication networks enable coordination across three primary levels:

1. ***Internal Communication:*** Within a single organization (e.g., a naval command center and its fleet), secure communication ensures operational cohesion through standardized procedures (IMO, 2020).
2. ***Inter-Agency Communication:*** Maritime security involves cooperation among navies, coast guards, customs, and police forces. Secure networks enable intelligence sharing and coordinated response via multi-agency platforms such as National Maritime Information Sharing Centres (NMISCs) (Onuoha, 2013).
3. ***Regional and International Cooperation:*** Transnational threats such as piracy, arms trafficking, and smuggling demand cross-border collaboration. Secure data networks facilitate the exchange of vessel-tracking data, enabling seamless pursuit and interdiction across jurisdictions (UNODC, 2021).

Maritime Fusion Centers

Systems such as Synthetic Aperture Radar (SAR), the Automatic Identification System (AIS), Vessel Monitoring System (VMS), and coastal radar provide the "eyes and ears" of maritime security. However, the maritime fusion center acts as the brain, functioning as a command-and-control hub where diverse streams of information are collected, integrated, and analyzed into a single, comprehensive, and actionable maritime picture (Bueger, 2015; IMO, 2020). The fusion center's primary purpose is to dismantle "information silos" between agencies—navy, coast guard, customs, and police—transforming raw data into real-time intelligence for effective threat detection and coordinated response (Kraska & Wilson, 2009; UNODC, 2021).

Functions of a Maritime Fusion Center

At the heart of a fusion center is data fusion—the process of combining information from multiple sources to produce a more consistent, accurate, and useful result than any single system can provide (NATO, 2011). The workflow typically follows several stages:

1. ***Data Ingestion:*** Fusion centers act as repositories for multiple streams of maritime data, including AIS and VMS signals from thousands of cooperating vessels, high-resolution SAR imagery for detecting "dark vessels," radar and electro-optical feeds from coastal systems, and human intelligence from field operators. Open-source commercial vessel databases and maritime news reports are also incorporated to provide broader context (Bueger, 2015).

2. ***Automated Correlation:*** Specialized software matches radar tracks with AIS signals, flagging any "uncooperative" vessels lacking valid identification. This automated filtering helps reduce false alarms and highlight potential threats (NATO, 2011).
3. ***Intelligence Analysis:*** Interdisciplinary teams of analysts review fused data to identify suspicious patterns—such as loitering fishing vessels in restricted areas, unannounced stops by cargo ships, or fast boats rendezvousing with larger vessels offshore.
4. ***Threat Assessment and Prioritization:*** Analysts rank threats by severity, enabling decision-makers to allocate scarce resources efficiently—dispatching patrol assets, alerting port authorities, or coordinating joint agency responses (UNODC, 2021).

Through this structured process, fusion centers generate actionable intelligence that enables timely and effective operational coordination.

Why Fusion Centers are Indispensable

The sheer expanse of the maritime environment makes it impossible for a single agency or technology to guarantee security. This is why fusion centers are indispensable: they transform fragmented data into a unified and strategic picture (IMO, 2020). By combining predictive analytics with real-time intelligence, fusion centers not only anticipate and preempt threats before they escalate but also optimize the use of scarce resources, ensuring that costly naval and aerial assets are deployed with precision where they are most needed (Kraska & Wilson, 2009). At the same time, they enhance decision-making by providing commanders with a clear operational picture that enables faster and more accurate responses, a capability that is critical in dynamic maritime environments (Bueger, 2015). Ultimately, maritime fusion centers embody the integration of Maritime Domain Awareness (MDA) systems, intelligence networks, and operational command, transforming disparate streams of information into cohesive intelligence and creating a smarter, faster, and more efficient maritime security architecture.

CYBERSECURITY IN MARITIME DEFENSE

As maritime security systems become increasingly advanced and interconnected, they also grow more vulnerable to cyber threats. A successful cyberattack on a naval vessel, a port's control systems, or a maritime fusion center could have devastating consequences, ranging from disrupted global trade and environmental disasters to the tragic loss of life (Kessler, 2019). Cybersecurity is therefore no longer an optional add-on but an indispensable component of modern maritime defense.

Nature of Maritime Cyber Threats

The maritime industry, with its complex integration of operational technology (OT) and information technology (IT), faces a wide range of cyber risks. Malware and ransomware can infiltrate navigation or cargo handling systems, causing operational paralysis or extorting critical data for ransom (Tam & Jones, 2019). Distributed Denial of Service (DDoS) attacks

may flood networks, temporarily blinding coastal defense systems by disabling radars (CyberKeel, 2014). Data breaches further expose sensitive information such as vessel movement schedules or classified intelligence (ENISA, 2019).

Particularly concerning are spoofing and signal manipulation attacks, in which adversaries corrupt AIS or GPS signals to misdirect vessels or create false traffic, potentially causing collisions and large-scale maritime disruption (Balduzzi et al., 2014; Kessler, 2019). These threats highlight the urgent need for a proactive and multi-layered cybersecurity framework.

Mitigation Strategies: A Multi-Layered Approach.

Protecting maritime digital infrastructure requires a comprehensive strategy addressing networks, hardware, and human factors.

Network and Data Security

Protecting sensitive maritime data requires a multi-layered approach to cybersecurity. Encryption ensures that information transmitted via satellite or terrestrial links remains secure, safeguarding it from interception and unauthorized use (ENISA, 2019). Complementing this, firewalls and Intrusion Detection Systems (IDS) serve as digital gatekeepers, providing real-time monitoring, filtering malicious traffic, and quickly identifying intrusions. In addition, secure remote access is vital; connectivity to vessels or port systems must be tightly controlled through measures such as multi-factor authentication and secure VPN protocols to minimize the risk of unauthorized entry (IMO, 2021).

System and Hardware Security

Ensuring the resilience of maritime security systems also depends on strong system and hardware protections. Regular software updates are essential, as frequent patching of navigation, communication, and data fusion platforms helps close known vulnerabilities and reduces exposure to cyber threats (Tam & Jones, 2019). Equally important is physical security: servers, radar installations, and communication nodes must be housed in controlled facilities to prevent tampering or unauthorized access (ENISA, 2019). In addition, system hardening—such as disabling unnecessary services and ports—further minimizes exploitable entry points, thereby reducing the overall attack surface of critical maritime infrastructure (Kessler, 2019).

Human and Organizational Measures

Human and organizational measures are equally vital in strengthening maritime cybersecurity. Regular training and awareness programs equip personnel to recognize phishing attempts, social engineering tactics, and insider threats, addressing the reality that human error remains the most common entry point for cyber intrusions (IMO, 2021). Effective access control further reinforces security by applying the principle of least privilege, ensuring that staff only interact with the data or systems necessary for their roles (ENISA, 2019). In addition, well-structured incident response planning—complete with predefined recovery protocols such as

system isolation, forensic analysis, and stakeholder communication—enables organizations to respond swiftly to cyberattacks and restore operations with minimal disruption (Kessler, 2019).

The Role of Enterprise Resource Planning (ERP) in Naval Fleet Readiness

A fleet's ability to respond to threats such as piracy, trafficking, and smuggling is inseparable from its operational readiness. ERP platforms consolidate real-time data on the status, availability, and location of assets, ranging from ships and aircraft to specialized equipment (Kapp et al., 2018). An ERP system for a naval fleet is an integrated digital platform that manages financial processes, supply chain logistics, maintenance, and human resources. By ensuring the operational efficiency of the fleet itself, ERP systems indirectly—but fundamentally—enhance a nation's ability to combat maritime insecurity. Commanders gain an instant, holistic view of resources, enabling smarter allocation, faster deployments, and more effective mission planning.

Predictive Maintenance (PM)

ERP systems are critical in predictive maintenance since they combine information of onboard sensors, which monitor the engines, navigation systems, and important machinery. Predictive analytics can be used to predict the time when a component may malfunction, and preventive maintenance is performed before a failure takes place (Alrabghi and Tiwari, 2016; Lee et al., 2014; Ali, 2025). This saves unnecessary expensive downtime which is not planned and guarantees maximum fleet preparedness.

Supply Chain Optimization

Prolonged maritime security activities will require uninterrupted supply of fuel, ammunition, spare parts and supplies. ERP systems automate this supply chain by monitoring the materials between procurement and delivery and avoiding the lack of mission-critical resources (Jonsson and Holmstrom, 2016). Automated ordering eliminates administrative bottlenecks, as well as provides transparency and efficiency (Beheshti et al., 2014).

Financial Accountability and Resource Efficiency

Due to the large expenditures of naval actions, financial discipline is essential. ERP systems enable a single and auditable history of all financial operations and enhance accountability and minimise fraud (Kumar et al., 2019). They also enable commanders to monitor the operational spending, including fuel usage and maintenance expenses, and to make the proper budgets (Ali, 2025). This financial transparency assists the leaders to put resources in the right context without compromising on security abilities (Madapusi & D'Souza, 2012).

Human Capital and Training Management

Staff preparation is equal to equipment preparation. ERP systems facilitate the assignment of

the crew, certifications and training records so that they are manned by competent employees (Taroun and Yang, 2011). They also plan and monitor training initiatives and allow continuous development of skills and adjustment to new technologies or threats. By integrating human capital management into the broader operational picture, ERP systems strengthen the effectiveness of naval forces.

CONCLUSION AND RECOMMENDATIONS

The pivotal role of technology in ensuring optimal security and efficient naval operations in Nigeria's maritime domain is undeniable. From advanced MDA systems that provide real-time situational awareness to modern naval platforms and AI-driven predictive maintenance, technology offers transformative solutions to combat persistent threats and enhance operational readiness.

While commendable progress has been made, particularly through initiatives like the Deep Blue Project, sustaining and expanding these gains requires a strategic, multi-faceted, and long-term commitment.

Recommendations

To further strengthen Nigeria’s maritime security through technology, several strategic actions are essential. First, there must be sustained and increased investment, with consistent funding dedicated to the procurement, upgrading, and maintenance of advanced maritime security technologies. Alongside this, robust human capacity development is critical; specialized training in technology operation, maintenance, data analytics, and cybersecurity will equip naval personnel and other maritime security agencies with the skills required to maximize these tools. Equally important is the strengthening of inter-agency and regional cooperation by leveraging technology to build interoperable information-sharing platforms, thereby fostering seamless collaboration with neighboring states and international partners, particularly under frameworks such as the Yaoundé Code of Conduct.

At the same time, a resilient cybersecurity framework must be developed to safeguard critical maritime infrastructure and digital networks against evolving threats. However, technology alone cannot provide lasting solutions; it must be complemented by efforts to address the root socio-economic drivers of maritime criminality, such as poverty and unemployment. Finally, fostering local innovation and research in maritime technology will reduce dependence on foreign solutions, enhance self-reliance, and build indigenous expertise. Together, these measures offer Nigeria a comprehensive pathway to enhancing its maritime security architecture through the strategic integration of technology.

By strategically integrating and effectively deploying these technological solutions, coupled with strong governance and human capacity, Nigeria can solidify its control over its maritime domain, protect its vital economic interests, enhance regional stability, and truly realize its potential as the 'Giant of Africa' on the global maritime stage.

REFERENCES

Adebayo, A. A., & Ojo, T. (2020). Maritime security in the Gulf of Guinea: Issues and prospects. African Security Review, 29(3), 237–252. https://doi.org/10.1080/10246029.2020.1778702

Agnew, D. J., Pearce, J., Pramod, G., Peatman, T., Watson, R., Beddington, J. R., & Pitcher, T. J. (2009). Estimating the worldwide extent of illegal fishing. PLoS ONE, 4(2), e4570. https://doi.org/10.1371/journal.pone.0004570

Akinwale, A. (2021). Nigeria's Suppression of Piracy and Other Maritime Offences (SPOMO) Act: Potentials and limitations. Journal of African Maritime Studies, 13(2), 55–70.

Akinyemi, A. (2019). The dynamics of smuggling in Nigeria's border communities. African Security Review, 28(3), 272–289.

Ali, B.O. (2025) Revamping Shipbuilding Capabilities in the United States: A Catalyst to Make America Great Again. Journal of Transportation Technologies, 15, 413-436. https://doi.org/10.4236/jtts.2025.153018

Al Jazeera. (2021, February 12). Turkish sailors freed after weeks in pirate captivity. https://www.aljazeera.com/news/2021/2/12/turkish-sailors-freed-off-nigeria-after-weeks-in-pirate-captivity

Alrabghi, A., & Tiwari, A. (2016). State of the art in simulation-based optimisation for maintenance systems. Computers & Industrial Engineering, 82, 167–182. https://doi.org/10.1016/j.cie.2015.11.010

Asuni, J. (2009). Blood oil in the Niger Delta. United States Institute of Peace.

Balduzzi, M., Pasta, A., & Wilhoit, K. (2014). A security evaluation of AIS automated identification system. Proceedings of the ACM Conference on Computer and Communications Security, 8(1), 436–447.

Baker, S., & Westwood, R. (2018). Autonomous underwater vehicles in port and harbor security. Journal of Marine Engineering and Technology, 17(2), 91–103.

Beheshti, H. M., Blaylock, B. K., Henderson, D. A., & Lollar, J. G. (2014). ERP systems benefits: Perceived and real. Business Process Management Journal, 20(3), 376–398. https://doi.org/10.1108/BPMJ-01-2013-0006

Bellingham, J. G., & Rajan, K. (2007). Robotics in remote and hostile environments. Science, 318(5853), 1098–1102.

Berkovic, A., Subasic, M., & Baric, M. (2019). Modern coastal radar systems in vessel traffic service. Pomorstvo, 33(1), 1–8. https://doi.org/10.31217/p.33.1.1

Big-Alabo, A., & Ezugwu, C. (2022). The concept of national security: A dynamic approach. Journal of Security Studies and Global Politics, 7(1), 44–59.

Bourbon Offshore. (2012, November 1). Liberation of crew members abducted in Nigeria. https://www.bourbonoffshore.com

Bowers, I., & Koh, C. H. (Eds.). (2017). Maritime Security in the Indo-Pacific: Perspectives from China, India, and the United States. Routledge.

Boraz, S. C. (2009). Maritime domain awareness and the challenge of integration. Naval War College Review, 62(3), 13–38.

Brume-Eruagbere, J. (2017). Maritime law enforcement in Nigeria: Challenges of combating piracy and armed robbery at sea. Journal of African Maritime Studies, 5(2), 45–63.

Bueger, C. (2015). Learning from piracy: Future challenges of maritime security governance.

Chijioke, C. (2020). Maritime insecurity and its implications for Nigeria's economic development. African Security Review, 29(1), 78–93.

Chandra, S., & Jain, S. (2019). Electro-optical and infrared sensors for coastal surveillance. Defence Science Journal, 69(3), 256–263.

Chaturvedi, S. K., Kumar, S., & Thomas, R. (2021). Synthetic aperture radar applications in monitoring fishing activity: Emerging trends. Marine Policy, 129, 104512. https://doi.org/10.1016/j.marpol.2021.104512

Clapperton, R. (2018). Maritime surveillance using UAV-based synthetic aperture radar. Defence Studies, 18(3), 245–262.

Cunliffe, B. W. (2017). On the Ocean: The Mediterranean and the Atlantic from Prehistory to AD 1500. Oxford University Press.

Cunningham, F., & Roberts, J. (2020). Drones and the future of maritime domain awareness. Maritime Affairs: Journal of the National Maritime Foundation of India, 16(2), 112–130.

CyberKeel. (2014). Maritime cyber-risks: An increasing threat to global shipping. CyberKeel Report.

Doorey, T. (2014). Maritime domain awareness: Key to protecting the maritime domain. Naval Forces Quarterly, 35(4), 52–59.

European Union Agency for Cybersecurity (ENISA). (2019). Port cybersecurity: Good practices for cybersecurity in the maritime sector. ENISA. https://www.enisa.europa.eu/publications/port-cybersecurity

Ewetan, O. O., & Ese, U. E. (2014). Insecurity and socio-economic development in Nigeria: Journalistic perspectives. Journal of Sustainable Development Studies, 5(1), 40–63.

FAO. (2007). Vessel monitoring systems (VMS): A practical handbook for fisheries monitoring, control and surveillance. Rome: Food and Agriculture Organization of the United Nations.

FAO. (2018). The state of world fisheries and aquaculture 2018: Meeting the sustainable development goals. Rome: FAO.

Ferraro, G., Bernardini, A., David, M., Meyer-Roux, S., Muellenhoff, O., Perkovic, M., ... & Tarchi, D. (2017). Applications of synthetic aperture radar (SAR) in maritime surveillance. European Journal of Remote Sensing, 50(1), 343–361.

Food and Agriculture Organization (FAO). (2018). The state of world fisheries and aquaculture. FAO.

Fuller, W. C. (1989). Strategy and Power in Russia 1600–1914. The Free Press.

Gilpin, R. (2009). Enhancing maritime security in the Gulf of Guinea. Africa Center for Strategic Studies.

Greidanus, H., & Alvarez, M. (2021). Detecting non-cooperative vessels in satellite synthetic aperture radar imagery. Remote Sensing, 13(8), 1452. https://doi.org/10.3390/rs13081452

Handbook of Engineering and Technology in the Classical World (pp. 90–130). Oxford University Press.

Hasselbach, L., & Kessler, O. (2019). Maritime cybersecurity: Securing the digital maritime environment. Journal of Transportation Security, 12(1), 1–17.

Hastings, J. V. (2009). Geographies of state failure and sophistication in maritime piracy hijackings. Political Geography, 28(4), 213–223. https://doi.org/10.1016/j.polgeo.2009.05.004

Ikelegbe, A. (2013). Oil, resource conflicts and the post-conflict transition in the Niger Delta region: Beyond the amnesty. GeoJournal, 78(3), 459–473.

International Maritime Organization (IMO). (2021). Maritime cyber risk management in safety management systems (MSC-FAL.1/Circ.3/Rev.1). IMO.

International Maritime Organization (IMO). (2016). GMDSS: The global maritime distress and safety system. IMO Publications.

International Maritime Organization (IMO). (2020). Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3). IMO.

International Telecommunication Union (ITU). (2018). Maritime communications handbook. Geneva: ITU.

IALA. (2016). IALA guideline 1082 on the automatic identification system (AIS). Saint Germain-en-Laye: International Association of Marine Aids to Navigation and Lighthouse Authorities.

International Maritime Bureau (IMB). (2013). Piracy and armed robbery against ships: Annual report 2012. ICC International Maritime Bureau.

International Maritime Bureau. (2021). Piracy and armed robbery against ships: Annual report 2020. ICC International Maritime Bureau.

Jonsson, K., & Holmström, J. (2016). Future of supply chain planning: Closing the gaps between practice and promise. International Journal of Physical Distribution & Logistics Management, 46(1), 62–81. https://doi.org/10.1108/IJPDLM-05-2014-0134

Jowitt, C. (2001). The culture of piracy, 1580–1630: Literature and seaborne crime. Ashgate. (used here as a reliable substitute for the cited Jowitt work on early modern voyages and navigation)

Kapp, C. A., Hall, T., & Anderson, T. (2018). Enterprise resource planning in defense logistics. Journal of Defense Analytics and Logistics, 2(1), 1–15. https://doi.org/10.1108/JDAL-07-2017-0016

Kanjir, U., Greidanus, H., & Oštir, K. (2018). Vessel detection and classification from spaceborne optical images: A literature survey. Remote Sensing of Environment, 207, 1–26.

Karjalainen, M., Virtanen, K., & Ruponen, P. (2021). UAVs in maritime search and rescue operations: Potentials and challenges. Journal of Navigation, 74(5), 1054–1072.

Kassab, M. (2021). Cybersecurity in maritime transport systems: Vulnerabilities and mitigation. Maritime Policy & Management, 48(4), 541–556.

Kersten, P. R., Skrunes, S., & Brekke, C. (2016). Small boat detection in coastal SAR imagery. Remote Sensing, 8(7), 567.

Kessler, G. C. (2019). Maritime cybersecurity. Springer. https://doi.org/10.1007/978-3-030-17274-3

Kourti, N., Shepherd, I., Schwartz, G., Pavlakis, P., & Keramitsoglou, I. (2005). Integrating spaceborne SAR imagery into operational systems for fisheries monitoring. ESA Bulletin-European Space Agency, 122, 26–33.

Kraska, J., & Wilson, B. (2009). Combating pirates of the Gulf of Aden: The Djibouti Code and the Somali Coast Guard. Ocean Development & International Law, 40(3), 207–232. https://doi.org/10.1080/00908320903076839

Kumar, A., Singh, R. K., & Shankar, R. (2019). Critical success factors for implementation of supply chain management in Indian SMEs and their impact on performance. IIMB Management Review, 31(3), 210–222. https://doi.org/10.1016/j.iimb.2019.03.002

Lambert, A. (2010). Battleships in Transition: The Creation of the Steam Battlefleet, 1815–1860. Conway Maritime Press.

Lee, J., Bagheri, B., & Kao, H. A. (2014). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manufacturing Letters, 3, 18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Manley, J. E. (2016). Unmanned surface vehicles, 15 years of development. Proceedings of MTS/IEEE OCEANS Conference.

Manley, J. E. (2008). Unmanned surface and underwater vehicles for mine countermeasures. Proceedings of the MTS/IEEE OCEANS Conference.

Madapusi, A., & D'Souza, D. (2012). The influence of ERP system implementation on the operational performance of an organization. International Journal of Information Management, 32(1), 24–34. https://doi.org/10.1016/j.ijinfomgt.2011.06.004

Mclaren, D., & Jakobi, T. (2017). The role of unmanned systems in maritime interdiction operations. Naval War College Review, 70(4), 55–72.

Millefiori, L. M., Braca, P., Bryan, K., & Willett, P. (2016). Multisensor data fusion for maritime surveillance. IEEE Transactions on Aerospace and Electronic Systems, 52(4), 1807–1825.

Moreira, A., Prats-Iraola, P., Younis, M., Krieger, G., Hajnsek, I., & Papathanassiou, K. P. (2013). A tutorial on synthetic aperture radar. IEEE Geoscience and Remote Sensing Magazine, 1(1), 6–43.

Murphy, M. (2010). Small boats, weak states, dirty money: Piracy and maritime terrorism in the modern world. Columbia University Press.

Murphy, R. R. (2014). Disaster robotics: Applications of unmanned systems in dangerous environments. MIT Press.

Murphy, M. N. (2021). Cyber threats to the maritime domain. Maritime Policy & Management, 48(5), 567–586. https://doi.org/10.1080/03088839.2020.1834464

Murphy, M. N. (2021). Small boats, weak states, dirty money: Piracy and maritime terrorism in the modern world. Columbia University Press.

National Institute of Standards and Technology (NIST). (2017). Advanced Encryption Standard (AES) (FIPS PUB 197). Gaithersburg, MD: U.S. Department of Commerce.

Natale, F., Carvalho, N., & Paulrud, A. (2015). Defining small-scale fisheries in the EU on the basis of their operational range of activity: The Swedish fleet as a case study. Fisheries Research, 164, 286–292.Nigerian Navy. (2023). Nigerian Navy annual report 2022/2023. Abuja: Nigerian Navy.

NAPTIP. (2021). Annual report on combating human trafficking in Nigeria. Abuja: Government of Nigeria.

North Atlantic Treaty Organization (NATO). (2011). Maritime security: NATO's role in energy security and critical infrastructure protection. NATO Parliamentary Assembly.

Obembe, E., & Ali, B. (2025). Evaluating the Applications and the Growing Importance of Autonomous Underwater Vehicles (AUVs) in Marine Geophysical Survey. Journal of Science Innovation and Technology Research, 7(9). https://doi.org/10.70382/ajsitr.v7i9.032

Obi, C. (2010). Oil extraction, dispossession, resistance, and conflict in Nigeria's oil-rich Niger Delta. Canadian Journal of Development Studies, 30(1–2), 219–236.

Oleson, J. P. (2008). Greek and Roman mechanical engineering. In J. P. Oleson (Ed.), The Oxford Turner, G. L'E. (1980). Instruments of Navigation. Science Museum.

Okafor-Yarwood, I. (2020). Illegal, unreported and unregulated fishing, and the complex relationship to maritime security in the Gulf of Guinea. African Security, 13(2), 116–146.

O'Hanlon, M. E. (2020). Forecasting change in military technology, 2020–2040. Brookings Institution Press.

Okafor-Yarwood, I. (2020). The cyclical nature of maritime security threats: Illegal, unreported and unregulated fishing as a threat to human and national security in the Gulf of Guinea. African Security Review, 29(2), 163–185. https://doi.org/10.1080/10246029.2020.1761643

Onuoha, F. (2012). Piracy and maritime security in the Gulf of Guinea: Nigeria as a microcosm. Al Jazeera Centre for Studies Report.

Onuoha, F. (2013). Piracy and maritime security in the Gulf of Guinea: Trends, concerns, and policy responses. Nigerian Journal of International Affairs, 39(1), 85–111.

Onuoha, F. (2018). Oil theft and insecurity in Nigeria's Niger Delta: Implications for national security and regional stability. African Security Review, 27(2), 135–150. https://doi.org/10.1080/10246029.2018.1495305

Otto, G. (2016). Maritime insecurity in the Niger Delta: Implications for Nigeria's national security. Nigerian Journal of International Affairs, 42(3), 112–130.

Park, J., Park, Y., & Kim, D. (2020). Automatic identification system (AIS) and SAR image fusion for vessel monitoring. Journal of Navigation, 73(4), 811–826.

Pranav, P. (2016). Crime and spatial attributes: Understanding the dynamics of maritime insecurity. Journal of Criminology and Justice Studies, 8(1), 55–70.

Ray, A., & Ghosh, S. (2015). Radar-based coastal surveillance for maritime safety and security. Journal of Ocean Engineering and Science, 1(2), 150–158.

Rigby, C. (2019). Mine countermeasure operations using autonomous underwater vehicles. Naval Forces, 40(3), 45–52.

Schmidt, H. (2020). Advances in autonomous systems for undersea surveillance. Annual Review of Control, Robotics, and Autonomous Systems, 3, 133–155.

Strode, C., & Hendrix, K. (2019). Persistent underwater surveillance using autonomous systems. Marine Technology Society Journal, 53(1), 56–67.

Schmidt, H., Petillot, Y., & Ferreira, F. (2020). Advances in autonomy for unmanned surface vehicles. Annual Review of Control, Robotics, and Autonomous Systems, 3, 111–137.

Tam, K., & Jones, K. (2019). Cyber-risk assessment for autonomous ships. Reliability Engineering & System Safety, 195, 106805. https://doi.org/10.1016/j.ress.2019.106805

Taroun, A., & Yang, J. B. (2011). Dempster–Shafer theory of evidence: Potential usage for decision making and risk analysis in construction project management. The Built & Human Environment Review, 4(1), 155–166.

Thomas, J. (2021). Maritime situational awareness and global security. Journal of Maritime Security and Safety, 13(2), 23–39.

Tournadre, J. (2014). Anthropogenic pressure on the open ocean: The growth of ship traffic revealed by altimeter data analysis. Geophysical Research Letters, 41(22), 7924–7932.

Tunaley, J. K., Vachon, P. W., & Campbell, J. W. (2016). The role of synthetic aperture radar in monitoring maritime activity. Canadian Journal of Remote Sensing, 42(1), 1–13.

United Nations Office on Drugs and Crime. (2022). Maritime crime and the rule of law: Gulf of Guinea update. UNODC.

UK Foreign, Commonwealth & Development Office. (2023). Foreign travel advice: Nigeria. https://www.gov.uk/foreign-travel-advice/nigeria

Ukoji, V., & Okolie, A. (2016). Networks of crime: Maritime insecurity and organized groups in Nigeria. African Journal of Criminology, 10(2), 101–119.

United States Department of Defense. (2013). National strategy for maritime security: Maritime domain awareness. Washington, DC: U.S. Government.

United Nations Office on Drugs and Crime (UNODC). (2021). Transnational organized crime in the fishing industry: Focus on West Africa. UNODC. Global Affairs, 1(1), 33–42. https://doi.org/10.1080/23340460.2015.960186

United Nations Office on Drugs and Crime (UNODC). (2021). Maritime crime and piracy in the Gulf of Guinea. UNODC.

United Nations Security Council. (2011). Resolution 2018 (S/RES/2018). United Nations.

United Nations Security Council. (2012). Resolution 2039 (S/RES/2039). United Nations.

United Nations Security Council. (2022). Resolution 2634 (S/RES/2634). United Nations.

Wright, P. (2021). The economics of unmanned systems in maritime security. Marine Policy, 131, 104608.

Yaoundé Code of Conduct. (2013). Code of conduct concerning the repression of piracy, armed robbery against ships, and illicit maritime activity in West and Central Africa.