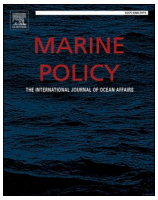
Marine Policy 160 (2024) 105976

Contents lists available at ScienceDirect

Marine Policy

journal homepage: www.elsevier.com/locate/marpol



Technology and maritime security in Africa: Opportunities and challenges in Gulf of Guinea

Ifesinachi Okafor-Yarwood [a,*], Oliver Eastwood [a,b], Noleen Chikowore [a], Lucas de Oliveira Paes [c]

[a] The School of Geography and Sustainable Development, The University of St. Andrews, St Andrews, UK
[b] School of International Relations, The University of St. Andrews, St Andrews, UK
[c] Norwegian Institute of International Affairs, Norway

ARTICLE INFO

Keywords:
Africa
Cyber Security
Gulf of Guinea
Maritime Domain Awareness, Maritime Security, Technology

ABSTRACT

Maritime security threats undermine safety and security at sea and, in turn, coastal states' efforts to harness the resources in their maritime domain. This assertion is true for coastal states and Small Island Developing States (SIDS) on the African continent, where limited maritime enforcement capabilities have increased security threats at sea, such as illegal, unreported and unregulated fishing, piracy and armed robbery at sea, toxic waste dumping and other illicit activities. African navies and their foreign partners are taking advantage of the opportunities that technology provides to improve safety and security. Technology has led to the identification of criminals at sea, their capture and prosecution, making it crucial in enhancing maritime security. As such, the merits of its use for maritime security are undeniable. However, using technology comes with challenges that need to be considered. With this in mind, our research makes an original contribution by exploring the opportunities for using technology to advance maritime safety and security in Africa, successes and challenges with an emphasis on the Gulf of Guinea region. Drawing from questionnaire data from maritime law enforcement personnel, agencies supporting the implementation of the Yaoundé Code of Conduct (2013), and a review of relevant literature and policy documents, we contend that technology has significantly improved maritime domain awareness and the effective implementation of maritime safety and security in the Gulf of Guinea. However, addressing existing limitations and enhancing human capacity is imperative to sustain this progress.

1. Introduction

As the world increasingly relies on the oceans for food, energy, employment, and environmental solutions, maritime security is becoming an important discussion topic among policymakers, policy implementers, and researchers. This is because the maritime space is under increasing threats, resulting from the overexploitation of fish stocks through both legal fishing and illegal, unreported and unregulated (IUU) fishing, piracy and armed robbery at sea, illegal oil bunkering, toxic waste dumping, drugs and human trafficking, and other illegal activities. Indeed, there has been a steep increase in global maritime insecurity since the end of the Cold War, which saw a decrease in naval sizes and has impacted state enforcement capacity. At the same time, surplus weapons, technology and vessels were acquired by organised criminal networks – such as pirates and terrorists [54].

While the last decades witnessed the rise of transnational public-private initiatives to enhance maritime security and had some success mitigating security risks to economic activities on the high seas [64], many threats are highly persistent in their effects on coastal states and communities, particularly on the African continent. The Gulf of Guinea (GoG) has become one of the global hotspots of maritime insecurity due to prevalent IUU fishing, piracy, armed robbery, oil theft and illegal oil bunkering. The reasons for that include a limited capacity for regional states to monitor and control activities at sea, as many countries cannot devote necessary resources to address maritime insecurity.

The colonial roots of maritime insecurity are also worth noting, as conflict over maritime borders is a major factor undermining maritime law enforcement cooperation and collaboration. The European partition of Africa, in particular, created numerous border conflicts, weakening state capacity and making maritime jurisdictions unclear. Following the end of colonialism, states worked to avoid secessionism and civil wars, which affected their investment in their navies. These, along with regional institutions with limited capacity and debt-ridden economies, place colonialism at the root of African nations' limited maritime

* Corresponding author.
E-mail address: imoy1@st-andrews.ac.uk (I. Okafor-Yarwood).

https://doi.org/10.1016/j.marpol.2023.105976
Received 20 July 2023; Received in revised form 11 November 2023; Accepted 3 December 2023
Available online 20 December 2023

capabilities [46].

Though traditional narratives define maritime security in terms of the presence or absence of actual threats, academic engagement in this area often fails to adequately consider maritime domain awareness (MDA). As Boraz [4] argues, a key misinterpretation that has caused this literary and policy gap is the myth that navies and security agencies have always 'done' MDA. While the need for situational awareness has always been recognised and pursued in the maritime sector, MDA as a cohesive approach is a relatively recent concept that has emerged in response to the rapid growth in security threats, data sources and maritime networks. Though technologies such as RADAR and Automatic Identification System (AIS) are long-established, the limits to their capacity have driven the development of MDA. As [40] writes, "what surveillance systems cannot do is to put the data they generate into context. They cannot, in other words, reveal purpose or intention." This is perhaps the most significant role of MDA: contextualisation of data, which allows maritime security actors to take informed actions to tackle threats at sea.

In discussing the centrality of MDA to maritime security in the GoG, Gilpin [29] argues that the prevailing "land-centric" security approach, where national law enforcement agencies primarily focus on land-based threats, contributes to the lack of MDA in the region and by extension, the increased insecurity at sea. Consequently, combating maritime insecurity in the GoG has involved addressing the limited (asymmetric) capabilities of regional countries through collective capacity building. This effort is centred around improving MDA tools and is fostered by international cooperation and collaboration. Considering the multi-layered responsibilities of the maritime security sector [43], write that while strong governance and enforcement capacity is necessary for securing maritime areas, "first and foremost though, we [the international maritime community] must understand the maritime domain and what is going on within it, so that we can formulate good policy, effectively deploy assets and ensure the uninterrupted flow of commerce." With this assertion, the authors establish MDA as not just a central component of maritime security but as a mandatory precondition to all other aspects of maritime security. It is through this lens that we seek to establish our own understanding of maritime security, wherein the extent and success of maritime security is defined by the attainment of MDA. As Doorey [21] suggests, the key to protecting a country's maritime domain is a timely and comprehensive understanding of all maritime activity in its inland waterways, territorial seas, Exclusive Economic Zone (EEZ), and high seas. Thomas [66] takes this further, arguing that maritime situational awareness is a critical component of maritime security; we adopt this to form our understanding of maritime security and inform our exploration of MDA-enhancing technologies that, under this new definition, are essential to securing maritime environments.

In the GoG, technology has proved to be a promising path to enhance regional capacity to address security threats at sea. This involves using technologies to boost MDA, facilitating improved information gathering, communication, and interventions and fostering smoother cooperation among various security actors within and across nations. The Yaoundé Architecture, established by the Yaoundé Code of Conduct 2013, is at the core of these efforts. The Yaoundé Code of Conduct is an international framework encompassing norms, conventions, and organizations and the Architecture serves as a platform for regional and international collaboration in maritime security, incorporating multi-level capacity building, information-sharing mechanisms, and operational cooperation ([45], pp. 75–86). The international community has rallied behind the GoG states to address security threats, as evident in the United Nations Security Council (UNSC) Resolutions 2018 (2011), 2039 (2012), and 2634 (2022). While these resolutions primarily emphasised piracy and armed robbery at sea, they urged GoG states to collaborate in countering security threats in their region [23]. This shift has established a regional imperative for MDA and actions against maritime insecurity, moving the region's focus from receiving security assistance to enhancing regional capacity through collaborations with coastal states.

To understand the extent to which regional agencies in the GoG are deploying technology for MDA and information sharing to enhance maritime security, we ask, what are the opportunities and challenges associated with using technologies for maritime security in the GoG? Our research advances our understanding of the subject area by being the first to present empirical evidence on the opportunities, successes, and challenges of using technology for maritime security on the African continent based on the realities of the GoG countries. In addition, as 2023 marks the 10th anniversary of the signing of the Yaoundé Code of Conduct, our research contributes to the literature by assessing how technology has helped the region achieve some of the agreement's key objectives, which include improving regional safety and security through enhanced information sharing. Using primary data from questionnaires distributed to key strategic and operational organisations focused on maritime safety and security in the GoG, and the review of literature and policy documents, we argue that technology has improved MDA and information sharing and, resultantly, maritime security in the GoG. However, the use of maritime technology must be complemented with necessary human resources and relevant assets (e.g., surface and air) for a sustainable outcome. Although technologies for maritime security more broadly would include those deployed for port monitoring and security, container control, digitisation of vessel navigation systems, MDA and information sharing, we limit our analysis to technologies deployed mainly for information gathering and sharing by the navies and coast guards.

To explore the opportunities, successes, and challenges associated with the use of technologies for maritime security, our paper is structured as follows. The introductory section is succeeded by a literature review that underscores the role of MDA technologies in enhancing maritime security. Following this, we detail the research methodology. Subsequent sections include the presentation of findings, commencing with the successful implementation of technology, and then moving on to the challenges faced and the corresponding solutions. Our paper concludes with a section dedicated to implications and overall conclusions.

2. From sea blindness to sea vision: maritime domain awareness as central to maritime security

Territorial states have long sought to extend their governing capacity and control over the sea [55], and yet oceans remain an elusive space for many coastal states due to limited capacity resulting from lack of access to infrastructure, technology and technical know-how. The vast nature of the marine environment raises the costs for states to monitor activities at sea. This ultimately translates into a security issue, impairing states' capacity to identify threats and sanction misbehaviour. Nevertheless, the centrality of maritime activities for the world economy has pushed states, international organisations, and private actors to establish joint efforts to try and render the sea governable [10]. Central to these efforts are initiatives that leverage technology to amplify the capabilities of states and other pertinent stakeholders in rendering the maritime domain more visible. The evolution of MDA is intrinsically linked to the rise of technologies promising to enhance states' surveillance capabilities. The progress in information technology has facilitated the creation of more efficient platforms for collecting, integrating, analysing, and sharing such data. This, in turn, has enabled the translation of MDA into a heightened maritime situational awareness, generating a comprehensive database of information, often in real-time. This information serves as a foundation for planning and targeting various maritime security operations, including but not limited to vessel interceptions and inspections at sea [10].

The initial development of MDA was limited by the capacities of available technologies, which historically have been RADAR and satellite imagery. Both have differing advantages and limitations: land-based RADAR is relatively low-cost (both in terms of installation and

operation) and can operate in all weather conditions but has a small sensor area. Space-based satellite imagery covers a large area but is expensive to install and operate while not providing persistent monitoring [36,50]. A key limitation of these technologies is their precision – the limited sensor resolution of RADAR makes it difficult to determine whether a detected object is a ship, while the pixel resolution required for wide-area satellite imaging is often unable to detect small vessels [28,57]. Even when a ship is detected, it is nearly impossible to ascertain its identity through RADAR or satellite imagery alone; additionally, these technologies cannot identify vessel activity, meaning illegal activity cannot be tracked [61]. While RADAR and satellite imaging have provided a useful starting point for enhancing MDA, their numerous disadvantages, combined with rapid growth in global maritime activity, have meant that maritime security stakeholders can no longer reliably use them without complementary data from other technologies.

Automatic Identification System (AIS) and Vessel Monitoring System (VMS) data, if properly utilised, is highly valuable for maritime stakeholders, from maritime security enforcement authorities such as navies and coastguards to fisheries regulators. Though originally developed as a tool to enhance vessel safety and collision avoidance through Vessel Traffic Services (VTS), the benefits that AIS vessel tracking would provide to MDA were quickly recognised [65]. In contrast to RADAR or satellite systems, which provide information either infrequently or on request, AIS transmits vessel identification data several times per minute, allowing for real-time tracking of vessels [13,47]. Additionally, as opposed to previous reliance on VTS and RADAR, AIS is not restricted to port areas; instead, it utilises a combination of satellite and terrestrial systems for data transmission, thus creating a global monitoring system [1,47]. The significance of this final point cannot be overstated, as previous monitoring systems were either terrestrial and thus could not capture shipping activity outside near-coast zones or space-based, which had a wider range but low frequency of data capture [51]. AIS combines the two systems to establish extensive coverage and a standardised and cheap means of tracking vessel activity. In contrast to the relatively incidental application of AIS to MDA, VMS was developed specifically for vessel tracking in the shipping and fisheries industry, making it, by some accounts, a more accurate and reliable monitoring system [59]. Though it transmits data at a much lower rate than AIS and in one direction (i.e. ship to shore), VMS systems are typically closed and privately operated, and opposed to the public nature of AIS – this makes them a more secure, albeit costly, option for improving vessel monitoring and security at sea [19,34].

A major challenge posed by the growing reliance on VMS and AIS is vessels "going dark", whereby communications and data reporting are switched off, allowing illegal activity to be obscured. In a recent meta-analysis, Welch et al. [74] showed that, between 2017 and 2019, up to 6% of global fishing vessel activity was obscured by AIS disabling, roughly equating to 4.9 million hours of fishing activity. Though switching off AIS is in contravention of the International Convention for the Safety of Life at Sea (SOLAS), captains argue that doing so hides their position from pirates; however, even for legitimate vessels, this poses a risk as it limits their ability to avoid collisions in congested areas [31]. Some vessels may go to even further lengths to obscure their activity, such as exploiting the poor cybersecurity of AIS reporting systems to introduce false signals to the system [2]. Additionally, though the installation of AIS is mandatory on large ships under International Maritime Organisation (IMO) regulations, there is no requirement for the system to be present on small commercial vessels, while the use of VMS is legislated on a national basis [76,20,52]. As a result, there are significant gaps in AIS and VMS reporting and data transmission, in addition to vessels going dark, mandating additional monitoring technologies to close these gaps.

Recent technological innovations are helping close these gaps, most notably Synthetic Aperture RADAR (SAR) and Vessel Infrared Imaging Radiometer Suite (VIIRS). SAR is, in essence, a more advanced version of traditional RADAR that can observe areas in any weather conditions and at any point in the day; additionally, the imaging and data it produces are of a significantly higher resolution compared to traditional RADAR, allowing for vessel activity and position to be recorded [36,56]. The proliferation of data processing algorithms means that vessels can be tracked and illegal activity identified much faster and with greater efficiency [18,60]. A further extension of this technology is in identifying trends in "dark zones". SAR can be used to identify areas in which ships frequently disable their tracking systems, which allows maritime security authorities to identify zones of high importance for tackling illegal activity at sea [53]. However, SAR still presents maritime security enforcement actors with the issues typically associated with satellite-based imaging, namely that it is a highly expensive system and can only observe a specific area every few days due to satellite orbit patterns [39]. VIIRS, on the other hand, is a system that detects light sources – this system greatly strengthens vessel tracking at night, which is when a significant proportion of illegal maritime activity, particularly IUU fishing, takes place [25]. Regarding fishing, VIIRS presents an especially useful technological solution as night-time fishing often uses high-powered lights to attract fish – though this is often legal, it is a fishing method that lends itself to illegal and over-exploitative fishing, thus making VIIRS an exceptionally powerful tool to detect fishing vessels that are operating illegally [24,37]. Thus, technological solutions such as these are essential for closing information and monitoring gaps when vessels disable their AIS to conceal illegal activity or fail to install AIS or VMS systems altogether.

A final technology that is in the early stages of development but has high potential for improving MDA is autonomous sensor networks. These networks, like information-sharing networks, are primarily used for risk identification - for example, Carapezza and Bucklin [12] proposed a low-cost sensor network that can be used to identify and track submerged threat objects such as submarines or uncrewed underwater vehicles (UUVs). In contrast to most current monitoring systems, which rely solely on waterborne sensors, the strength of these networks lies in their combination of in-water and on-shore sensors, resulting in a more resilient and reliable system [41,71]. Similarly, Ismail et al. [32] make a case for using uncrewed surface vehicles and UUVs for remote sensing and monitoring, the latter of which, at the time of publication, included models capable of diving to depths of up to 6000 m. While this technology is still in its early stages and has a high financial cost, it has great potential for augmenting existing monitoring systems and expanding threat detection capabilities [62,75].

A common issue in the literature on MDA-enhancing technologies is data gaps, which are particularly pervasive since all technological solutions have inherent limitations. As such, it is of high importance that MDA systems are not used in isolation and that data is instead synthesised to establish a more accurate information system which can track vessel identity, activity, movements and interactions to most effectively 'map' the maritime domain [15,17,49,67]. However, the maritime sector has historically grappled with significant barriers to information sharing – first and foremost is the "culture of secrecy" promoted by security stakeholders, whereby the inherent perception is that making data open and accessible makes shipping more vulnerable, thereby rendering information-sharing undesirable [40,43]. Furthermore, in areas of corrupt governments, information-sharing enhances the potential for collusion between maritime security officials and criminals [73]. This also creates a culture of mistrust, whereby shipping and fishing companies are reluctant to voluntarily share data due to fear that weak governance and corruption will result in the mishandling of criminal activity reports [73]. Infrastructural and financial issues also pose a serious barrier – this creates an overreliance on external actors to fund technological systems and install and maintain infrastructure where governments lack the domestic resources to devote to maritime security [63]. The outsourcing of MDA investment and capacity-building also risks power being automatically delegated to the financer of the networks and technologies, thus further disenfranchising governments who already have agendas set and political priorities

defined by foreign governments [46]. Adding further insight, Vogel [72] argues that institutional incentives exacerbate this issue, where African governments invest heavily in front-line capacity while neglecting the informational networks that support these operations. Finally, African coastal states have limited capacity to analyse data before sharing, which, combined with the multiplicity of data sources, information-sharing networks and systems of persecution, creates a highly complex and multi-layered data-sharing regime [20,38]. This network complexity, combined with the sheer volume of data, can overwhelm databases and analysts, rendering information-sharing networks inoperable [33] and, by extension, undermine efforts to ensure security at sea effectively.

Technological systems are being developed to address these issues with data sharing – these allow coastal states and maritime security authorities to not only access but share information on maritime activity, thus establishing networks of MDA. In regions with low technological capacity, such as the Gulf of Guinea (GoG), these systems have typically been sourced from external partners, such as Skylight, SOLARTA (developed by the UK government) and SeaVision (developed by the US Navy) [7]. In the GoG, a specific MDA information-sharing system has been developed – the Yaoundé Architecture Regional Information System (YARIS). Developed by the EU Gulf of Guinea Interregional Network (GoGIN) Project in support of Article 2.3 of the Yaoundé Architecture, YARIS is a high-tech information system that integrates chat, email and video conferencing [35]; additionally, the system integrates multiple data sources, such as AIS, VMS, RADAR and satellite data, which makes it more accurate and responsive than traditional single-source databases [30].

Although all these tools play important roles in enhancing MDA and contributing to maritime security, there is a need to complement them with other approaches to enhance data collection and information sharing. Looking to the Western Indian Ocean, Bueger [8] notes that as opposed to data-sharing or developing high-tech information-sharing platforms, the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP) Information Sharing Centre and the Information Fusion Centre, have built reputation and visibility by compiling and sharing regular reports on regional maritime security developments. This helps to make information accessible while at the same time increasing the transparency and legitimacy of maritime security operations, thus facilitating cooperation. There is also a role for communities in contributing to maritime security through MDA. Such is the case of Pakistan's Joint Maritime Information Coordination Centre, where staff regularly visit coastal communities. This allows maritime security operatives to hear concerns on maritime sustainability and security issues while establishing the Centre as a first point of contact when communities observe suspicious or criminal activity [9]. This is essential work, as it positions maritime security authorities as legitimate and trustworthy while establishing a network for rapid data sharing to complement surveillance technologies [3,9]. Community reporting systems prove especially effective when national maritime security authorities lack the resources for independent monitoring of maritime security threats. A good example is the K3M app in Malaysia, which allows fishers and coastal resort owners to report maritime security threats [58].

The role of technology in MDA and maritime security capacity is crucial and undeniable. Our research provides a comprehensive evaluation of technology integration in maritime security practices since adopting the Yaoundé Code of Conduct in 2013. We have utilized questionnaire data to analyze the perspectives of maritime security practitioners associated with the Yaoundé Architecture on the successes, challenges, and areas that need improvement in the use of technology in maritime security.

3. Methodological considerations

The qualitative study explored the opportunities, success stories, and challenges of using technology for maritime security in the Gulf of Guinea (GoG), specifically those operating within the Yaoundé Architecture. The Yaoundé Architecture comprises the Interregional Coordination Centre (ICC), a coordination and information-sharing structure that links the Regional Maritime Security Centre (RMSC) for Central Africa (CRESMAC) and the Regional Maritime Security Centre for West Africa (CRESMAO). The coastal area is divided into five operational Maritime Multinational Coordination Centre (MMCC) zones, specifically named zones A, D, E, F, and G. See Fig. 1 for a visual representation of the countries in the GoG Yaoundé Architecture.

The study used an open-ended questionnaire, which offers an opportunity to explore a 'wide-angle lens' on an un- or under-explored research topic [5]. The questionnaire was distributed to 25 representatives from the Yaoundé Architecture, and only 16 participants completed the questionnaire on time. A purposive sampling method was used to select participants from the Yaoundé Architecture at operational and strategic levels for their expertise and experience with maritime security in the region. Furthermore, apart from their knowledge and experience, it was essential for participants to be available, willing to take part in the study and capable of effectively communicating their experiences and opinions in an articulate, expressive, and reflective manner [48]. Table 1 highlights the characteristics of the participants.

The participants were assigned an anonymous code made up of the acronyms of their organisation and a number to ensure the confidentiality of the participants. The numbers were randomly allocated to the acronyms and do not indicate positions, seniority or roles. The following identification codes were used: YA represents Yaoundé Architecture, and the following denotes the views of personnel from the agencies within it. YA1 represents ICC, and the three participants are denoted as YA1.1, 1.2 and 1.3. YA2 represents CRESMAO, and YA3, YA4, and YA5 represent Zones D, E, and F, respectively. L1, L2, L3, and L4 represent law enforcement agents (naval) personnel from Angola, Côte d'Ivoire, Guinea, and Nigeria. L2.1 and L2.2 will be used to identify the two Ivorian Navy participants. FA represents the FCWC, and XXX 1, 2.1, and 2.2 represent participants from non-regional outside organisations that provide indirect support to the Architecture as shown in Table 1.

The open-ended questionnaire focused on assessing the maritime technology currently available or used in the GoG and how it has improved MDA and facilitated safety and security in the region. In addition, participants were asked to identify success stories, challenges, and possible solutions to address maritime technology challenges in the region. Participants responded to the following five open-ended questions:

i. What maritime technology is currently available or utilised in the Gulf of Guinea region?
ii. Has technology improved safety and security in the Gulf of Guinea? If yes, how?
iii. Are there examples of the benefits of using technology in maritime law enforcement?
iv. What are the challenges?
v. What are the solutions to the challenges you identified?

The participants typed their responses and returned the completed questionnaire via email and WhatsApp. Sixteen participants responded to the questionnaire, and some responses were more detailed than others. The data was collected between August and November 2022. Corresponding emails were sent to clarify responses that needed further clarification until March 2023, when data saturation was reached.

Data were treated as a cohesive dataset to identify themes and analytic patterns across the entire dataset [6]. The School of Geography and Sustainable Development at the University of St Andrews granted ethical approval for the study, and informed consent was obtained from each participant before participation.

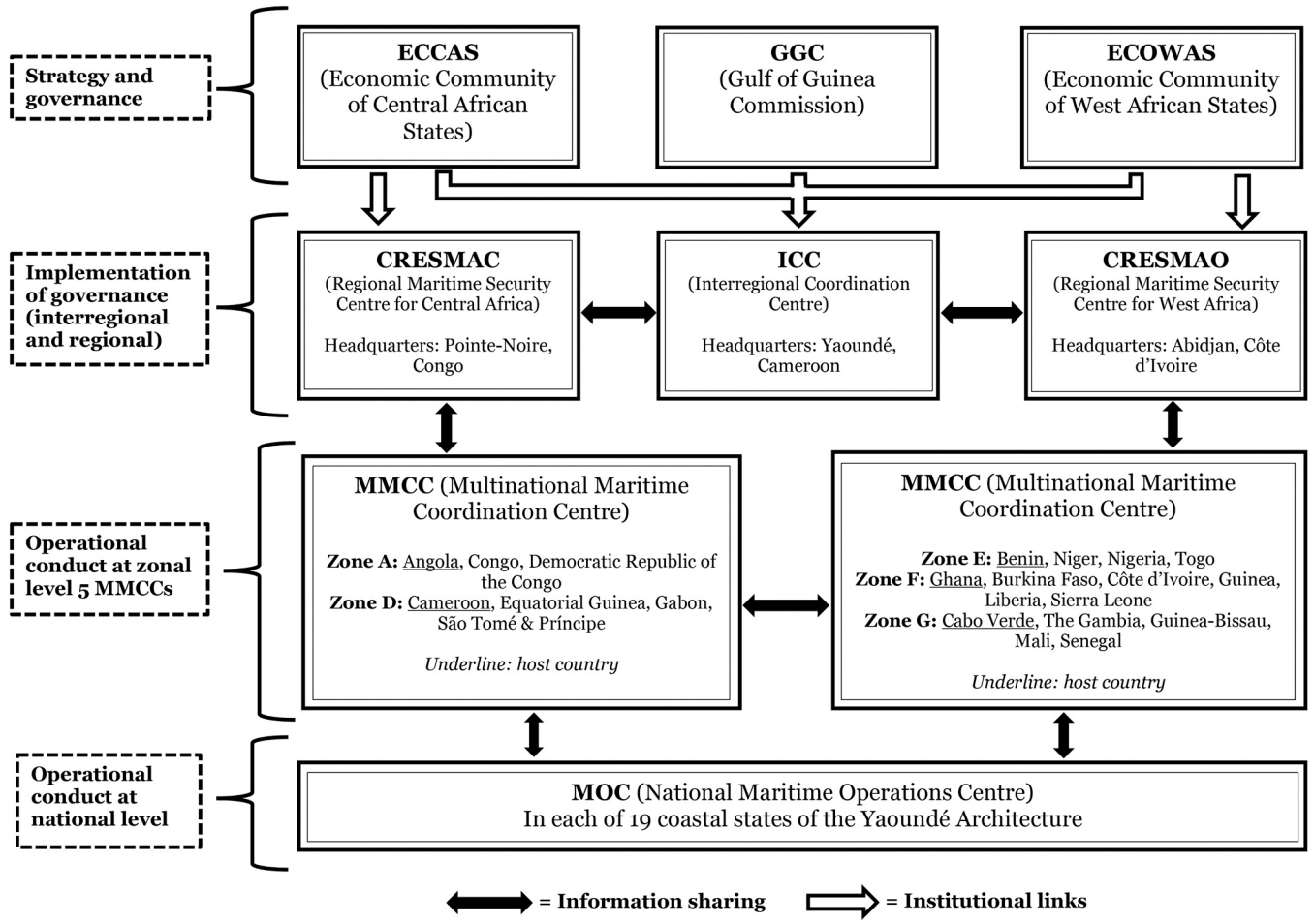


Fig. 1. The Maritime Multinational Coordination Centre (MMCC) zones of the Yaoundé Architecture (adapted from ICC [14]**).**

Table 1
Represents the organisations and sixteen participants that participated in the questionnaire.

S/ no.	Agencies represented	Number of participants	Anonymous ID
1.	Interregional Coordination Centre (ICC) Yaoundé	3	YA1.1 YA1.2 YA1.3
2.	The West Africa Regional Maritime Security Centre (CRESMAO)	1	YA2
3.	Zone D	1	YA3
4.	Zone E	1	YA4
5.	Zone F	1	YA5
6.	Angolan Navy	1	L1
7.	Cote d'Ivoire Navy	2	L2.1 L2.2
8.	Guinean Navy	1	L3
9.	Nigerian Navy	1	L4
10.	Fisheries Committee for West Central Gulf of Guinea (FCWC)	1	FA
11	International Non-governmental Organisation (INGO)[a]	1	XXX1
12	The Support to West Africa Integrated Maritime Security (SWAIMS)	2	XXX2.1 XXX2.2

[a] The contributor work for an INGO and wishes to remain anonymous.

3.1. Limitations

Out of the twenty-five (25) invitees, only sixteen (16) responded in time for us to analyse the data. This reduced the representativeness of some maritime agencies in Yaoundé Architecture, such as CRESMAC. However, this was mitigated because we had participants working at both the strategic and operational levels from the ICC in Yaoundé and CRESMAO responsible for overseeing all the GoG-wide and West African maritime operation centres, respectively. Respondents also included senior personnel from Zone D, which is under the purview of CRESMAC, and they have a broader knowledge and understanding of how technology is being used to improve maritime security in their region. The questionnaire was only provided in English, which could be problematic for Francophone and Lusophone countries in the region. However, this was not an issue as the participants had a working knowledge of English. Lastly, the use of a mixed methods data collection approach helped to minimise systematic bias from the use of one data collection method.

4. Results

Sea blindness is often associated with the pervasiveness of maritime threats in the GoG. The general perception from respondents is that for so long, the region had been, lacking maritime situational awareness or MDA capabilities. But this is changing, thanks to technology, as technology is facilitating efficient monitoring of the marine environment, communication and information sharing among law enforcement agencies which is improving safety and security at sea. Notably, technology has played a crucial role in detecting and apprehending vessels involved in illegal activities such as IUU fishing and illegal oil bunkering, as well as individuals engaged in piracy and armed robbery at sea.

In the following sub-sections, we will present a comprehensive review encompassing the use of technology, its contributions, successes, challenges, and potential solutions spanning the entire GoG region.

4.1. The current state of maritime technology in the Gulf of Guinea: some success stories

According to the analysis of questionnaire responses, various technologies are deployed at the national and regional levels for MDA to improve safety and security in the GoG – see Table 2. It is worth noting that there are likely to be other technologies not represented in this table.

Nigeria, previously known as a piracy hotspot in the GOG, has witnessed a notable improvement in maritime security. This positive transformation can be attributed to the increased adoption of MDA technologies alongside improved infrastructure such as naval assets and the bolstering of human resources for maritime patrols. In particular, the Nigerian Navy has augmented its traditional assets with the Regional Maritime Awareness Capability (RMAC) facility and the FALCON EYE system. The Nigerian Maritime Administration and Safety Agency (NIMASA) have also made advancements with its 4CI system, and the Nigerian Ports Authority (NPA) has implemented a C3I system. The Nigerian Air Force (NAF) has established a Maritime Patrol Aircraft (MPA) squadron. The Nigerian National Petroleum Corporation (NNPC) operates a Command and Control (C2) Center. The MDA tools and the other improvements have enabled Nigeria to gather the information to detect what it is that is the threat, fuse the information to know that it is a threat truly, and analyse the information so that the necessary corrective action can be determined. Although challenges persist, such as ensuring effective collaboration and integration of security systems among these agencies, adopting these technologies and other pertinent advancements has been credited to improved situational awareness and maritime security that Nigeria enjoy today.

Table 2
List of some of the technologies in use in the Gulf of Guinea.

S/no	Name of Technology	No of respondents that mentioned it
1	Automatic Identification System (AIS)	8
2	Electronic Chart Display and Information System (ECDIS)	1
3	RADAR	11
4	Vessel Monitoring System (VMS)	9
5	SeaVision[a]	11
6	Falcon Eye	7
7	Yaoundé Architecture Regional Information System (YARIS)	11
8	iSailor	1
9	Regional Maritime Awareness Capability (RMAC)[b]	2
10	Unmanned Aerial Vehicle (UAV)	4
11	Surveillance cameras	3
12	Global Fishing Watch	2
13	Long-range identification and tracking (LRIT)	4
14	Satellite imagery	6
15	Global Positioning System (GPS)	1
16	Command, control, communications, computers and intelligence (C4i)[c]	2
17	Virtual Infrared Imaging Radiometer Suite (VIIRS)	1
18	Electronic Monitoring System (EMS)	1
19	Skylight	6
20	SOLARTA	2
21	Ship Security Alert System (SSAS)	2
22	Drone technology	2
23	Time zero system[d]	1
24	Vehicle Traffic System (VTS)/Very High-Frequency Radio (VHF)[e]	5

[a] SeaVision is a web-based maritime situational awareness tool that allows users to view and share a wide range of maritime information to improve maritime operations, increase maritime security, and build partnerships among maritime stakeholders

[b] The *RMAC* system is integrated into the *Maritime* Safety and Security Information System, a global database to track ships all over the world.

[c] This is more of a security approach rather than a technology but was mentioned twice by respondents.

[d] This system, like the VTMIS, has radar components that assist with detecting vessels when off.

[e] Seems like separate tech/systems, but they were always mentioned together by respondents.

Evidently, some of the key technologies discussed in the literature are already in use in the GoG, such as the VMS and AIS identified by Chang [13] as systems critical to increasing MDA. Respondents raised this key point and agreed that technologies aimed at improving MDA in the GoG had demonstrated significant success in improving the region's maritime security architecture. A respondent gave an example of how VMS was used to help foil a piracy attack in 2015. During the attack on the fishing vessel FV Lu Rong Yuan Yu in January 2015, the pirates turned off the VMS; however, it continued to transmit data for 72 h after being turned off, allowing authorities to gather information about its location and intercept the vessel off the coast of Togo.[1] Another respondent mentioned that VMS and AIS systems are increasingly being installed as standard practice on commercial vessels, allowing for increased data collection, improved regional MDA, and informed responses in emergencies.[2]

Another system widely used in the region, albeit a recent development, is the YARIS, developed with the support of the EU, as part of the operationalisation of Yaoundé Architecture to streamline information sharing amongst parties to the Yaoundé Architecture. In addition to monitoring, mapping and analytical systems, YARIS has information-sharing modules embedded in the system, thus creating, for the first time, a technological system that captures all functions and aspects of regional MDA. According to YA1.1, the considerable improvement in information gathering and sharing has contributed to the significant reduction in piracy cases in Zones D and E (see Fig. 1) of the Yaoundé Architecture, and the introduction of YARIS has sustained this progress. Relatedly, L3 provided an example of how the use of YARIS and Sea-Vision by the Guinean MOC resulted in the successful interdiction of a vessel engaging in illegal fishing. Specifically, In July 2022, the Maritime Operational Centre (MOC) in Conakry, using the Yaoundé Architecture Regional Information Systems (YARIS) and Sea vision platforms to monitor the activities of the vessels operating in its waters, found an Egyptian-flagged vessel, *FADH Aleslam*, with a Sierra Leonean licence, fishing in its waters. The vessel was monitored for three days, and an operation to intercept, board and divert the vessel to the harbour followed. The vessel was fined €800,000 for unauthorised fishing in Guinean waters during a biological rest period (during the fishing ban) and for its cargo size.

The perspectives of the participants align with the analysis by Côrte-Real [16], who argues that due to the lack of national capacity among states in the GoG, regional information and resource-sharing regimes are highly important to improving maritime security in the region. This system, in conjunction with the establishment of MOC in each of the Yaoundé Architecture states, has generated a substantial information-gathering and information-sharing regime in the region. One example that highlights the effectiveness of information sharing through MOCs is highlighted by another respondent. The respondent recalled how effective information sharing between the Navy MOCs of Cote d'Ivoire, Ghana, Togo, Benin and Nigeria regarding the piracy attack of MT MAXIMUS in Ivorian waters in February 2016 led to the Nigerian Navy foiling the attack, arresting the pirates and freeing the crew in the EEZ of São Tomé and Príncipe.[3]

[1] Excerpt based on the response by XXX1 on how technology has contributed to improved maritime security in the GoG.

[2] Excerpt from the response from L2.1 to how technology contributes to maritime security in their country.

[3] The example is based on the response from XXX1, an INGO personnel.

5. Challenges to the use of maritime technology in the Gulf of Guinea

Respondents acknowledged that improved MDA and information sharing have enhanced maritime security in the region but also noted that they have their limitations – summarised in Table 3. For practitioners, maritime technologies alone are not a panacea. L2.1 expressed this viewpoint by noting:

Table 3
Summary of advantages and disadvantages of select technologies deployed in the GoG.

Technology	Advantages	Disadvantages
RADAR	- Low installation and operating cost - Operates in all weather conditions	- Small sensor area - Limited sensor resolution - Limited to port or coastal areas
Satellite imagery	- Large monitoring area - Visual imagery generates situational awareness	- Low resolution when monitoring large areas - High installation and operating cost - Does not provide constant monitoring
Automatic identification system (AIS)	- High rate of data transmission - Operates on global scale - Low operating cost -Allows for precise vessel identification	- Public system so can be exploited or manipulated - Can be switched off to stop data transmission - Not legally required on all ships
Vessel monitoring system (VMS)	- Developed specifically for vessel tracking and identification - Allows for precise vessel identification	- Unidirectional data transmission (ship-to-shore) - Lower data transmission rate than AIS - Can be switched off to stop data transmission
Synthetic Aperture RADAR (SAR)	- Operates in all weather conditions and any time of day - Can track vessel activity as well as identity - Higher resolution than traditional radar - Utilises data processing algorithms to identify and track vessels at a high rate	- High operating cost - Infrequent data capture (once every few days)
Vessel Infrared Imaging Radiometer Suite (VIIRS)	- Powerful tool for detecting nighttime vessel activity - High resolution allowing for precise detection	- Can only detect presence, not vessel identity or activity
Autonomous sensor networks	- Can be used to track submerged threats - Low costs for installation and maintenance	- Still in development, so efficiency is largely unknown
Unmanned underwater vehicles	- Can be used to track submerged threats - Some models can operate autonomously	- High financial cost - Still in development, so efficiency is largely unknown - Deep-water operation may hinder communications
Information-sharing platforms (SOLARTA, Skylight, SeaVision, YARIS)	- Synthesises data from multiple sources - Integrates communication systems to facilitate cooperation	- Low efficiency if participants do not openly share data - High reliance on external actors for development and funding

Technology alone cannot impact sustainable maritime security. Governance and intra/interservice and international collaboration/cooperation are needed to support technological means.[4]

Effective maritime governance should be considered essential to maritime security and where this is lacking, it should be addressed for a holistic view of what is needed to ensure sustainable security in the region. This point was also made by YA2.1, who stated that the region's governance challenges are causing a "lack of focus [and] investment on the maritime environment," which is a significant barrier to effective maritime security provision. As a result, the capacity of states to address maritime security challenges is limited, and the scope of land-based security and governance challenges means there is little incentive to focus on the maritime domain.[5] This view is consistent with Gilpin's [29] depiction of land-based security challenges as impeding state action at sea in the GoG, in which the overwhelming nature of security, development and sustainability challenges on land means that the maritime domain is less of a priority for policymakers.

The vastness of the maritime space makes it impossible for any nation or region to safeguard their maritime space without collaboration. In the context of the GoG, external support is frequently cited as a powerful means of addressing the region's limited capacity. However, this is not without its difficulties. For example, YA1.3 notes that rising technological costs, as well as concerns about the sustainability of donor partnerships, threaten the future viability of maritime security operations, particularly regarding the use of new technological systems for MDA and information sharing. Specifically, once the Gulf of Guinea Interregional Network (GoGIN+) project's funding for YARIS expires, the operating costs will be transferred from the EU to Yaoundé Architecture states.[6] The YARIS platform, developed by GoGIN with funding from the EU, [30] has enabled the development of an integrated regional threat detection and communication system. However, there are no plans from regional states to improve or sustain the existing capacity, and it is unclear how the YARIS will be sustained once the funding cycle ends. As a result, many programs and technological systems may be at risk once external funding is exhausted unless GoG countries step in to fill the gap. Other respondents shared similar views; in particular, XXX2.1 noted:

> [O]ne view is that the GoG region is a technology importer at every level, including in the security field. This comes with a level of dependence that again cuts across different sectors but also affects the way institutions and agencies operate. They depend on imports and are responsive to developments rather than being able to produce in accordance with their requirements. Put this next to another regional feature, which is structural poverty and resource constraints, which leaves agencies dependent not only on external technology but also on that technology being provided at low cost or gifted.

The reliance on external actors to bankroll or subsidise the region's technological systems has resulted in other challenges, such as the duplication of technological systems and the failure to integrate new technologies into existing systems. There is the Skylight, Global Fishing Watch system, SeaVision, YARIS and others at the regional level, which are not fully integrated. As a result, several watchkeepers are required to be trained to monitor and analyse the data from these systems for them to produce the desired results.[7] One respondent noted that "the YARIS system is having difficulty establishing itself in the field because of other

[4] Excerpt from the response by personnel from the Cote d' Ivoire.
[5] The excerpt and analysis are based on the response from CRESMAO, Cote d'Ivoire.
[6] This is based on the analysis of the response by personnel of the ICC in Yaoundé.
[7] This is based on the analysis of the response by personnel of the MMCC Zone F in Ghana.

competing solutions".[8] As noted above, duplications of technological systems and lack of interoperability is stretching the human capacity of maritime security agencies, which, if not addressed, results in the inefficient use of technological resources and diminished capacity to monitor security threats.

Further, while acknowledging the positive things that the region has achieved due to the use of technology, respondents noted that the existing technology does not go far enough in terms of coverage of regional exclusive economic zones, which is a vulnerability that criminals continue to exploit. The lack of RADAR coverage along the GoG coasts, in particular, limits the robustness of MDA. Related to this, the scarcity or non-existence of national data centres for Long Range Vessel Identification and Tracking (LRIT) makes using existing technology difficult. Furthermore, the overall lack of regional data centres for utilising satellite information for the Global Maritime Distress and Safety System (GMDSS) impedes the optimal utilisation of the available information for MDA.[9] Other challenges mentioned by respondents include high-frequency communication difficulties, the absence of AIS and internet connections onboard some vessels, low internet speed or the lack of a permanent dense internet network, all of which are costly for Maritime Operation Centres to bear. These are just a few of the obstacles to capitalising on the opportunities that maritime technology can provide.[10]

Another key challenge relates to the lack of utilisation of the services provided by the Yaoundé Architecture by private operators such as the shipping industry. Instead, vessel operators rely on external agencies for information sharing on incidents. While technologies like RADAR, Satellite systems, VMS, and AIS have improved maritime situational awareness and the ability to share information about potential incidents at sea, vessel operators must still report incidents to ensure safety and security at sea. Unfortunately, reports of incidents are usually communicated to agencies outside the region, such as Maritime Domain Awareness for Trade – Gulf of Guinea (MDAT-GoG) based in France or the International Maritime Bureau in Malaysia. One respondent noted that, "regional navies are often accused of not responding to incidents on time due to lack of assets, such claims can only be valid if incidents are reported on time".[11] In 2018, The Oil Companies International Marine Forum (OCIMF) urged its members to report to the France-based MDAT-GoG, a secure and trusted agency and this remains the position of the shipping industry to date [46].

Another key challenge to the success of maritime security technologies in the GoG is the lack of physical and human capacity, which is critical to understanding the slow uptake and positive utilisation of existing technologies. L2.1 makes the point that:

> There is little chance for ships operating illegally at sea to be seized because of the weakness of the physical means of maritime surveillance and interdiction, [making the compelling point that any gaps in enforcement capacities means that] the expense put into the technology would be wasted. L2.1 adds that insufficient cover from limited Offshore Patrol Vehicles (OPVs) and…lack of long-range patrol vessels and aircraft makes it [challenging for naval authorities to monitor the oceans, tackle illegal activity and respond to security situations].[12]

Other respondents agreed, with one adding that while technology has enabled regional navies to see what is going on at sea, the navies' lack of assets in the form of response capacity to go further at sea to verify what they are seeing remains a challenge.[13] In addition to the lack of physical capacity, there are also issues with human capacity, with a shortage of trained operators and professionals in the region to analyse the data received from satellite imagery. Economic factors play a significant role in these capacity gaps, with YA1 identifying financial resources as:

> Fundamental to finding the necessary personnel and material infrastructure for the development, maintenance, training of personnel and maintenance of systems and equipment.[14]

As a result, there are significant issues with technological literacy among operatives, with L1, XXX1, L2.2, and XXX2.2[15] all stating that a lack of technological prowess and training among operatives will be dangerous when it comes to implementing maritime security technologies, with a need for an emphasis on enhancing capacity and locally embedding training programmes to raise the operational capacity of maritime centres. The issue of maintenance of existing technology was also raised as lack of maintenance disrupts the ability of law enforcement to effectively utilise the technologies if they are not serviced, updated and softwares upgraded.

6. Solutions to maritime security technology challenges

Having discussed some of the challenges, we now focus on the solutions. Regional and external partnerships have been vital to capacity-building for maritime security in the GoG like elsewhere. This inter-agency, cross-border, regional and international cooperation and collaboration has contributed significantly to stemming the tides of security threats at sea in the region, especially piracy [46,68]. Therefore, there is an incentive to continue this collaborative approach to maritime safety and security—the research respondents are of the same view.

Respondents recommended increased extra-regional partnership as critical to raising funds for increasing MDA and addressing maritime security threats in recognition of the economic challenges and nature of insecurity on land across the GoG states, which creates a negative feedback loop in which nations grow increasingly unable to tackle the ramping security threats in the maritime domain. The prohibitive cost of acquiring technologies for L1 can be addressed through affordability plans or subsidies to GoG countries, which can take the form of direct investment or organisational funding schemes such as those offered by the EU or other partners.[16] XXX2.1 added that to sustain the progress, external partners need to coordinate and bear the running costs of existing and new tools.[17] In addition, addressing the maintenance issues, thus, requires that a systematic maintenance programme be put in place.[18] Well formalised, the extra-regional partnerships allow for the duplication of technological and other maritime enforcement systems to be avoided while ensuring interoperability as new systems are integrated for effective utilisation.[19]

In response to the valid concerns which have been raised by participants over the complications involved with the provision of MDA-enhancing technologies by extra-regional actors, partnerships should focus on enhancing enforcement and governance capacity. As noted above, GoG navies often lack the enforcement capacity to tackle

[8] The excerpt is from the response from personnel working with an implementing agency, and this view is echoed by some of the other respondents.

[9] The analysis is based on the response of a representative from MMCC Zone D in Cameroon.

[10] This analysis is drawn from all the respondents' responses, especially the representatives of Zones E, F, ICC and CRESMAO.

[11] The excerpt from the response from XXX1, an INGO personnel.

[12] Excerpt from the response from a personnel of the Cote d'Ivoire Navy.

[13] The analysis is based on the response from YA3, an MMCC Zone E, based in Benin Republic.

[14] Excerpt from the response of personnel of ICC in Yaoundé.

[15] L1—personnel of the Nigerian Navy, XXX personnel from an external agency that has opted for anonymity, L2.2. Personnel of the Cote d'Ivoire Navy and XXX2.2; Personnel of the SWAIMS programme.

[16] This is based on the analysis of the response by personnel of the Nigerian Navy.

[17] XXX2.1 is a personnel from the SWAIMS programme.

[18] XXX2.1 is a personnel from the SWAIMS programme.

[19] XXX2.1 is a personnel from the SWAIMS programme.

maritime security threats once they have been identified, thus undermining the efficacy and impact of new MDA and information technologies. International cooperation will be key to closing this gap in capacity. The EU's CMP concept exemplifies an attempt to close the existing gap through international support. Developed to promote strong maritime governance while addressing the root causes of security issues, the implementation of the CMP in the GoG lays the groundwork for EU partnerships focussed on development resilience and capacity-building [27]. A key component of the CMP is the designation of the GoG as a Maritime Area of Interest, which establishes a mandate for the continuation of EU naval operations in the region: this designation allows the EU to utilise Member States' naval assets already deployed in or passing through the GoG [44]. Launched in January 2020, five Member States (Denmark, Spain, Italy, France and Portugal) participated in multilateral exercises in the region and ensured that at least one ship was present in the GoG through 2021 [22]. For the CMP to be effective, it needs to prioritise cooperation and collaboration with the GoG navies rather than unilateral actions; such cooperation would ensure that incidents like the one that occurred in 2021 when the Danish Navy deployed the Esbern Snare under the CMP are not repeated [46].

Additionally, as noted in the literature and amongst respondents, poor governance poses a significant barrier to effective efforts to enhance maritime security. As with enforcement capacity, external partnerships can play a substantial role in building good governance, particularly regarding the enhancement of legal prosecution systems. The EU is a large player in this area, operating several programs in partnership with the United Nations Office on Drugs and Crime's Global Maritime Crime Programme. These programmes – Programme to Support the Maritime Safety and Security in Strategy in Central Africa (PASSMAR) and Strengthening Criminal Justice Systems in West and Central Africa (SWAIMS) - have a combined budget of €10.7 million and aimed to develop and strengthen legal frameworks amongst GoG states through capacity-building and training [70]. There have been some concerns raised over these external partnerships due to the nature of EU bureaucracy – its capacity-building approaches risk "conflating output with impact" and the abundance of strategies risks policy conflict and divergence [11] - but overall, the EU's engagement has been welcomed by domestic maritime security agencies in the GoG.

To close some of the loopholes resulting from the lack of coverage of the GoG coasts, respondents suggested that consideration should be given to the installation of coastal RADAR systems. Related to this is the need for states to update their naval assets, especially vessels and boats equipped with terminals compatible with satellite information and GMDSS, with fast internet connectivity on board patrol vessels. Given that not all states have the capability to acquire assets and increase their maritime presence, there is a need for cooperation and collaboration between states, including through regular exercises to improve capacity and interoperability. To address the existing gap in patrols, perhaps the Combined Maritime Task Force (CMTF), of which, as of May 2023, 11 GoG countries have signed the Concept of Operations aimed at coordinating patrol of the regional waters is one way to ensure regional ownership and closing the loopholes resulting from lack of assets for patrols [69].

The limitations of internet connectivity can be addressed by providing funds for subscriptions, software updates and maintenance of communication systems. Importantly, respondents recognised the need for a secured communication platform for regional law enforcement to share information given the increased risk of cyber sabotage that is associated with the use of technology. Fully aware of the financial constraints in the region, respondents noted that some of these provisions, for instance, the installation of coastal RADARS could be done through partnerships with multinational companies who would equally benefit from the resultant benefit of regional law enforcement being more maritime domain aware. Relatedly, technology companies could also support the efforts of regional navies as part of their corporate social responsibility by making internet connectivity available at a subsidised rate.[20]

While previous discussions raised concerns about the dependency on external actors created by extra-regional partnerships, solutions to these issues do exist. XXX2.2 highlights the need for states in the GoG to pool resources as well as information "so that the least well-off countries also benefit from the means of the most well-off countries", including exploring opportunities from public-private partnerships to meet rising procurement and operating costs.[21] For L2.2, since the extra-regional dependencies stem from a lack of technological literacy amongst maritime security operatives in the region, there is a need for a targeted capacity enhancement campaign that focuses on developing technological solutions that are adapted to both local contexts and levels of technological skills amongst maritime security operatives, with external partners providing training and logistical support rather than replacing African states as maritime security providers.[22] Importantly, continuous training is needed for analysts and other law enforcement who engage with these technologies to effectively interpret the data they are receiving for effective maritime safety and security.

There is a role for civil society organisations in promoting a renewed focus on the maritime sector. Through research and advocacy, NGOs, academics, and the media all play a role in developing an environment that places higher value on the maritime domain, as well as undertaking crucial research that will be of a great use to states looking to enhance their MDA.[23] However, states seem reluctant to partner with civil society stakeholders, a trend that must change for the sake of future maritime security. As is often the case in the field of maritime governance, policy-makers are increasingly looking to Europe – for example, in 2020 the EU established the International Ocean Governance, aiming to bring together governments, civil society policy-makers and other ocean stakeholders to share ideas and solutions to improve ocean governance [26]. Although at its nascent stages, forums such as this provide models for governments and maritime security experts in the GoG and the African continent at large to foster better relationships between the state and civil societies and coordinate on best practices for the effective utilisation of technologies for maritime safety and security.

7. Implications and conclusions

Based on our analysis of questionnaire data, literature review, and policy documents, we have presented compelling evidence to emphasize the importance of MDA for enhancing maritime security. In the context of the GoG, we have demonstrated how technology has improved MDA and information sharing, leading to improved maritime security in the region. We have also highlighted some who challenges and proposed solutions to address them.

It is evident that the GoG states have made significant progress in the past decade since the signing of the Yaoundé Code of Conduct. However, it is crucial to maintain this progress by acknowledging that the implementation of maritime technology necessitates the training of personnel who possess the necessary expertise to analyse and interpret the data transmitted by these technologies. Therefore, for technology to continue to be effectively deployed by maritime law enforcement on the continent, there is a need for such technological deployment to run in tandem with capacity enhancement programs for maritime law

[20] The recommendations are based on the analysis of the views of all the respondents.

[21] The analysis and excerpt are based on the response by a personnel from the SWAIMS project.

[22] The analysis is based on the view of personnel of the Cote d'Ivoire Navy.

[23] The analysis is based on the views of a personnel of the ICC, Yaoundé.

enforcement agencies. The analysis of the data has shown that security technologies that focus on threat identification are only effective if law enforcement officials have the necessary resources to interdict these threats. Therefore, the implementation of security technology should be accompanied by the provision of assets that law enforcement needs to carry out interdiction effectively.

As the Yaoundé Code of Conduct commemorates ten years since it was signed, it is important to acknowledge the progress made. Before 2013, countries had a limited picture of the maritime domain and often were unaware of activity outside their own exclusive economic zones. This is not the case today due to the advancements in the use of technology and other relevant measures [42] However, there is room for improvement as the current technologies for MDA, such as Skylight, Sea Vision, YARIS, Global Fishing Watch, and others, lack regional ownership. Optimising technology usage and establishing a regionally owned and managed tool for real-time data collation and analysis is essential. Empowering the existing Maritime Fusion Centers to function at optimal capacity is a logical next step. These Centers would provide a common operating picture for GoG countries allowing for the ownership of data collection, fusion, and utilisation to produce valuable threat intelligence, facilitate efficient enforcement and monitoring, and foster collaboration for enhanced security at sea.

Ultimately, the renewed focus on governance to enhance MDA and maritime security provision is helping to integrate the marine domain into a wider environment of security, which will facilitate investment and in the long run enhance the capacities of the maritime enforcement agencies to be better able to fulfil their mandate. Achieving this requires that the regional government prioritises securing the maritime domain and the resources within it, by investing in the much-needed technology and other assets that would allow law enforcement agents to do their jobs effectively.

Funding

This research was supported by funding from the St Andrews Research Internship Scheme (StARIS). Lucas de Oliveira Paes's contribution to this publication was funded by a grant from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 803335, 'The Lorax project: understanding ecosystemic politics').

CRediT authorship contribution statement

The idea was conceptualized by I.O-Y, who also conducted the survey and drafted the initial manuscript. OL provided valuable insight and support by contributing to the initial literature review, and data analysis, as well as assisting with the writing and reviewing of the manuscript. NC played an important role by contributing to the methods section, data analysis, and manuscript review. LO also contributed significantly to the data analysis and manuscript review. Finally, all authors collaborated on the manuscript revision, resulting in a comprehensive and polished final product.

Data Availability

Data will be made available on request.

Acknowledgements

We are grateful to the research participants whose contributions provided us with the rich data we needed to understand the extent to which technology has improved Maritime Domain Awareness and, as a result, security in the Gulf of Guinea, the challenges associated with the use of technology, and solutions to these challenges. We are especially grateful to participants from the ICC in Yaoundé, CREASMAO, MMCC Zones D, E and F, the navies of Cote d'Ivoire, Guinea and Nigeria, FCWC, SWAIMS and others who do not wish to be identified. Your generosity with your time and expertise has allowed us to write this seminal work, and we are grateful for that. We express our gratitude to the editors of Marine Policy and the reviewers of our paper, whose valuable insights and thoughtful critique have significantly contributed towards enhancing the overall quality of the paper.

References

[1] Balci, M., Pegg, R. (2006) Towards global maritime domain awareness – recent developments and challenges, 9th International Conference on Information Fusion. Florence, 10–13 July. IEEE. DOI: 10.1109/ICIF.2006.301702.

[2] Balduzzi, M., Pasta, A., Wilhoit, K. (2014) A security evaluation of AIS Automated Identification System, ACSAC '14: Annual Computer Security Applications Conference. New Orleans, 8–12 December. ACSAC. Available at https://dl.acm.org/doi/10.1145/2664243.2664257.

[3] Benson, J. (2020) Human intelligence: the missing piece to comprehensive maritime domain awareness, *CIMSEC,* 28 April. Available at ⟨https://cimsec.org/human-intelligence-the-missing-piece-to-comprehensive-maritime-domain-awareness/⟩.

[4] Boraz, S.C. (2009) Maritime Domain Awareness: Myths and Realities, Naval War College Review, vol. 62, no. 3, pp. 137–146. Available at: ⟨https://digital-commons.usnwc.edu/nwc-review/vol62/iss3/10⟩.

[5] V. Braun, V. Clarke, E. Boulton, L. Davey, C. McEvoy, The online survey as a qualitative research tool, Int. J. Soc. Res. Methodol. 24 (6) (2021) 641–654. DOI: 1080/13645579.2020.1805550.

[6] V. Braun, V. Clarke, Thematic analysis, in: H. Cooper, P.M. Camic, D.L. Long, A. T. Panter, D. Rindskopf, K.J. Sher (Eds.), APA Handbook of Research Methods in Psychology; Vol. 2: Research Designs: Quantitative, Qualitative, Neuropsychological, and Biological, American Psychological Association, Washington D.C, 2012, pp. 57–71.

[7] Brewster, D. (2022) New satellite-based technologies a game change for Indo-Pacific maritime security, *The Strategist*, 13 July. Available at ⟨https://www.aspistrategist.org.au/new-satellite-based-technologies-a-game-changer-for-indo-pacific-maritime-security/⟩.

[8] Bueger, C. (2017a) Effective maritime domain awareness in the Western Indian Ocean. Available at https://orca.cardiff.ac.uk/id/eprint/102573/1/Bueger%20(2017)%20Maritime%20Domain%20Awareness%20in%20WIO.pdf.

[9] Bueger, C. (2017b) 'People first: Pakistan's approach to Maritime Domain Awareness', *Christian Bueger*, 16 February. Available at ⟨https://bueger.info/people-first-pakistans-approach-to-maritime-domain-awareness/⟩.

[10] C. Bueger, T. Edmunds, 'Beyond sea blindness. A new agenda for maritime security studies, Int. Aff. 93 (6) (2017) 1293–1311, https://doi.org/10.1093/ia/iix174.

[11] C. Bueger, T. Edmunds, The European Union's Quest to become a global maritime-security provider, Nav. War. Coll. Rev. 76 (2) (2023) 73–92. Available at: ⟨https://digital-commons.usnwc.edu/nwc-review/vol76/iss2/6⟩.

[12] E.M. Carapezza, A. Bucklin, Intelligent maritime security system with sensor networks for coastal environmental and homeland security applications, Proc. Soc. Photo-Opt. Instrum. Eng. 6736 (2007), https://doi.org/10.1117/12.753480.

[13] Chang, S.-J. (2003) Vessel identification and monitoring systems for maritime security, IEEE 37th Annual 2003 International Carnahan Conference on Security Technology. Taipei, 14–16 October. IEEE. Available at ⟨https://ieeexplore.ieee.org/abstract/document/1297537⟩.

[14] CIC (2023) Yaoundé Architecture. Available at: https://icc-gog.org/?page_id=1575.

[15] Claramut, C., Ray, C., Camossi, E., Jousselme, A.-L., Hadzagic, M., Andrienko, G., Andrienko, N., Theodoridis, Y., Vouros, G.A., Salmon, L. (2017) 'Maritime data integration and analysis: recent progress and research challenges', *20th International Conference on Extending Database Technology*. Venice, 21–24 March. OpenProceedings. Available at ⟨https://www.researchgate.net/publication/312601728_Maritime_data_integration_and_analysis_recent_progress_and_research_challenges⟩.

[16] Côrte-Real, J. (2022) Maritime security in the Gulf of Guinea, threats, and challenges, *Negócios Estrangeiros*, vol. 22, pp. 61–72. Available at ⟨https://idi.mne.gov.pt/images/Revista_NE/PDF/n%C2%BA22_Oceanos/RNegociosEstrangeiros_5_Maritime_Security_in_the.pdf⟩.

[17] M.E. de Magalhães, C.E. Barbosa, Faria de, K. Cordeiro, D.K.M. Isidorio, J.M. de Souza, Improving maritime domain awareness in Brazil through computer technology, J. Mar. Sci. Eng. 11 (7) (2023). DOI: 10.3390/jmse11071272.

[18] Del Prete, R., Graziano, M.D., Grasso, M., Renga, A., Cricielli, L., Centobelli, P., Moccia, A., Piscane, V., Aurigemma, R., Virelli, M., Sacco, P., Montuori, A. (2022) 'Maritime Monitoring by Multi-Frequency SAR Data', *2022 IEEE International Synopsium on Geoscience and Remote Sensing (IGARSS)*. Kuala Lumpur, 17–22 July. IEEE. Available at ⟨https://ieeexplore.ieee.org/document/9884613⟩.

[19] E. Detsis, Y. Brodsky, P. Knudtson, M. Cuba, H. Fuqua, B. Szalai, Project Catch: a space based solution to combat illegal, unreported and unregulated fishing: Part I: vessel monitoring system, Acta Astronaut. 80 (2012) 114–123, https://doi.org/10.1016/j.actaastro.2012.06.009.

[20] P.D. Doherty, B.C. Atsango, G. Ngassiki, A. Ngouembe, N. Bréheret, E. Chauvet, B. J. Godley, L. Machin, B.D. Moundzoho, R.J. Parnell, K. Metcalfe, Threats of illegal, unregulated, and unreported fishing to biodiversity and food security in the Republic of the Congo, Conserv. Biol. 35 (5) (2021) 1463–1472, https://doi.org/10.1111/cobi.13723.

[21] T.J. Doorey, Maritime domain awareness, in: P. Shemella (Ed.), Global Responses to Maritime Violence: Cooperation and Collective Action, Stanford University Press, Stanford, 2016, pp. 11–29.

[22] EEAS (2021) EU Maritime Security in The Gulf of Guinea: Strategy and Action Plan. Available at ⟨https://www.eeas.europa.eu/sites/default/files/note_eu_gog_strategy.pdf⟩.

[23] E.E. Egede, Gulf of guinea and maritime (In)Security: musings on some implications of applicable legal instruments, Brooklyn J. Int. Law 46 (2) (2021) 369–419. ⟨https://brooklynworks.brooklaw.edu/cgi/viewcontent.cgi?article=1972&context=bjil⟩.

[24] Elvidge, C.D., Baugh, K., Zhizhin, M., Hsu, F.-C., Ghosh, T. (2017) Supporting international efforts for detecting illegal fishing and gas flaring using VIIRS, 2017 IEEE International Symposium on Geoscience and Remote Sensing (IGARSS). Fort Worth, 23–28 July. IEEE. DOI: 10.1109/IGARSS.2017.8127580.

[25] Elvidge, C.D., Ghosh, T., Hsu, F.C., Zhizhin, M. (2022) VIIRS Monitoring and Reporting on Lit Fishing Vessel Detections in Southeast Asia, 2022 IEEE International Symposium on Geoscience and Remote Sensing (IGARSS). Kuala Lumpur, 17–22 July. IEEE. DOI: 10.1109/IGARSS46834.2022.9883658.

[26] European Commission (2022) Setting the course for a sustainable blue planet: Recommendations for enhancing EU action. Available at https://3rd-iog-forum.fresh-thoughts.eu/wp-content/uploads/sites/89/2021/04/IOG-recommendations-2021-WEB.pdf.

[27] Fiott, D. (2021) Naval gazing? The Strategic Compass and the EU's maritime presence. Available at https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_16_2021.pdf.

[28] J.S. Fowdur, M. Baum, F. Heymann, Real-world marine radar datasets for evaluating target tracking methods, Sensors 21 (14) (2021), https://doi.org/10.3390/s21144641.

[29] Gilpin, R. (2007) Enhancing Maritime Security in the Gulf of Guinea, Strategic Insights, vol. 6, no. 1. Available at ⟨https://apps.dtic.mil/sti/pdfs/ADA520363.pdf⟩.

[30] GoGIN (2023) Maritime security in the Gulf of Guinea. Gulf of Guinea Interregional Network. Available at ⟨https://www.gogin.eu/wp-content/uploads/2023/01/221125-Depliant-GoGIN-par-page.pdf⟩.

[31] Heubl, B. (2021) How Europe's dark fishing fleets threaten West Africa. Available at https://eandt.theiet.org/content/articles/2021/03/europe-s-dark-fishing-fleets-in-west-africa-s-waters/.

[32] Ismail, M.A., Ali, S., Khan, S., Babar, Z., Mazhar, M. (2021) A survey of Indian Ocean region maritime security: Technological advancements and innovative solutions, 2021 International Conference on Frontiers of Information Technology (FIT). Islamabad, 13–14 December. IEEE. Available at: https://ieeexplore.ieee.org/document/9701384/.

[33] J.G. Kallimani, The challenges of digitisation and data analysis in the maritime domain, Marit. Aff.: J. Natl. Marit. Found. India 14 (1) (2018) 36–50, https://doi.org/10.1080/09733159.2018.1478433.

[34] G.I. Lambert, S. Jennings, J.G. Hiddink, N.T. Hintzen, H. Hinz, M.J. Kaiser, L. G. Murray, Implications of using alternative methods of vessel monitoring system (VMS) data analysis to describe fishing activities and impacts, ICES J. Mar. Sci. 69 (4) (2012) 682–693, https://doi.org/10.1093/icesjms/fss018.

[35] Larsen, J.P. (2023) The Gulf of Guinea Declaration one year on – status report, *BIMCO*, 12 July. Available at ⟨https://www.bimco.org/insights-and-information/safety-security-environment/20220712-gulf-of-guinea-declaration-one-year-on⟩.

[36] Lehmann, M. and Middleditch, A. (2022) Satellite dark vessel detection for maritime domain awareness. Available at ⟨https://starboard.nz/case-study-dark-vessel-detection-for-mda/⟩.

[37] Y. Li, L. Song, S. Zhao, D. Zhao, Y. Wu, G. You, Z. Kong, X. Xi, Z. Yu, Nighttime fishing vessel observation in Bohai Sea based on VIIRS fishing vessel detection product (VBD), Fish. Res. 258 (2023), https://doi.org/10.1016/j.fishres.2022.106539.

[38] J. Lindley, E.J. Techera, Overcoming complexity in illegal, unregulated and unreported fishing to achieve effective regulatory pluralism, Mar. Policy 81 (2017) 71–79, https://doi.org/10.1016/j.marpol.2017.03.010.

[39] Motomura, K., Nagao, T. (2020) Fishing activity prediction from satellite boat detection data, IEEE International Conference on Systems, Man and Cybernetics. Toronto, 11–14 October. IEEE. DOI: 10.1109/SMC42975.2020.9283451.

[40] Murphy, M.N. (2009) Lifeline or Pipedream? Origins, Purposes, and Benefits of Automatic Identification Systems, Long-Range Identification and Tracking, and Maritime Domain Awareness, in Herbert-Burns, R., Bateman, S. and Lehr, P. (eds), Lloyd's MIU Handbook of Maritime Security. Boca Raton, Taylor & Francis, pp. 13–28.

[41] M. Nakano, S. Hiroshi, J. Muramatsu, K. Mihara, M. Kobayashi, M. Yagi, Underwater surveillance system to counteract associated underwater threats, NEC Tech. J. 8 (1) (2013) 63–67 (Available at), ⟨https://www.nec.com/en/global/techrep/journal/recommend_year/2013/10.html⟩.

[42] Ngada, T. (2023) A Decade of Maritime Security, ADF, 24 July. Available at https://adf-magazine.com/2023/07/a-decade-of-maritime-security/.

[43] Nimmich, J.L., Goward, D.A. (2007) Maritime domain awareness: the key to maritime security, International Law Studies, vol. 83, pp. 57–65. Available at https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1160&context=ils.

[44] N. Nováky, The coordinated maritime presences concept and the EU's naval ambitions in the Indo-Pacific, Eur. View 21 (1) (2022) 56–65, https://doi.org/10.1177/17816858221089871.

[45] Okafor-Yarwood, I., Pigeon, M., Amling, A., Ridgway, C., Adewumi, I., Joubert, L. (2020) Stable seas: Gulf of Guinea. DOI: 10.18289/OEF.2020.043.

[46] I.M. Okafor-Yarwood, F.C. Onuoha, Whose security is it? Elitism and the global approach to maritime security in Africa, Third World Q. 44 (5) (2023) 946–966, https://doi.org/10.1080/01436597.2023.2167706.

[47] Page, E. (2017) Maximising maritime safety and environmental protection with AIS: (Automatic identification system), OCEANS 2017 – Anchorage. Anchorage, 18–21 September. IEEE. Available at https://ieeexplore.ieee.org/document/8232402.

[48] L.A. Palinkas, S.M. Horwitz, C.A. Green, J.P. Wisdom, N. Duan, K. Hoagwood, Purposeful sampling for qualitative data collection and analysis in mixed implementation research, Adm. Policy Ment. Health 42 (5) (2015) 533–544, https://doi.org/10.1007/s10488-013-0528-y.

[49] P.M. Perera, Integrated maritime picture for effective domain awareness, Marit. Technol. Res. 2 (3) (2020) 108–113, https://doi.org/10.33175/mtr.2021.224463.

[50] Ponsford, A.M. (2015) Radars for Maritime Domain Awareness, Military Radar Summit. Washington, D.C., 23–25 February. IDGA. DOI: 10.13140/RG.2.1.3961.7687.

[51] Proud, R., Browning, P., Kocak, D.M., Wiafe, G., Agyekum, K. (2017) 'Small vessel tracking using AIS for enhanced maritime domain awareness', *OCEANS 2017 – Anchorage*. Anchorage, 18–21 September. IEEE. Available at ⟨https://ieeexplore.ieee.org/document/8232293⟩.

[52] L.A. Roberson, J.J. Kiszka, J.E.M. Watson, Need to address gaps in global fisheries observation, Conserv. Biol. 33 (4) (2018) 966–968, https://doi.org/10.1111/cobi.13265.

[53] Rodger, M., Guida, R. (2022) Mapping dark shipping zones using multi-temporal SAR and AIS data for maritime domain awareness, 2022 International Symposium on Geoscience and Remote Sensing (IGARSS). Kuala Lumpur, 17–22 July. IEEE. DOI: 10.1109/IGARSS46834.2022.9883797.

[54] D. Russell, Who Rules the Waves? Piracy, Overfishing and Mining the Oceans, Pluto Press, London, 2010.

[55] B.J. Ryan, The disciplined sea: a history of maritime security and zonation, Int. Aff. 95 (5) (2019) 1055–1073, 10.1093/ia/iiz098.

[56] Schwegmann, C.P. (2014) Ship detection methods for maritime domain awareness using SAR satellite data, Master of Engineering (Computer Engineering) thesis, Pretoria, The University of Pretoria.

[57] Schwegmann, C.P., Kleyhans, W. (2014) Synthetic aperture radar for maritime domain awareness: Ship detection in a South Africa context, Tenth International Conference of the African Association of Remote Sensing of the Environment. Johannesburg, 27–31 October. CSIR. Available at http://hdl.handle.net/10204/8479.

[58] Shahrudin, H.S. (2017) Mobile app K3M enables faster response time to emergencies at sea, New Straits Times, 23 March. Available at https://www.nst.com.my/news/2017/03/223743/mobile-app-k3m-enables-faster-response-time-emergencies-sea,

[59] J.L. Shepperson, N.T. Hintzen, C.L. Szostek, E. Bell, L.G. Murray, M.J. Kaiser, A comparison of VMS and AIS data: the effect of data coverage and vessel position recording frequency on estimates of fishing footprints, ICES J. Mar. Sci. 75 (3) (2017) 988–998, https://doi.org/10.1093/icesjms/fsx230.

[60] Sikaneta, I., Gierull, C. and Cerutti-Maori, D. (2014) Enhancing global maritime domain awareness through SAR with multiple apertures, 2014 International Symposium on Geoscience and Remote Sensing (IGARSS). Quebec City, 13–18 July. Available at https://ieeexplore.ieee.org/abstract/document/6946628.

[61] Smith, B. (2022) Enhancing Maritime Domain Awareness With Maxar's Crow's Nest Solution, *Maxar Blog*, 31 February. Available at ⟨https://blog.maxar.com/earth-intelligence/2022/enhancing-maritime-domain-awareness-with-maxars-crows-nest-solution⟩.

[62] Sonardyne (2019) Deep, covert & long range Autonomous Underwater Vehicles (AUVs), *Sonardyne*, 12 September. Available at ⟨https://www.sonardyne.com/deep-covert-and-long-range-auvs/⟩.

[63] Soto, A.A. (2010) Maritime information-sharing strategy, Naval War College Review, vol. 63, no. 3. Available at ⟨https://digital-commons.usnwc.edu/nwc-review/vol63/iss3/10⟩.

[64] J. Stockbruegger, US Strategy and the Rise of Private Maritime Security, Secur. Stud. 30 (4) (2021) 578–602, https://doi.org/10.1080/09636412.2021.1976821.

[65] Tetreault, B.J. (2005) Use of the Automatic Identification System (AIS) for maritime domain awareness (MDA), Oceans 2005 MTS/IEEE. Washington, D.C., 17–23 September. IEEE. Available at ⟨https://ieeexplore.ieee.org/document/1639983⟩.

[66] Thomas, G. (2019) Collaborative Space-based Maritime Situational Awareness (CSMSA) - Pathway to Global Maritime Cooperation for Security, Safety, Environmental Protection, and Resource Conservation. Available at ⟨https://www.cmre.nato.int/msaw-2019-home/msaw2019-papers/1383-msaw2019-thomas-collaborativespacebasedmaritimesituationalawarenesscsmsa/file⟩.

[67] P. Thoya, J. Maina, C. Möllmann, K.S. Schiele, AIS and VMS ensemble can address data gaps on fisheries for marine spatial planning, Sustainability 13 (7) (2021), 10.3390/su13073769.

[68] UN (2022) Adopting Resolution 2634 (2022), Security Council Calls on Gulf of Guinea Countries to Criminalize Piracy, Armed Robbery at Sea under Domestic Laws, Meetings Coverage Security Council. Available at ⟨https://press.un.org/en/2022/sc14915.doc.htm⟩.

[69] UN (2023) Ongoing Decline in Gulf of Guinea's Piracy, Armed Robbery Encouraging, But Support Needed to Fully Implement Yaoundé Architecture, Briefers Tell Security Council, United Nations Meetings Coverage and Press Releases, 21 June. Available at https://press.un.org/en/2023/sc15331.doc.htm.

[70] UNODC (2019) EU-GMCP Partnership. Available at ⟨https://www.unodc.org/documents/Maritime_crime/EU-GMCP_PARTNERSHIP_REPORT.pdf⟩.

[71] Uppal, R. (2021) Rising importance of non-acoustic detection technologies of stealthy submarines in anti-submarine warfare, International Defence, Security & Technology, 10 February. Available at ⟨https://idstch.com/geopolitics/rising-importance-of-non-acoustic-detection-technologies-of-stealthy-submarines-in-anti-submarine-warfare/⟩.
[72] Vogel, A. (2011) Investing in science and technology to meet Africa's maritime security challenges. Available at ⟨https://africacenter.org/publication/investing-in-science-and-technology-to-meet-africas-maritime-security-challenges/⟩.
[73] Walker, T. (2015) Enhancing maritime domain awareness in Africa. Available at ⟨https://www.files.ethz.ch/isn/194504/PolBrief79.pdf⟩.
[74] H. Welch, T. Clavelle, T.D. White, M.A. Cimino, J. van Osdel, T. Hochberg, D. Kroodsma, E.E. Hazen, Hot spots of unseen fishing vessels, Sci. Adv. 8 (44) (2022), https://doi.org/10.1126/sciadv.abq2109.
[75] E. Zereik, M. Bibuli, N. Mišković, P. Ridao, A. Pascoal, Challenges and future trends in marine robotics, Annu. Rev. Control 46 (2018) 350–368, https://doi.org/10.1016/j.arcontrol.2018.10.002.
[76] IMO (2023) AIS transponders. Available at ⟨https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx⟩.