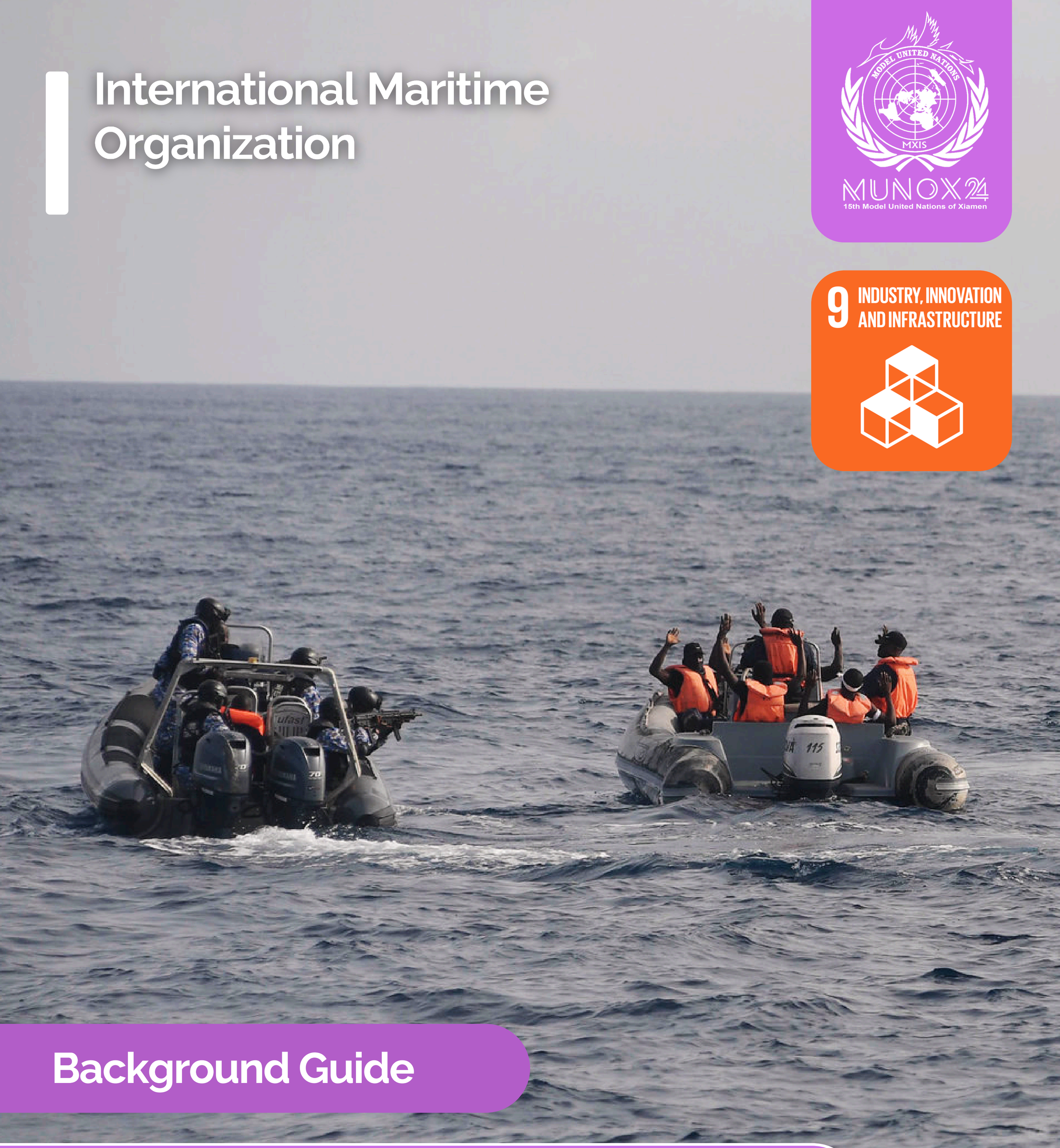
International Maritime Organization

MODEL UNITED NATIONS
MXIS
MUNOX24
15th Model United Nations of Xiamen

9 INDUSTRY, INNOVATION AND INFRASTRUCTURE



Background Guide

Preventing and Countering Maritime Cyber Attacks in Gulf of Guinea

Table of Contents

Welcome Letter From The DAIS

Dear Delegates,

We welcome you to MUNOX 2024! It is with immense pleasure that we have you attending our upcoming conference and debating relevant issues that are impactful and applicable to the maritime world.

My name is Julie Chen, and I am incredibly excited to serve as the Director of the International Maritime Organization at MUNOX 2024. I am currently a grade 10 student at Manila Xiamen International School, where I have been actively involved with MUN since 5th grade. Along with me on the dais team is Grade Cai.

Hello! I am Grace Cai, a 11th grade student from Chiway Repton School, Xiamen. Since I participated in MUNOX last year as a delegate, I have been looking forward to this chance of being a DAIS member. I'm very excited to work with you guys as the assistant director!

Since its formal inception in 1959, the International Maritime Organization (IMO) has been the specialized agency of the United Nations dedicated to improving the conditions of seafarers and increasing the efficiency and safety of international maritime trade. IMO's main area of work focuses on ensuring the safety, security, and environmental performance of the maritime domain. This year, delegates are tasked to construct functional frameworks and solutions to assist African states along the Gulf of Guinea in their digitalization of vital maritime infrastructures in face of potential cyberattacks that may prove detrimental to Africa's recovering economy since the economic recession due to COVID-19. You will delve into the intricacies in maintaining sound maritime cybersecurity in the region and examine existing external cases to formulate practical solutions that will strengthen Africa's capacity to prevent and mitigate cybersecurity risks in the near future.

One advice we would like to mention is that a superficial review of the topic will not suffice to attain true success in this simulation. We look forward to reading well-researched position papers and seeing a rich debate of the nuances surrounding the issue. Although it is our hope that this Background Guide serves you well in grasping the topic, we hope that you will treat it as a jumping point to all the research that has yet to be done. A delegate's preparation is an essential facet of MUN – so as in any other aspects of life -- and it constitutes a great part of your performance in the committee room.

It is the joint effort of both the dais team and delegates to foster a collaborative and exciting

environment for everyone. Expand your horizons, engage in meaningful debates, and ultimately formulate a feasible and robust resolution to address one of IMO's key global issue that is growing in significance. We as dais members, do hope to see you come to the conference with an open-minded attitude and in a fighting spirit to debate, and leave with your joyful memories and experiences of new friends and insights.

Best Regards,

Julie Chen: sisterbigfish@163.com

Grace Cai : youyacai@outlook.com

Committee Introduction

The International Maritime Organization(IMO) is the United Nations specialized agency responsible for mainly the safety and security of shipping and the prevention of marine and atmospheric pollution by ships. Established in 1948 and headquartered in London, the IMO primarily develops and enforces regulatory frameworks that govern maritime operations worldwide. Its mission is to promote safe, efficient, and environmentally responsible maritime transport, facilitating cooperation between member states to address the challenges posed by international maritime trade.

The IMO's work is critical in safeguarding the interests of more than 170 member states, as maritime transport remains the backbone of global trade, accounting for over 80% of goods transported worldwide. The organization has developed numerous international conventions and agreements that set global standards for ship design, construction, operation, and disposal. Among its key accomplishments are the International Convention for the Safety of Life at Sea (SOLAS), which sets minimum safety standards for the construction, equipment, and operation of ships to ensure safety, and the International Convention for the Prevention of Pollution from Ships (MARPOL), which includes six regulations of harmful substances such as oil and sewage to minimize pollution from ships. These conventions form the bedrock of modern maritime regulation.

In recent years, the IMO has expanded its focus to address emerging issues such as climate change, cybersecurity, and autonomous shipping. The shipping industry's significant contribution to greenhouse gas emissions has driven the IMO to set ambitious targets for reducing carbon emissions through the adoption of innovative technologies and cleaner fuels. Additionally, the increasing reliance on digital systems in maritime operations has exposed vulnerabilities to cyber threats, prompting the IMO to develop robust guidelines to safeguard ships and ports from potential attacks. As it has been fifty years since the adoption of the SOLAS, on 1 November 1974, it is recognized that safety remains paramount in such a changing environment, whether it pertains to seafarers handling new green fuels, safeguarding passengers in the latest cruise ships, regulating AI-managed autonomous ships or ensuring cybersecurity in a digital world.

As a global regulatory body, the IMO plays a pivotal role in promoting international cooperation, ensuring maritime safety, and mitigating the environmental impact of shipping. In this committee, delegates will have the opportunity to discuss pressing maritime challenges and propose innovative solutions to improve the future of global shipping.

Topic Introduction

- **Preventing and Countering Maritime Cyber Attacks in Gulf of Guinea**

As Africa's maritime industry is undergoing rapid digital transformation, cyber security is becoming an integral aspect of Africa's maritime security needs. The escalating frequency of maritime cyberattacks has become a chief concern in the maritime industry. While the continuous digitalization and connectivity of maritime systems, vessels, and ports has noticeably enhanced operational efficiency and profitability, it exposes ports, communication systems and vessels to potential maritime cyber-attacks that will disrupt and disable key maritime infrastructures, often leading to significant operational disruptions, widespread supply chain ramifications, and even put lives at risk. A series of notable incidents have reflected the maritime sector's rowing susceptibility to cyberattacks. Cases such as the NotPetya ransomware attack on Danish corporation Maersk in 2017 crippled the company's information systems worldwide and resulted in financial losses of more than USD 300 million. Likewise, the cybercrime targeting the International Maritime Organization (IMO) in 2020 damaged the agency's website and intranet services. These incidents underscore the profound implications of cyberattacks, particularly in terms of sizable financial loss, disruption to operations, impact to reputation, and possible threats to security.

Maritime operational technology and fleet operations management technologies that applies automized navigation and communication systems are at risk of being compromised by cyberattacks, targeting systems such as vessel communications, management of cargo and ballast water, and engine monitoring and control. The average cost of such attacks rose 200% worldwide in 2024, resulting to more than $550,000 monetary lost per incident.

- **Managing Maritime Cyber Risk**

The IMO deems maritime cyber risk as "a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised." The IMO has detailed a series of functional guidelines on

maritime cyber security risk management that entails a universally adoptable approach to risk minimization:

1. Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

2. Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

3. Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

4. Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

5. Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

In the ever-changing contemporary maritime environment of GoG, the escalating menace of maritime cyber risks stands as a multifaceted challenge. Today, cybertechnologies are highly vulnerable to cybersecurity threats due to the accessing, interconnecting or networking of systems that can induce cyber risks which should be addressed. Systems of vulnerability could include but are not limited to:

1. Integrated Bridge systems – a combination of interconnected systems that allow a centralized monitoring of navigational tools. It enables acquiring and control of sensor information of various of operations such as passage execution, communication, machinery control, and safety and security

2. Cargo handling and management systems - is a set of equipment, technology, and processes applied to manage and monitor movement of cargo throughout the shipping process

3. Propulsion and machinery management and power control systems - determines the power consumption of the entire ship network

4. Access control systems - a series of devices that regulate access among visitors and employees within a port or vessel. It typically operates through a centralized control system

5. Passenger servicing and management systems - a system that facilitates crewmembers to manage all the passenger-related operations from ticketing to boarding

6. Passenger facing public networks – passengers exposed to digital operational system whether as a duty or not. Access to vital operational systems should be strictly regulated to minimize security risks

7. Administrative and crew welfare systems – a system designed to monitor and maintain the welfare of seafarers

8. Communication systems - technologies utilized by maritime platforms to facilitate effective coordination and communication both internally and externally. These systems could include radios, satellite communications (SATCOM), and etc.

In that sense, the IMO need to not only develop standardized management protocols in the maritime cyber security industry of GoG striving towards alignment and frameworks for feasible and universally applicable methodologies but also to facilitate surrounding countries' digitalization process to ensure transparent, reliable and sustainable maritime cybersecurity management and promote future innovations and green technology.

- **Topic Focus**

Africa's development goals are inextricably linked to the optimal functioning of its maritime industry as 90% of the continent's imports and exports are carried through maritime trade according to a report published by Institute for Security Studies; however, its maritime cybersecurity is vulnerable to external cyber-attacks due to the lack of collective maritime

cybersecurity management measures, limited regional efforts and the absence of adequate legislations and technology to implement preventative and counter maritime cyber-attack measures in an age of growing reliance to automation in the shipping industry. A cyber-attack of considerable scale and impact would prove devastating to especially the developing nations recovering from economic recession of COVID-19, therefore, it is imperative that the International Maritime Organization (IMO) provide further assistance to accelerate the integration of maritime cybersecurity management into African maritime security instruments and frameworks to prepare it for potential cyber-attacks.

Our discussion will center around African maritime industry situated along the Gulf of Guinea (GoG)— a vast region of the eastern tropical Atlantic Ocean covering around 6,000 kilometers of coast from Senegal to Angola who earned the reputation of most hazardous waters in the world due to its prevalent offshore crimes with piracy accounting for 95% of total global piracy encounters. It is only a matter of time before communication systems of essential African ports are compromised and corporations threatened by cyber extortion in the current state of the region's cybersecurity environment. Delegates will aid surrounding nations of the GoG in navigating their maritime cybersecurity landscape to identify vulnerabilities. This will be achieved by managing cyber risks in maritime systems through capacity building for African nations and organizations concerned.

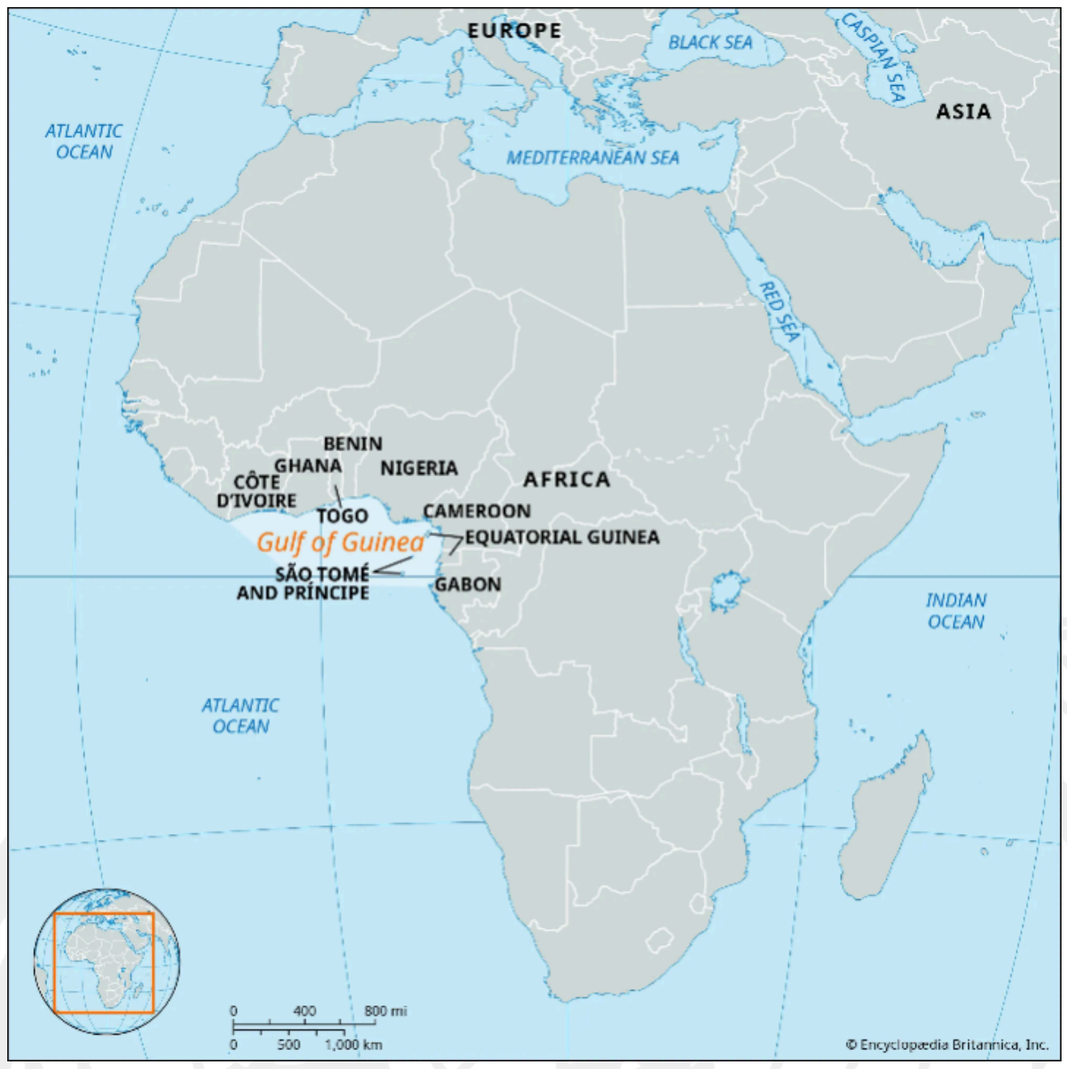
Sustainable Development Goal (SDG)

SDG 9 Industry, Innovation, and Infrastructure

Sustainable Development Goal (SDG) 9 pertains to the development of resilient infrastructure and the promoting of inclusive and sustainable industrialization and fostering innovation. In this topic, delegates of IMO will contribute to SDG 9 by facilitating countries of the Gulf of Guinea in their integration of new technologies such as autonomous ships and digitalized port sectors that are critical to the optimal functioning of the entire transportation sector vital to Africa and the world and, as a result, a primary driver for the delivery and achievement of several SDGs. Ultimately, ensuring Gulf of Guinea's maritime domain's safe and sustainable process of digitalization will be a major step to the stability of local economics and politics and a milestone on the global stage.

Current Situation

Gulf of Guinea (GoG)



The transition between operation and control systems and the information technologies in the maritime industry calls for the rethinking of threats, risks and vulnerabilities, as well as actors and perpetrators of crime. As a consequence of this process, the frequency of cyber-attacks is rising in number, targeting vital infrastructures and organizations.

The GoG, comprising of 16 countries in West and Central Africa, has experienced tremendous improvement in its maritime security institutions over the last five years as a result of both concentrated regional and international endeavors to combat traditional maritime crimes such as piracy, ransom, human-trafficking, and etc., building some of the world's most fortified and sophisticated sets of maritime security architecture. For example, according to the International Maritime Bureau (IMB) Piracy Report, the total number of reported piracy incidents narrowed to five in 2023, a great stride compared to its peak of 28 cases in 2020. Concurrently, however, the security menaces across West and Central Africa have continued to grow in complexity. Ironically, the region has become a victim of its own success: strengthened maritime policy implementation prompted criminals to innovate in their ways to illicit profit,

which is one of the reasons why its high maritime crime rate is projected to persist according to the United Nations.

GoG has hitherto encountered any reported cybercrime incidents. Nonetheless, this also highlights the need for formal monitoring systems to be developed for the maritime cybersecurity environment of GoG to ensure timely and accurate documentation.

Existing Relevant Legal Frameworks

At the apex of its maritime security framework is the 2013 Code of Conduct Concerning the Repression of Piracy, Armed Robbery against Ships, and Illicit Maritime Activity in West and Central Africa, regarded informally as the Yaoundé Code of Conduct, which catalyzed an intensive process of national, zonal, regional, and inter-regional advancements that continues to gain momentum to this day. As Article 2 of the Code states, “the Signatories intend to co-operate to the fullest possible extent in the repression of transnational organized crime in the maritime domain, maritime terrorism, IUU fishing, and other illegal activities at sea.” this salient initiative encouraged multi-sectoral and collaborative efforts among member states of GoG.

The chief governing body concerning the Yaoundé Code of Conduct is the Inter-regional Coordination Center (CIC) in Yaoundé. Its main role is to manage the operational, strategic, and political aspects of maritime safety and security in the GoG. CIC both coordinates and assists the development of the two regional centers, the five zones, and the 25 member states. Simultaneously, it is tasked with the responsibility of engaging both with international partner and national governments to construct political commitment and ensure the effective implementation of the GoG’s initiatives.

Effect of Current Operative Legal Frameworks and Organizations

Despite the extensive actions done in GoG, both previous and recent efforts failed to fully consider the maritime dimension of cybersecurity, thus, leaving the GoG unprepared for cyberattacks, a fast-approaching future due to the rapid digitalization of maritime infrastructures and the already high crime rate in the region. Other initiatives such as the African Union

Convention on Cyber Security and Personal Data Protection (Malabo Convention) have justified Africa's need to reinforce its cybersecurity management measures; however, its influence is constrained by lack of awareness on the issue, regional disputes that discourages harmonized policies, and financial constraints to fully comply to the measures.

Despite the reliance of GoG states on the maritime industry and access to a vast number of marine resources, land-based conflicts have remained the focus of member states. For instance, the African Charter on Maritime Security and Safety and Development (Lomé Charter) is a legally binding document that serves as AU's fundamental architecture for maritime security. The scope of the Charter only extended to maritime crimes listed under the SUA (Suppression of Unlawful Acts against the Safety of Maritime Navigation) Convention and refers to violations unincluded in the convention as 'other unlawful acts' at sea. Although the inclusion of other unlawful acts presents a leeway for the Charter to be understood as appliable to cybercrimes, regulations on cybercrime are insufficient in comparison to other aspects of maritime security. The Charter also calls for the harmonization of national laws of member states to comply to international legal instruments. While mentioning these factors, it is also notable that the Charter is yet to come into force and some of its major functions are pending extensive discussions before being included as the nineth annex of Charter, none of which, as they currently stand, address the issue of cybersecurity.

Financial Constraints

Gulf of Guinea Commission (GGC) is a regional institution established in 2001 that aims to allow closer coordination among member states and resolve issues such as maritime security. The organization was criticized for its lack of relevancy and inaction in current issues such as maritime crimes and other regional disputes. As a response, the Strategy for the Revitalization of the Gulf of Guinea Commission was produced to detail areas of improvement of the commission in its role in the region's maritime peace, security, and development framework. However, this initiative is yet to make effect due to the constant reporting of insufficient funding for the commission.

An encouraging note is that these intensified challenges are no longer as insurmountable as ones were a decade ago. In 2018, at the recommendation of the Specialized Technical Committee on Communication and ICT, the AU Executive Council recognized the increasing significance of cybersecurity in achieving African development goals and included it as one of the projects of Agenda 2063. GoG now possess the foundation to take on the new challenges of maritime cybersecurity wherein prevailing legal frameworks and international alliances provide the platform for further developments in areas such as investment in security measures, employee training, cybersecurity network architecture, and collaboration with experts to safeguard preventative and counter cyber threat measures. With the unified effort of IMO members, states, zones, regions, and the interregional mechanisms will be able to explore ways of preventing and combating maritime cyberattacks.

Bloc Positions

Nigeria

Nigeria relys on the Gulf of Guinea for oil and trade and is undergoing rapid digital transformation, making it prime targets for economic disruption through cyberattacks. Therefore, Nigeria has been at the forefront of maritime cybersecurity efforts, with its Nigerian Maritime Administration and Safety Agency (NIMASA) focusing on integrating cyber risk management into broader maritime security strategies. The Nigerian Navy has also collaborated with international partners to improve port security and cyber resilience, often through training arranged with the U.S. Africa Command (AFRICOM) in areas including counter-privacy and maritime cybersecurity. On the other hand, the Yaoundé Code of Conduct adopted in June 2013, initially focused on combating piracy, is evolving to address cyber threats as well, promoting regional cooperation among all the Gulf states.

On the other hand, the nation is working on enhancing cybersecurity frameworks with help from organizations like the World Bank and the International Telecommunication Union (ITU). However, it still lacks the resources and advanced cybersecurity capabilities necessary to fully address the threat. Thus, it will likely advocate for increased technical assistance and capacity building from international partners, emphasizing the importance of safeguarding vital infrastructure while calling for foreign investment in cybersecurity capabilities. Such as more international funding and technical support from developed nations and private sector partners to establish cyber monitoring centers and improve port infrastructure security.

African Union

The African Union plays a crucial role in developing continental policies on cybersecurity and maritime security. Through initiatives like the African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), the AU seeks to create a cohesive legal and policy framework for addressing cyber threats across Africa. Another of AU's focus has been on facilitating collaboration between member states in maritime security, primarily through the 2050 Africa's Integrated Maritime Strategy (2050 AIMS) which highlights the need for maritime

domain awareness (MDA) and information-sharing platforms to detect and mitigate cyber threats. At the Gulf of Guinea level, the AU supports regional organizations such as the Economic Community of West African States (ECOWAS) in their efforts to coordinate a unified approach to maritime cyber threats.

However, as the implementation of these policies has been slow, only 15 out of 55 member states adopted the Malabo Convention, the AU is expected to push for more international funding and technological support, particularly from global powers, to make African maritime cybersecurity efforts more sustainable. AU member states still face significant challenges in harmonizing national cybersecurity efforts.

United States of America

The United States have substantial economic interests in ensuring safe and secure shipping routes through the Gulf of Guinea, as it is a key trade route for oil, gas, and other goods. The USA is concerned that cyberattacks could disrupt the flow of oil and goods, affecting not just African economies but global markets as well.

As such, the U.S. has worked to provide technical support, training, and threat intelligence to African nations. These include initiatives to promote cyber threat information-sharing and capacity building, for example, the U.S. Department of Homeland Security (DHS) has collaborated with African maritime authorities to improve the cybersecurity of port operations and shipping systems. It also supports the use of public-private partnerships, involving American companies like Maersk, which suffered a devastating cyberattack in 2017, to help African states fortify their maritime cyber defenses.

European Union

The European Union is highly invested in the security of the Gulf of Guinea due to its reliance on West African oil and its position as a vital shipping route to Europe.

The EU, through initiatives such as the Critical Maritime Routes in the Gulf of Guinea

(CRIMGO), which has focused on improving information-sharing systems between EU member states and Gulf of Guinea nations, aiming to establish real-time threat intelligence platforms that can detect and respond to cyber threats quickly. The EU also implemented the Coordinated Maritime Presence (CMP) to ensure that cyber risk management becomes part of standard maritime safety protocols by providing funding and technical assistance to West African nations to strengthen both traditional and cyber-related maritime security.

China

China is heavily invested in Africa, particularly through its Belt and Road Initiative (BRI), which includes the development of key ports and maritime infrastructure along the West African coast. China views the security of these investments as paramount and has begun to offer cybersecurity technology and expertise to African countries in the Gulf of Guinea.

China prefers to focus on bilateral agreements rather than participating in multilateral efforts led by Western countries, arranging formal meetings between only two countries, emphasizing the importance of African countries retaining sovereignty over their cybersecurity efforts. Technical support and cybersecurity hardware are often provided through Chinese firms like Huawei, which is known for assisting with port and communication systems in developing regions.

However, China's approach is often centered around promoting sovereignty over cyber policy, meaning that African countries are encouraged to adopt cybersecurity frameworks that are locally managed, with minimal external interference. China's involvement in the region is likely to grow as it seeks to protect its economic interests and ensure that its shipping routes are secure from both traditional and cyber threats.

Questions To Consider

1. How can the IMO mobilize relevant parties and resources to solve the issue?

2. How can current frameworks concerning cybersecurity in the Gulf of Guinea (GoG) be optimized? (Consider identifying possible vulnerabilities.)

3. What are the existing training and education centers in the maritime cybersecurity sector of GoG?

4. What are the potential tools or mechanisms that can be utilized to minimize maritime cybersecurity risk?

5. How can international partners aid GoG nations in leveraging relevant technologies in the most cost-effective way?

6. How can external technological support promote inter-regional harmonization?

7. To what extent have GoG countries adopted existing maritime cybersecurity management frameworks and policies?

8. Why are regional efforts to combat future maritime cyberattacks limited in GoG?

9. Do the impending cybersecurity threats demonstrate a path for maritime criminals (i.e. pirates, human-traffickers) to evolve into maritime cybercriminals?

10. To what extent should external intervention be implemented? (Consider the possibility of GoG nations being overdependent on external support and utilizing technologies and other forms of foreign aid unsustainably.)

For Further Research

- IMO’s strategic plan:

https://www.imo.org/en/About/Strategy/Pages/Default.aspx

- IMO and the Sustainable Development Goals:

https://www.imo.org/en/MediaCentre/HotTopics/Pages/SustainableDevelopmentGoals.aspx

- “Maritime Cyber Security: Getting Africa Ready” by Denys Reva:

Reva, Denys. Maritime Cyber Security. issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf.

- “Cyber Security Environment in The Gulf of Guinea” by Burak Şakir Şeker & Harun Abubakar Siddique:

Hasret Çomak, et al. Cyber Environment and International Politics. Transnational Press London, 2022.

Past and Recent Maritime Cybercrime Incidents:

- “Major Maritime Cybersecurity Incident Exposes Vulnerabilities | Offshore Cyber”: Offshore Cyber, 2024, www.offshorecyber.com/news/major-maritime-cybersecurity-incident-exposes-vulnerabilities. Accessed 16 Aug. 2024.

- “Cyber Attacks Expose the Vulnerability of South Africa’s Ports”:

ISSAfrica.org. “Cyber Attacks Expose the Vulnerability of South Africa’s Ports.” ISS Africa, 29 July 2021, issafrica.org/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports.

- Case Study 17: Port of Durban, South Africa | UNCTAD:

Resilientmaritimelogistics.unctad.org, resilientmaritimelogistics.unctad.org/guidebook/case-study-17-port-durban-south-africa.

Bibliography

Ancheta, Andrew. "International Maritime Organization (IMO): Definition and Purpose." Investopedia, 2 Jul. 2024, *www.investopedia.com/terms/i/international-maritime-organization.asp*.

"2024 World Maritime Day anchors focus on maritime safety" International Maritime Organization(IMO), 24 Sep, 2024.*www.imo.org/en/MediaCentre/PressBriefings/pages/2024-World-Maritime-Day-Safety.aspx*

“Cybersécurité Maritime : Préparer l’Afrique | ISS Africa.” ISS Africa, 2020, issafrica.org/fr/recherches/rapport-sur-lafrique/cybersecurite-maritime-preparer-lafrique. Accessed 15 Oct. 2024.

“Enhancing Maritime Domain Awareness in Africa | ISS Africa.” ISS Africa, 2015, issafrica.org/research/policy-brief/enhancing-maritime-domain-awareness-in-africa. Accessed 15 Oct. 2024.

I:\CIRC\MSC-FAL\1\MSC-FAL.1-Circ.3-Rev.2.Docx E 4 ALBERT EMBANKMENT LONDON SE1 7SR Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210. 2022, wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

“IMCSO - Maritime Cybersecurity.” Imcso.org, 2021, imcso.org/. Accessed 7 Oct. 2024.

“IMO and the Sustainable Development Goals.” Www.imo.org, www.imo.org/en/MediaCentre/HotTopics/Pages/SustainableDevelopmentGoals.aspx.

“Maritime Cyber Security: Getting Africa Ready | ISS Africa.” ISS Africa, 2020, issafrica.org/research/africa-report/maritime-cyber-security-getting-africa-ready. Accessed 15 Oct. 2024.

Bibliography

Reva, Denys. Maritime Cyber Security. issafrica.s3.amazonaws.com/site/uploads/ar-29-2.pdf. Accessed 7 Oct. 2024.

“Can the Gulf of Guinea Commission Step up to Maritime Threats? | ENACT Africa.” ENACT Africa, 2018, enactafrica.org/enact-observer/can-the-gulf-of-guinea-commission-step-up-to-maritime-threats. Accessed 15 Oct. 2024.

“Gulf of Guinea | Gulf, Atlantic Ocean | Britannica.” Encyclopædia Britannica, 2019, *www.britannica.com/place/Gulf-of-Guinea*.

“INTEGRATING NATO’S CYBERSECURITY and MARITIME STRATEGY: UPHOLDING the MONTREUX CONVENTION.” Avim.org.tr, 2023, avim.org.tr/en/Analiz/INTEGRATING-NATO-S-CYBERSECURITY-AND-MARITIME-STRATEGY-UPHOLDING-THE-MONTREUX-CONVENTION. Accessed 15 Oct. 2024.