Scientia Militaria
2023, VOL. 51, NO. 3, 89-112
DOI: 10.5787/51-3-1427

Investigating the Intersection of Maritime and Cyber Crime in the Gulf of Guinea

Elsie Amelia Tachie-Menson
Faculty of Academic Affairs and Research
Kofi Annan International Peacekeeping Training Centre

Abstract

As technology expands and spreads worldwide, the maritime industry and maritime crime are rapidly evolving While the heightened adoption of digital technologies has positively impacted the efficient and prompt execution of tasks like maritime surveillance, policing, monitoring, and early warning systems, it has also brought about significant challenges that impact the interconnected network of maritime actors. This dilemma can be attributed to geographical location, surveillance, and navigation systems of ports, vessels, and other state intuitions. With the emergence of cyber threats, West Africa is poised to face a dual-pronged threat at its ports and shores, affecting the broader security environment of coastal states as actors in the maritime domain are increasingly using digital technologies. Moreover, these threats demonstrate a path for maritime criminals to evolve into maritime cybercriminals.

The central theme of this article is the connection between cybercrime and maritime crimes, and the cybercrimes that have found a lucrative avenue in the maritime industry. It also discusses cybercrime in maritime criminal activities occurring in West Africa, and the implications for the maritime and cyber landscape of the region. Finally, the article concludes with approaches for dealing with the risks posed by maritime cyber risks.

Keywords: Maritime, Digital, Security, Cyber, Gulf of Guinea, Maritime Cybercrime.

Introduction

The Gulf of Guinea greatly relies on the maritime domain as a crucial lifeline that underpins economic development, regional integration, and prosperity for the coastal communities of West Africa. Significant maritime operations, such as oil exploration, shipping, and fishing, occur in the region. At the same time, over the past decade, maritime crimes have emerged and evolved in West Africa, with piracy, oil theft, and other criminal activities in the region posing an increasing danger to maritime security. With numerous actors – with varying roles to play in the various blue economies of West African states – maritime crime has progressed to become the most talked-about organised crime in the region.

At the same time, the development of technology has added a new dimension to the subject of security. As the globe becomes more interlinked, the interplay between cyber security and maritime security is becoming increasingly vital. The progressively increasing use

of digital devices and networks has brought about speed, ease and accessibility regarding communications and the use of various resources and services, but also presents new threats and vulnerabilities for the maritime sector.

The high prevalence of organised criminal activities at sea, coupled with the rising use of technology in maritime operations, could make the Gulf of Guinea a hotspot for cyber-enabled maritime crimes. A potential convergence of cybercrime and maritime crime in the Gulf of Guinea poses a substantial challenge to law enforcement authorities, shipping firms, and the maritime industry as a whole. This is accompanied by a disadvantage, which creates insecurities and compromises the safety of digitised activities for users and systems, while providing lucrative grounds for criminals who employ these networks in their criminal activities.

In this article, discussions will centre on cybercrimes, maritime crimes, as well as the repercussions of the nexus borne as the two crimes intersect. The study on which this article reports, examined the significance of a dual-dimensional approach for strategy, policymaking, and law enforcement in the region.

The next section provides a conceptual analysis of the motivations underlying both of the crimes mentioned. The subsequent discussion addresses cybercrime and maritime crime in a continuation of the discussion on how there has become an intersection point between the two types of crimes, as well as the way they exhibit similarities in modes of execution. Following this, the dynamics of the junction between these two crimes, as well as the dual-dimensional approach required to address maritime cybercrime, are considered. The article finishes with a list of suggested approaches that stakeholders may apply to address the growing trend in cybercrime.

The Rational Choice Approach and Organised Crime

The rational choice approach (RCA) provides the best explanation for why criminals conduct crimes despite the risks involved; the advantages of the illicit act outweigh the negative effects. People get upset, according to economists, when the subjective benefit-cost ratio exceeds what they perceive they will receive by spending the same amount of time and other resources on lawful activities (Mehlkop & Graeff, 2010: 190). Consequently, it varies with theories that assert crime is the result of a lack of self-control, differential affiliation, poor social relationships, tension, labelling, disadvantaged neighbourhoods, or other social experiences or causes. Due to its restrictive definition and conceptualisation of rationalisation, the idea has been met with scepticism although it has gained acceptance (Boudon, 1998: 821). According to White (2014), people are motivated to breach the law by biological, psychological, and social causes (Marongiu & Newman, 1997: 128).

In contrast to many other crime theories, the RCA discusses how people's preferences influence their decisions rather than explaining the source of their preferences.

Sociologists and political scientists, such as Browning, Halcli and Webster (2000: 126), presume that people are driven by money and the potential for profit, which allowed them to develop formal and frequently predictive models of human behaviour. After constructing a framework for the exchange theory based on behaviourist psychology assumptions, Homans (1961: 4) introduced the RCA. This idea is also known as the rational decision strategy (Homans, 1961: 4). Homans' concept has been embraced by later authors, whose arguments have drawn inspiration from Homans' concept notwithstanding the objections of other authors. Hollis (1987: 818) contends that the RCA "is an explanation of itself" (Boudon, 2003: 16). The application of the idea of sound choice to social interactions is characterised by reciprocity and mutuality (Coleman, 1990). The foundational assumptions of this theory are based on neo-classical economic, utilitarian, and game theories. *Leviathan*, by Thomas Hobbes, contains numerous fundamental ideas of rational decision. Hobbes believed that individuals are rational actors who pursue self-improvement regardless of the repercussions to others (Hobbes, 1984: 2). The RCA differs from other proposed theories in that it denies the reality of all actions other than those that are solely practical and wise (Scott, 2000: 126).

- In its entirety, the RCA assumes that:
- People have preferences for outcomes (goods, services, states of being, and so on); choices rarely refer to actions or behaviour;
- The expected benefits of an outcome influence people's preferences concerning its costs;
- The anticipated benefits of an outcome influence people's taste in comparison to its costs;
- People's attitudes toward time also have an influence on their preferences;
- Attitudes toward risk and uncertainty influence choices;
- Rational actions are those that are consistent with the assumptions stated above;
- The RCA does not preclude people from acting irrationally, and people may pursue a course of action that is contrary to their preferences for a variety of reasons;
- The RCA does not argue that people always think in ways that are commonly associated with rationality (e.g., reasoned, thoughtful, and reflection), neither does it assume that people perform literal calculations; and

The information people gather influences their assessments of the benefits and costs of outcomes. (Ruhl, 2023: 1).

Consequently, understanding this context allows law enforcement and policymakers to make better-informed decisions with regard to the prevention and suppression of crime (UNODC, n.d.; 1). Based on the RCA theory, changing the balance of the cost–benefit analysis by reducing the perceived profit and increasing risks could help reduce criminal activity. Within this context, it is also important to look at the definition of organised crime.

According to Gastrow, 'organised crime' refers to "major criminal offences committed by a criminal organisation that is founded on a structured association of more than two people acting in concert over an extended period of time in pursuit of both their illicit objectives and profits" (Gastrow, 2011: 42). Organised crime unit is defined by Interpol as

"any group with a corporate structure whose principal objective is to gain money through criminal operations, frequently thriving on fear or corruption." (Interpol, n.d.). Other definitions of organised crime may vary in specifics, but the vast majority incorporate some combination of the main characteristics stated in the 2010 United Nations Convention against Transnational Organized Crime (UNODC, n.d.: 1), such as human trafficking and smuggling and the trafficking of firearms and ammunition. Due to a lack of consensus among states regarding the definition of 'organised crime', (UNODC, n.d.: 1), defines it as "a structured group of three or more persons existing for some time and acting in concert to commit one or more serious crimes or offences established under the convention to obtain, directly or indirectly, financial or other material benefits". It also defines 'serious crimes' as "any offence punishable by a maximum term of imprisonment of at least four years or a more severe penalty" (United Nations Convention against Transnational Organized Crime, 2010: 2).

There are controversies because of two restrictions in the United Nations Convention against Transnational Organized Crime (UNTOC). The first concentrates on the notion of serious crime. This idea varies considerably throughout civilisations, and is heavily dependent on appropriate legalisation and criminalisation processes (Edwards & Levi, 2008: 366).

Second, the UNTOC definition of transnationality is restricted by its emphasis on two or more states. In other words, the offence must have occurred in multiple states. While transnational organised crime at sea happens regularly between states, it also encompasses crimes perpetrated within or between particular, partial, or shared state authority areas. As a result, the definitions and scope are flawed. These circumstances divide the discourse on organised crime and transnational organised crime.

The discourse on spaces and their regulation can have significant consequences for research questions, potentially leading to confusion and muddled inquiries. This impact extends to overall investigations and conversations within the academic realm. The complexity deepens as the discourse expands, introducing challenges related to the regulation of various spaces. (Griffin, 2021: 12).

In the context of the current study, the discourse explores the modern and worldwide extent of cyberspace, treating it as a shared place. This approach implies that the consequences observed in the cyber domain resonate with those in physical spaces, specifically the seas and waters of the maritime domain. The intertwining of cyberspace with the maritime domain introduces similar geographical difficulties, creating a complex landscape for researchers and policymakers to navigate.

Understanding the parallels between cyberspace and physical spaces is crucial for addressing the regulatory challenges and potential consequences that may arise. As the discourse continues to evolve, researchers must carefully consider the implications for research questions and methodologies to ensure a comprehensive understanding of the interplay between cyberspace and maritime environments. (Afenyo, Mawuli & Livingstone, 2023: 2).

Following on this section, the next section discusses cybercrime and maritime crime in the context of West Africa.

The case of cybercrime in West Africa

Internet usage and digitisation in West Africa have expanded over the past few years, as mobile device accessibility and connection have improved (Adeleye & Eboagu, 2019: 32). This trend has offered various chances for economic development and progress, but it has also led to an increase in cyber risks and vulnerabilities. When an increasing number of individuals and organisations in an area get online, they become potential targets for hackers looking to exploit vulnerabilities in their digital infrastructure. West Africa needs significant investments in cybersecurity awareness, education, and infrastructure to address these dangers. Data by the International Telecommunication Union (ITU) indicates that between 2019 and 2020, the number of internet users in West Africa increased by 10%, reaching 104 million people (ITU, 2020: 1).

Below is a matrix on internet penetration rates in West African countries, based on data from the World Bank as of September 2021:

Table 1: Respective internet penetration rates of West African states

Country	Internet penetration rate
Benin	35.2%
Burkina Faso	12.4%
Cabo Verde	72.2%
Cote d'Ivoire	46.1%
Gambia, The	33.6%
Ghana	45.1%
Guinea	18.8%
Guinea-Bissau	16.5%
Liberia	28.2%
Mali	11.4%
Mauritania	24.0%
Niger	6.8%
Nigeria	44.7%
Senegal	48.6%
Sierra Leone	38.6%
Togo	35.8%

Source: World Bank (2021)

This fast spread of internet connectivity in West Africa and the advancement of technology have facilitated the transmission, storage, and retrieval of data. However, According to Boakye (2021: 1), as per the 2021 Global Cybersecurity Index (GCI), West African countries, including Ghana, exhibit remarkable levels of cybersecurity readiness that are among the highest and fastest-growing globally (Boakye, 2021: 1). The current Ghanaian score of 86.69% shows major progress from the previous ratings in 2017 and 2018 of 32.6% and 43.7% respectively. Its third-place ranking in Africa is also a major leap from the eleventh place attained in the previous rating, and projects Ghana among the best in the region and globally (Boakye, 2021: 1).

Cybercrime has become one of the most urgent concerns of law enforcement globally. Generally, if cybercrime originates in the physical realm, it typically occurs in the digital landscape. 'Cybercrime' is a broad word referring to criminal activities in which computers or computer networks are utilised as a tool, goal, or location (Das & Nayak, 2013: 153). Cybercrime generally refers to criminal operations that take advantage of modern information technology, such as computers, networks, and the like. There are a variety of cybercrimes, including unauthorised access (such as hacking), unauthorised interception, data interference, system interference, device misuse, forgery (identity theft), electronic fraud, and ransomware (Moore, 2014: 49).

Understanding the nature of the different types of crimes and their repercussions is vital for conversation and inquiry that are more effective. Globally, cybercrimes such as fraud, hacking, cyberbullying, catfishing, spoofing (sexual), harassment, and phishing have happened (Zhang, Geng and Ha, 2020: 425). These crimes have harmed the lives of people regardless of their location.

While there are other crimes – such as victimisation of persons, child pornography, and catfishing – the above-mentioned crimes were the focus of the current study as these are related to the activities of the criminal actors in the cyberspace of the maritime domain.

Cyber fraud, which dates back to more than a decade ago, is commonly known as 'Sakawa' in Ghana, 'Yahoo-Yahoo' or '419' (so named because of the section number of Nigerian criminal legislation pertaining to it (Whitty, 2018: 106). Although these crimes are perpetrated in different ways, Attah-Asamoah (2009) categorises them into three stages: scouting and harvesting, relationship building and profiling, and operational (Atta-Asamoah, 2009: 110). Nigeria has been ranked as the number one state in the region for malicious internet activity (Aransiola & Asindemade, 2011: 761). In addition, in Jackson's overview of the 2013 Financial Action Task Force (FATF) report, he identified cyber fraud as a major source of terrorist financing for insurgent organisations and other operations throughout the West African sub-region and the world (Jackson, 2017: 7).

As the mechanics of these crimes continue to evolve, several West African nations have begun to implement crime-prevention programmes. The Economic Community of West African States (ECOWAS), Ghana, and Nigeria, among others, have worked to prevent and combat cybercrime through legislation, regulations, and public awareness initiatives (Boes & Leukfeldt, 2017:185). Ghana has enacted the 771 Electronic Transaction Act, for

instance (*Electronic Transactions Act*, 2008 (Act 772). In 2011, Nigeria hosted the first-ever West African cybercrime summit, which was attended by leaders from a variety of African nations and institutions, including Microsoft (Quarshie & Martin-Odoom, 2012: 98). In addition, Nigeria has made progress in institutionalising measures against these crimes, serving as an example for other regional states.

Governments and enterprises in West Africa must adopt a proactive stance to address the cybersecurity threats posed by increasing digitisation and internet use in the region. This involves investing in cybersecurity education and training, installing contemporary cybersecurity technologies, and establishing cybersecurity rules and laws. In addition, coordination between nations in West Africa and international partners is essential for building a coordinated response to cyber threats (World Bank, 2021: 1).

The case of maritime crime in West Africa

The Gulf of Guinea greatly relies on the maritime domain as a crucial lifeline that underpins economic development, regional integration, and prosperity for the coastal communities of West Africa. While it is a lucrative route for the flow of food, trade, and travel, criminals have found its lucrativeness accessible; therefore, criminal activities in many bodies of water around the world.

Between 1991 and 2012, there were a total of 734 pirate attacks in the region, with Nigeria responsible for 335 incidents (representing 46% of the total) (Onuoha, 2013: 273). Forty per cent of reported piracy occurrences in 2020 took place in the Gulf of Guinea, or 81 out of 195 incidents worldwide (IMB, 2021: 1). According to research undertaken by the United Nations Office on Drugs and Crime (UNODC) and Stable Seas, ransom payments to pirate gangs in the Gulf produce almost $5 million each year (UN Security Council [UNSC], 2022: 1). According to the report, piracy costs twelve Gulf of Guinea nations $1.925 billion annually in lost trade (UNSC, 2022: 1).

Despite an overall drop in global piracy during 2021, threat levels in the region remain high (IMB, 2021). Only twelve maritime incidences were recorded in the first half of 2022, compared to twenty-three in the same period of 2021 (International Chamber of Commerce-International Maritime Bureau [ICC-IMB], 2022: 1). The sharp decline in reported piracy and other sea crimes is a result of the combined efforts of some West African member states and international communities (IMB, 2021: 1). It has decreased substantially in 2021 but still poses threatening situations for the blue economies[1] of various West African states (Statista, 2023, n.d: 1).

In addition to posing a threat to the safety and security of seafarers, these crimes have substantial economic effects on the maritime sector and the area as a whole. Many factors, including ineffective law enforcement, political instability, and poverty, contribute to the high rate of crime in the Gulf of Guinea (Oceans Beyond Piracy, 2020: 1).

[1] Blue Economies are a contemporary economic development paradigm focusing on the sustainable utilisation of ocean resources for economic growth, job creation, and improved livelihoods while preserving marine ecosystem health. See <https://www.lse.ac.uk/granthaminstitute/explainers/what-is-the-role-of-the-blue-economy-in-a-sustainable-future/>

It is essential to highlight that authors, along with global donors and institutions, have underscored maritime piracy as the most prevalent naval crime in the region. Simultaneously, in both the broader region and individual states, other maritime offenses, including, in certain instances, piracy, demand scrutiny and focus. This situation has resulted in a significant gap in the availability of data and publications on other maritime crimes in the area.

In countries, such as Togo and Nigeria, illegal, unregulated, and unreported (IUU) fishing crimes characterise the waterways (Okafor-Yarwood, 2019: 414). Aning, Birikorang, Pokoo, Mensah & Tachie-Menson (2021: 2) refer to this issue as they discuss the case of Ghana, where IUU fishing crimes, as the most frequently occurring maritime crimes are overshadowed by piracy, with which global media and donors agree. While this is one of the major setbacks of addressing maritime crime in West Africa, it creates antiquatedness in knowledge emanating from maritime research in West Africa. Jacobsen (2022: 135) also discusses the prioritisation of piracy over other maritime crimes, which are more prevalent than piracy.

In this regard, maritime security is one of the most recent additions to the international security lexicon. Since the year 2000 and the rise of contemporary piracy off the coast of Somalia and elsewhere, the notion of maritime security has garnered increasing attention. The term was initially coined in the 1990s. Consequently, the highest levels of international policymaking are focusing increasingly on maritime crimes (Bueger & Edmunds, 2020: 2). On 5 February 2019, the UNSC convened its first-ever discussion on "transnational organised crime at sea as a threat to international peace and security" (United Nations Security Council, 2019: 1).

Various authors, including Bueger and Edmunds (2017), have scrutinised the UNTOC framework, pointing out limitations in its definition of severe crime. According to Bueger and Edmunds (2017: 3): Firstly, the emphasis on the state as a constraint is deemed insufficient in addressing the broad scope of maritime crimes; and secondly, the statement suggests that the UNTOC framework "takes serious crime as a given," referring to one or more serious crimes or offenses punishable at the threshold specified in Article 2 of the UNTOC Convention. The high seas are, by definition, a shared-sovereignty international environment in which the state is only one among many actors. The characteristics of maritime space are comparable to those of cyberspace. Koops and Galic (2017: 26), for example, have conceptualised space and place, including digital space or place. In practice, however, it is a diverse and unpredictable environment that unearths difficulties when questions of territoriality and jurisdiction arise. Similarly, to maritime space, cyberspace has become a necessity for a variety of global entities with a variety of applications, including illegal ones.

In this context, the management of maritime insecurity must inevitably involve a variety of actors and agendas, including those of the involved littoral states, local communities and fishermen, flag states, international shipping or fishing interests, resource extraction, and tourism industries, and, in some instances, private security firms. "Wherever seafarers go, maritime criminals will follow," wrote Rediker (1989: 21) just over three decades ago,

and it still holds true. In the Indian Ocean, piracy has been almost abolished, but it is on the rise in the Gulf of Guinea. Despite growing international awareness of maritime crime in the region (Osinowo, 2015:14), the number of other naval crimes has steadily climbed over the past several years (United Nations [UN], 2019: 1), with a considerable increase in 2018. Human trafficking on the high seas is one of the maritime crimes linked to the increasing importance of the blue economy and maritime environmental protection and resource management problems. The discussion is based on the Blue Seas classification of Bueger and Edmunds, which divides maritime crimes into crimes against mobility, illicit flows of persons and things, and crimes against nature (Bueger & Edmunds, 2017: 3).

As per the aforementioned classification scheme, Table 2 below provides a concise summary of the numerous offences.

Table 2: Classification of blue crimes

	Crimes against mobility	**Criminal flows**	**Environmental crimes**
Relation to the sea	On the sea	Across the sea	In the sea
An ideal type of object	Ships and ports	Societies and communities	Nature and installations
Sub-categories	• Kidnap and ransom Ship and/or cargo seizure • Robbery and theft • Crimes in and against ports • Stowaways • Cyber crimes	• People smuggling • Human trafficking • Small arms and light weapons, and weapons of mass destruction • Narcotics • Illicit goods • Counterfeits • Wildlife • Waste	• Fisheries crimes • Pollution • Illegal mining and/or resource extraction • Crimes against critical infrastructure • Crimes against cultural heritage
Forms of harm and victims	• Maritime trade • Supply chains • Seafarers • Coastal economies • Port facilities	• Formal economy • Public health • Environmental destruction • Trafficked persons • National security	• Environmental destruction • Biodiversity • The legitimate coastal economy of coastal livelihoods • Food security
Cross-cutting facilitating activities	Bribery, blackmail, corruption, slavery, forced and child labour, insurance, cargo theft, document fraud, money laundering, obstruction of justice, and other forms of support for criminal groups.		

Source: Bueger and Edmunds (2017)

The matrix above was proposed by Bueger and Edmunds (2017: 2) in an attempt to conceptualising organised crime at sea. The discussions in the next section focus on the aspects that are relevant to the cybercrime–maritime crime intersection and how it is operationalised. The mapping of the various maritime crimes, which have a cyber component, are highlighted as part of the discussion in Figure 2 below.

With the surge in digital technological advances, industries and institutions, including the maritime industry, have adopted digital components in their activities and processes. Actors in the maritime domain use digital devices and software in geolocation, for tracking vessels, keeping records, and monitoring persons and vessels alike. This has created a lucrative alternative and/or additional chance for maritime criminals to creep into the various maritime networks. This paper seeks to bring to light that the intersection borne out of this fusion is that of cybercrimes, when safety and security in these digital networks are breached and compromised, effecting insecurity due to the utilisation of these technologies and networks in the maritime domain. While these crimes are not synonymous, their machinations are alike, and this is discussed later in this article.

Crimes targeting mobility, supply chains, vessels, and ports exploit sophisticated software and digital technologies, rendering them vulnerable to network breaches and illicit activities. The challenge at ports extends beyond thwarting intruders; it encompasses the capability to operate equipment and ensure its ongoing safety and security. In essence, even a secure network could face compromise if inadequate resources hinder the establishment of robust defenses, thereby posing security concerns even in the absence of cybercriminals.

West Africa is an important region for the maritime supply chain, which plays a crucial role in international trade (see United Nations Council on Trade and Development (UNCTAD, 2022). Cyber threats are not immune to the marine supply chain and port infrastructure in West Africa. Cyber risks in marine supply chains and threats at port facilities in West Africa are growing, and it is essential to comprehend these risks to mitigate them effectively.

According to the International Association of Ports and Harbours (IAPH, 2021: 1), supply chains are intricate processes involving multiple parties, such as ship owners, port operators, cargo owners, goods forwarders, and customs officials. Using digital technologies and networked systems has rendered the maritime supply chain susceptible to cyberattacks. Cyberattacks against vessel navigation systems, cargo-tracking systems, and port management systems are among the cyber risks in maritime supply chains (Androjna *et al*. 2020: 776).

A cyberattack on any of these systems has the potential to disrupt the entire supply chain, causing considerable economic harm and impeding international trade (Terra Nova Security, 2023: 1). Supply chain attacks are on the rise, with 45% of respondents in CrowdStrike's 2021 Global Security Attitude Survey suffering a supply chain attack within the last 12 months. (Benjer, 2023: 1)

The occurrence of such an incident in West Africa could lead to a significant escalation of instability and insecurity across the entire region. This is due to West Africa's pivotal role in international trade, with its port facilities being crucial to the regional economy.

Yet, West African port infrastructure is susceptible to cyberattacks. Cyberattacks on cargo tracking and scanning systems, vessel navigation systems, and port management systems are among the threats posed to West African port infrastructure (International Maritime Organization (IMO, 2021: 1). These attacks have the potential to interrupt the entire supply chain, resulting in substantial economic losses. In addition, the lack of sufficient cybersecurity protections at West African port facilities makes these facilities an accessible target for fraudsters. Cyber risk components are included in the maritime security strategies of both Ghana and Nigeria. Apart from this being a desirable addition, it also reveals the readiness of some West African states to confront the concerns discussed here.

The hybridised emerging crime resulting from the convergence of maritime crimes and cybercrime could produce a dual-dimensional threat to the regional security in the Gulf of Guinea (GoG). Existing crimes in the digital and maritime realms offer new dynamics for the blue economy at the junction of cyber and maritime crimes in the region. These crimes interact not just because their mechanisms are similar, but also because the commonalities between them promote a hybridised type of criminal activity: maritime cybercrimes.

In the context of the emerging nexus, and in line with the RCA mentioned above, the insufficiency of cyber laws and maritime laws in West Africa creates gaps that can be exploited by criminals. If cybercrime is a pandemic, and maritime crime is a growing concern, then the combination of the two offers a significant risk not only to users of digitisation technology but also to individuals and networks in cyberspace and diversified blue economies.

The maritime cyber- (in)security nexus in the context of the Gulf of Guinea

In several ways, the relationship between cybersecurity and maritime security is clear. Cybersecurity is vital in the maritime industry to avoid cyberattacks on ships, ports, and other key infrastructure. For example, a cyberattack on a shipping corporation might result in supply chain interruption, cargo theft, and financial loss. While this nexus is not a new phenomenon globally or in Africa, in West Africa, it marks a new development in the maritime sector as well as the cybersecurity domain.

As this paper underlines a crucial feature of the influence of digital technology is the establishment of dynamic, real-time linkages between disparate sites. Because the maritime sector is often sea-locked and cut off from land, technological advancements have proved to be extraordinarily efficient and successful (DiRenzo, Goward & Roberts, 2015: 4). Despite this, the presence of digitisation opens the door to digitally related crimes. There is a robust connection between cybercrime and some maritime offences in the maritime business. This connection shows the disadvantages of the utility of digital technology, as technology has become a necessity in practically every industry around the globe. In addition to computer systems, hardware and software, technology also encompasses larger platforms, such as ships and ports. At the junction of humans and computers or computer networks, the possibility of error, coercion, sedition and manipulation exists.

There have been several incidences of cyberattacks aboard ships, notably the 2017 Maersk cyberattack, which resulted in major financial losses for 17 shipping firms and 300 ports globally. The 2017 Maersk cyberattack was a devastating cyberattack that affected the global shipping industry. The attack was caused by the NotPetya ransomware, which locked users out of their systems and encrypted data until a ransom was paid. (Walton, 2022: 1). Maersk, the largest shipping container company in the world, was severely impacted, with its operations disrupted for two weeks. (Leovy, 2017: 1). The attack cost Maersk between $200 million and $300 million, and it took the company 10 days to rebuild its entire IT infrastructure. (Walton, 2022: 1).

There has been an upward trend in pirate incidents in the Gulf of Guinea, and there is rising worry that cyberattacks may be used to support these illegal operations. The diagram below illustrates the relationships between humans, information, and the technological networks that support the processing and exchange of information.

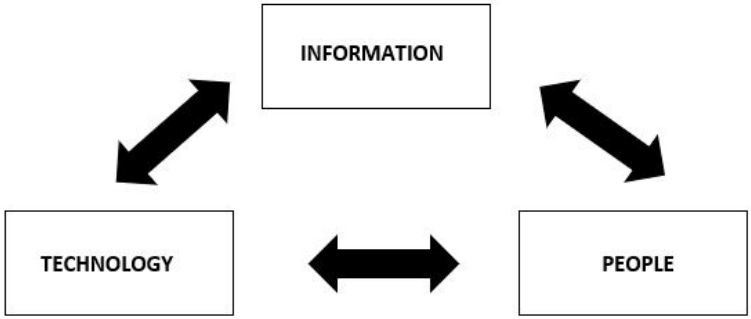

Figure 1: The three elements of cyber operations in the maritime domain

Source: Author's own construct

People

The use of technology to carry out criminal activities, such as piracy, smuggling, and fraud is referred to as 'maritime cybercrime'. The perpetrators of these crimes are frequently part of a larger network of transnational individuals and organisations, making it difficult to monitor and punish them.

The hacker or cybercriminal is an integral part of the maritime–cybercrime network. Using many methods, hackers gain unauthorised access to the systems on ships to steal data and disrupt operations. They may operate on their own or as members of a larger criminal organisation engaging in cybercrime on the high seas. These groups may be involved in a variety of illegal operations, such as drug trafficking, human smuggling, and arms trafficking. They frequently facilitate their other criminal operations through cybercrime.

The insider threat is another crucial component of the maritime–cybercrime network. Insiders are persons with authorised access to the systems on a ship who utilise such access for nefarious reasons. This may involve the theft of sensitive data or the sabotage of operations. Insiders can be crew members, contractors, or anybody else with access to the systems on board of ships.

Government agencies and law enforcement organisations are engaged in the fight against cybercrime in the maritime environment. In addition to identifying and prosecuting cybercriminals, these businesses build policies and procedures to avoid future cyberattacks.

Information

There is a constant flow of communication as a direct result of the increase in the number of people living on the globe and the spread of the internet.

In the area of digital technology, information has evolved into a formidable tool, and its significance in maritime research is steadily expanding (Det Norske Veritas Group, n.d.: 1). Before the emergence of digital technology, information, the interchange of information, and the transfer of information were already lucrative endeavours (Det Norske Veritas Group, n.d.: 1). Depending on the hands within which it lands at any given time, the exploitation of knowledge for either evil or altruistic purposes can result in powerful and advantageous outcomes. Everyone involved in the maritime business must have access to information regarding vessels and interconnected networks.

Technology

The maritime industry has embraced technology, with ships and ports relying on digital systems for navigation, cargo management, and communication. Unfortunately, these systems are susceptible to cyberattacks, which can result in substantial financial losses, environmental catastrophes, and endangering human lives. Cybersecurity experts have identified various potential cyberattack vectors in the marine industry, including communication systems, navigation systems, cargo management systems, and other important ship systems.

In recent years, the marine industry has been the target of numerous high-profile cyberattacks, notably the 2017 Maersk breach (Regalado, 2018: 1), which caused substantial disruption to shipping operations worldwide. In another case in 2019, a ransomware attack on a shipping company resulted in a ransom payment of almost $1 million (Cimpanu, 2019: 1). These instances demonstrate that the marine industry must upgrade its cybersecurity safeguards.

Many groups and efforts are attempting to improve cybersecurity in the maritime industry. The Singapore Maritime and Port Authority has established a Maritime Cybersecurity Operations Centre to monitor and respond to cyberattacks (Maritime and Port Authority of Singapore, n.d.). The International Maritime Organization (IMO) has issued regulations and guidelines for maritime cyber security. One key regulation is IMO Resolution

MSC.428(98), which came into force on January 1, 2021. This regulation is applicable to all vessels and requires ships to include cyber risk management in their safety management systems, in accordance with the International Safety Management (ISM) (IMO, n.d.: 1)

Computer networks are responsible for some of the most vital infrastructures in the world. Included are power, water supply, air traffic control, building control, transportation, and vessel traffic systems (VTS). Governments and government institutions require cyberattack protection for maritime transportation systems (MTS), automated identification system (AIS) systems, global positioning systems (GPS), and global navigation satellite systems (GNSS).

Not only vessels are susceptible to cyber assaults in the maritime environment. A problem could occur if a jamming attack occurred during a very complex manoeuvre demanding intense focus, such as docking in extremely poor light (Grant, Williams, Ward & Basker, 2009: 175, 176). Especially troubling is the fact that such GPS jamming can be done with inexpensive jammers that can be purchased online for as little as $20 per unit (albeit illegally). Cargo handling is essential to port operations, but it is not the only port system vulnerable to cyberattacks. For cargo tracking, check-in, and inspections, ports rely extensively on computer networks nowadays. In the maritime industry, these networks govern shipboard systems, oil rig activities, and other port operations. Spoofing attacks, i.e. by way of substituting signals or by superimposing deceptive signals on genuine satellite signal receptors are carried out (Günther, 2014: 159).

Even if the intersection between maritime and cybercrimes is not yet prominent in the sub-region of West Africa, it is crucial to investigate the possibility of it, and to discuss how its occurrence in other regions and states has been experienced and addressed.

A dual-dimensional approach to addressing maritime cybercrimes

Aning and Aubyn (2013:309) emphasise the importance of examining and bridging the gap between and among security risks in the West African sub-region. The IMO has a unified definition of maritime cyber threats, namely that it is the degree to which technological assets could be threatened by a potential circumstance or event that could result in maritime-related safety security failures due to information or systems being corrupted, lost, or compromised.

In 2017, the IMO and other organisations produced guidelines and suggestions for securing maritime infrastructure from cyber threats (Lagouvardou, 2018: 19). The overarching goal of IMO maritime cyber risk management is to ensure safe and secure shipping that is also operationally flexible in terms of cybercrimes. The guidelines, MSC-FAL.1/Circ. 3 (IMO, 2021: 1), give high-level recommendations for maritime cyber risk management to safeguard ships from existing and potential cyber threats and vulnerabilities, as well as functional aspects, to enable effective cyber risk management. In 2017, the ninetieth session of the Maritime Safety Committee (MSC) saw the adoption of the MSC.428(98) resolution, which encourages administrators to ensure that cyber threats are effectively addressed in existing safety management systems. In addition, functional aspects that aid

in the management of cyber hazards are included in the guidelines. Standardisations, such as ISO/IEC 27001 (International Organisation for Standardisation [ISO], 2013), were jointly produced by the ISO and the International Electrotechnical Commission (IEC).

Concerns over the applicability and adaptability of current conventions and regulations in various states pose challenges to their effectiveness in both the maritime and digital sectors. Disputes surrounding jurisdiction and territoriality render established standards and rules ineffectual. This issue becomes particularly pronounced in the convergence of crimes, where the common thread is the challenge of managing space and distinct governing powers in both domains. Creating an infrastructure that ensures the interconnected safeguarding of both maritime and digital terrains is crucial. In the discourse of territoriality and law, ungoverned areas emerge as hotspots for criminal activity and undetected crimes, further complicating the implementation of security measures. The complexities arise from the need to address concerns about applicability and adaptation in states with existing conventions and norms, making it imperative to navigate jurisdictional and territorial challenges in both the maritime and cyber security realms. In exploring maritime security challenges, it becomes apparent that predominant concerns center around deficiencies in management knowledge, a lack of information regarding cyber threats, a disproportionate focus on physical security, and inadequate cybersecurity training for workers (DiRenzo *et al*., 2015: 4). This analysis sheds light on the dual nature of technological innovation. While it generates numerous opportunities, it also introduces obstacles leading to the convergence of various crimes. Consequently, this indicates the potential emergence of a hybridized phenomenon affecting both land and sea.

Countries like Ghana have shown a significant interest in the development and implementation of cyber security policies. Despite this, it is essential to be aware of the numerous other industries or sectors that require specialised cyber laws and safeguards. Numerous programmes and projects have been developed in response to all of these challenges in an effort to reduce insecurity in the region. Since the United Nations Security Council passed Resolution 2039 in February 2012 condemning acts of piracy in the Gulf of Guinea, more than a decade has passed.

In 2022, Ghana and Norway led negotiations on the first Security Council resolution on maritime security in the Gulf of Guinea in ten years. The resolution, numbered 2634, was adopted on May 31, 2022, and called upon member states in the Gulf of Guinea region to criminalize piracy and armed robbery at sea under their domestic laws, and to investigate, prosecute or extradite, in accordance with applicable international law, perpetrators of such crimes, as well as those who incite, finance or intentionally facilitate them. Spearheaded by Ghana and Norway to bring renewed attention to piracy and armed robbery in the Gulf of Guinea, the negotiations were drawn out, but not because of notable differences between members over how to address Gulf of Guinea piracy. Instead, the main dispute was over how to refer to the UN Convention on the Law of the Sea (UNCLOS). The United Nations General Assembly enacted Resolution 2634 in May 2022, making maritime piracy and violent robbery at sea illegal, although, by definition both are criminal.

Nonetheless, it remains crucial to develop a comprehensive plan that accounts for the rise of maritime crimes, including the exploitation of digital networks and linkages. As the digital technology and maritime industries continue to develop and undergo rapid expansion, crimes, opportunities, and potential security flaws will become more obvious (Security Council Report, 2022: 1).

States, donors, and all other concerned parties must pay careful thought to the combination of these two separate phenomena – maritime crimes and cybercrimes – and the potential repercussions if wide and specific measures are not taken. If measures are not put in place, a merger between cybercrime and maritime crime is conceivable.

The establishment of the Maritime Trade Information Sharing Centre for the Gulf of Guinea (MTISC-GoG) in 2014 is also a noteworthy initiative. The MTISC-GoG seeks to strengthen maritime security by giving shipping businesses operating in the region quick and reliable information on potential security risks (International Chamber of Shipping: 2014: 1).

To contribute to the above-mentioned interventions, some recommendations are provided that could be adopted to address the intersection between maritime crimes and cybercrimes in the West African sub-region:

- West African states and state institutions should enhance maritime situational awareness.
- There should be an established integrated maritime domain awareness system that incorporates cybersecurity considerations to enhance real-time situational awareness and intelligence sharing among maritime stakeholders.
- States and port authorities should strengthen port cybersecurity. They should endeavour to develop and enforce cybersecurity standards and protocols for respective ports in the Gulf of Guinea to prevent cyberattacks on critical infrastructure, including vessels, cargo, and port operations.
- States and agencies need to enhance maritime law enforcement. These stakeholders should enhance capacity building and training of maritime law enforcement personnel to detect, prevent, and respond to cyber-enabled maritime crimes, including piracy and cyber-enabled theft of cargo and vessel hijacking.
- Improvement in information sharing and collaboration among state institutions and regional intuitions are required. Agencies should establish partnerships among maritime stakeholders – including governments, law enforcement agencies, the private sector, and international organisations – to share information and collaborate in addressing maritime and cybersecurity threats.
- Stakeholders should explore and adopt emerging technologies in an attempt to address maritime cyber insecurities. They could employ emerging technologies, such as blockchain, artificial intelligence (AI), and the Internet of Things (IoT), to enhance maritime security and cybersecurity in the Gulf of Guinea. Although these come along with other vulnerabilities, it is expedient to explore the option and highlight the benefits that they elucidate.

- States and agencies must develop cybersecurity awareness campaigns to develop and implement cybersecurity awareness initiatives targeting maritime stakeholders – including ship owners, port operators, and seafarers – to enhance their knowledge and skills in preventing and responding to cyberattacks.
- West African states and agencies must develop and enforce new regulatory frameworks in addition to existing ones thus, promoting better cybersecurity in the maritime sector, including mandatory reporting of cyber incidents, and the establishment of cybersecurity incident response teams.
- While addressing issues on the dark web[2] could be daunting, states must endeavour to enhance their monitoring and intelligence-gathering capabilities to detect and thwart illicit activities. This may involve investing in advanced analytics and machine learning technology capable of detecting illicit activity on the dark web. To gain a better knowledge of criminal networks and their operations, authorities should strengthen collaboration and information sharing between states, agencies, and the corporate sector.
- Authorities and governments must further adopt and execute international policies and regulations to prevent marine criminal activity, including the use of the dark web.
- Governments and port facilities in West Africa should employ stringent cybersecurity measures to safeguard their systems and data against cyber threats. Firewalls, anti-virus software, intrusion detection systems, and routine security audits are examples of such methods. Port facilities in West Africa should adopt a comprehensive cybersecurity strategy that describes the roles and responsibilities of all stakeholders in the management of cyber hazards.
- It should be mandatory for all parties participating in the maritime supply chain to attend cybersecurity training to increase their awareness of cyber hazards, ways to identify such hazards and ways to minimise the hazards.
- Port facilities across West Africa should engage among themselves and with other stakeholders to exchange threat intelligence and maintain awareness of evolving cyber risks.

While these suggestions are not exhaustive they are explorable with regard to the discussions in this article.

---

[2] The dark web is a part of the World Wide Web that exists on darknets, which are overlay networks that require specific software, configurations, or authorization to access. It is a subset of the deep web and is not indexed by search engines. The dark web is often associated with anonymity and is used for both legal and illegal activities. Available at: <https://theconversation.com/what-is-the-dark-web-and-how-does-it-work-63613> [Accessed 1 December 2023].

Conclusion

The connection between cyber security and maritime security is essential for safeguarding the safety and security of maritime activities, especially in the Gulf of Guinea. Cyberattacks might be used to promote piracy and other illicit activities, necessitating the implementation of a comprehensive cyber security architecture. This article should act as a clarion call for increased awareness of cyber security training among maritime sector academics, professionals, and donor organisations, in addition to shipping companies and port authorities. Threats to maritime security have several facets, including instability, asymmetries, the potential for rapid escalation, and global ramifications. Current legislation and processes are undergoing a process of modernisation to place greater emphasis on the physical aspects of maritime security. Even if migration and urbanisation continue unabatedly, the oceans will remain crucial to the running of international commerce. It is vital to approach the creation of policies and the implementation of interventions from two distinct perspectives, as numerous types of crime could occur, such as cybercrimes committed by ambulatory individuals, and maritime crimes. As a result, it is essential to acknowledge that maritime crimes could occur. Concerning maritime cyber hazards and cybercrimes in the sub-region of West Africa, there is little doubt that a global and regional approach is necessary. Consequently, cyber security and maritime security should be considered as mutually reinforcing, with a robust cyber security framework essential for boosting maritime security.

About the Author

Elsie Amelia Tachie-Menson is a Researcher at the Faculty of Academic Affairs and Research (FAAR) within the esteemed Kofi Annan International Peacekeeping Training Centre (KAIPTC) located in Accra, Ghana. Over the past six years, her research has been dedicated to the realms of cybersecurity, and for the last four years, she has delved into the critical field of Maritime Security Studies. She earned her Bachelor of Science degree in Environment and Development Studies from Central University, Ghana, as a beneficiary of the prestigious MasterCard Scholarship. Currently, Elsie is on the verge of completing her Master of Arts in Gender, Peace, and Security at KAIPTC, demonstrating her commitment to academic excellence. In her capacity, she actively participates in policy dialogues and consultations with influential institutions, including but not limited to the African Union, the European Union, ECOWAS, NATO, MasterCard Foundation, Campaign for Female Education (CAMFED), UNDP, as well as various think tanks. These engagements revolve around issues concerning policy development and social advancement.

References

Adeleye, N., & Eboagu, C., 2019. Evaluation of ICT development and economic growth in Africa. NETNOMICS: Economic Research and Electronic Networking, 20(1), 31-53.

Afenyo, Mawuli & Caesar, Livingstone. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management. 10.1016/j.ocecoaman.2023.106493.

Androjna, A., Brcko, T., Pavic, I. and Greidanus, H., 2020. Assessing cyber challenges of maritime navigation. *Journal of Marine Science and Engineering*, *8*(10), 776.

Aning, E. K., Birikorang, E., Pokoo, J., Mensah, A., & Tachie-Menson, E. A., 2021. Maritime Insecurity in the Gulf of Guinea: Ghana's actual maritime crime picture. Available at: Safe Seas: Available at:<http://www.safeseas.net/maritime-insecurity-in-the-gulf-of-guinea-ghanas-actual-maritime-crime-picture/>[Accessed 1 December 2023]

Aning, K. and Aubyn, F., 2013. Bridging the Capacity Gaps to meet West Africa's Security Challenges. '*Strategie und Sicherheit'*, 2013(1). https://doi.org/10.7767/sus-2013-0128.

Aransiola, J.O. and Asindemade, S.O., 2011. Understanding Cyber crime Perpetrators and the Strategies They Employ in Nigeria. *Cyberpsychology, Behavior, and Social Networking*, 14(12), 759–763. https://doi.org/10.1089/cyber.2010.0307.

Atta-Asamoah, A., 2009. Understanding the West African cyber crime process. *African Security Review*, 18(4), 105–114. https://doi.org/10.1080/10246029.2009.9627562.

Beccaria, C., Newman, G. and Marongiu, P., 2009. On crimes and punishments. (New Brunswick: Transaction Publishers).

Bender J., 2023. Supply Chain Cyberattacks on the Rise: What Your SMB Needs to Know. Business News Daily. (20 October). Available at: <https://www.businessnewsdaily.com/supply-chain/smb-cyberattacks> [Accessed 3 December 2023].

Boakye E.A. 2021. Ghana ranked third in Africa on Global Cybersecurity Index Available at: <https://citinewsroom.com/2021/07/ghana-ranked-third-in-africa-on-global-cybersecurity-index/> [Accessed 3 December 2023].

Boes, S. and Leukfeldt, E.R., 2017. Fighting cybercrime: A joint effort. *Cyber-physical security: Protecting critical infrastructure at the state and local level*, in Clark, R., Hakim, S. (eds.) Cyber-Physical Security. Protecting Critical Infrastructure, vol 3. (Springer:Cham), 185-203.

White, M.D., 2014. On Beccaria, the Economics of Crime, and the Philosophy of Punishment. *Philosophical Inquiries*, *2*(2), 121-137.

Boudon, R., 1998. Limitations of Rational Choice Theory. *American Journal of Sociology*, 104(3), 817–828. https://doi.org/10.1086/210087.

Boudon, R., 2003. Beyond Rational Choice Theory. *Annual Review of Sociology*, 29(1), 1–21. https://doi.org/10.1146/annurev.soc.29.010202.100213.

Browning, G.K., Halcli, A. and Webster, F., 2000. Understanding Contemporary Society: Theories of the Present. (London; Thousand Oaks, Calif.: Sage), 26–136.

Bueger, C. and Edmunds, T. 2017. Beyond sea blindness: a new agenda for maritime security studies. *International Affairs*, 93(6), 1293–1311. https://doi.org/10.1093/ia/iix174.

Bueger, C. and Edmunds, T., 2020. Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy*, 119, 104067.

Cimpanu, C. 2019, August 22. Ransomware hits US Maritime facility. ZDNet. Available at: <https://www.zdnet.com/article/ransomware-hits-us-maritime-facility/> [Accessed 1 December 2023].

DiRenzo, J., Goward, D.A. and Roberts, F.S. 2015. The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), 1–5.

Det Norske Veritas Group, n.d. Digitalisation in the maritime Industry. Available at: <https://www.dnv.com/maritime/insights/topics/digitalization-in-the-maritime-industry/index.html> [Accessed 1 December 2023].

Edwards, A. and Levi, M. 2008. Researching the organization of serious crimes. *Criminology & Criminal Justice*, 8(4), 363–388. https://doi.org/10.1177/1748895808097403.

Electronic Transactions Act, 2008 (ACT 772) Available at: <https://bcp.gov.gh/acc/registry/docs/ELECTRONIC%20TRANSACTIONS%20ACT,%202008%20(ACT%20772).pdf> [Accessed 3 December 2023].

Gastrow, P., 2011. Termites at work: Transnational organized crime and state erosion in Kenya. (New York: International Peace Institute).

Grant, A., Williams, P., Ward, N. and Basker, S., 2009. GPS Jamming and the Impact on Maritime Navigation. *Journal of Navigation*, 62(2), 173–187. https://doi.org/10.1017/s0373463308005213.

Griffin A.M., 2021 Maritime Cybersecurity Strategies for Information Technology Specialists, Available at: <https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?article=12685&context=dissertations> [Accessed 29 November 2023].

GSMA Intelligence, 2021. The Mobile Economy West Africa 2021. Available at: <https://www.gsmaintelligence.com/research/?file=2690b4a3b2d1da844db8ad372ee82c95&download> [User access only].

Günther, C., 2014. A Survey of Spoofing and Counter-Measures. *Navigation*, 61(3), 159–177. https://doi.org/10.1002/navi.65.

Hobbes, T., 1984. *Leviathan*, (Frankfurt a. M.: Suhrkamp).

Hollis, M., 1987. *The cunning of reason* (Cambridge:Cambridge University Press).

Homans, G.C., 1961. The humanities and the social sciences. *American Behavioral Scientist*, 4(8), 3-6.

ICS Shipping, 2014. Shipping Industry Releases Updated Anti-Piracy Guidelines on Gulf of Guinea Region. Available at: <https://www.ics-shipping.org/press-release/shipping-industry-releases-updated-anti-piracy-guidelines-on-gulf-of-guinea-region/> [Accessed 3 December 2023].

International Association of Classification Societies (n.d.) Recommendation on Cyber Resilience Contents, [online] Available at: <https://www.iacs.org.uk/download/10714> [Accessed 9 Sep. 2021].

International Association of Ports and Harbors., 2021. IAPH Cybersecurity Guidelines for Ports and Port Facilities. Version 1.0. Published 2 July.

International Chamber of Commerce-International Maritime Bureau July 12, 2022. Available at:<https://www.icc-ccs.org/index.php/1320-global-piracy-and-armed-robbery-incidents-at-lowest-level-in-decades> [Accessed on June 19, 2023].

International Maritime Bureau. 2021. Piracy and Armed Robbery against Ships: Annual Report 2020. Available at: <https://www.icc-ccs.org/piracy-reporting-centre/request-piracy-report> [Accessed 1 December 2023].

IMO, n.d. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 29 November 2023].

International Telecommunication Union., 2020. Measuring Digital Development: Facts and Figures 2020. Available at: <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx [Accessed 1 December 2023].

Interpol, n.d. Available at: <https://www.interpol.int/en/Crimes/Organized-crime> [Accessed 26 November 2023].

ISO., 2013. ISO/IEC 27001 Information security management. Available at: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed 16 Nov. 2021].

Jackson, J.K., 2017. The Financial Action Task Force: An Overview. Congressional Research Service. (March), 1-16.

Jacobsen, K.L., 2022. The Politics of Piracy Numbers: The Gulf of Guinea Case. In Bosica, R-L.; Ferreira, S and B. Ryann (eds.) *Routledge Handbook of Maritime Security* (Oxon: Routledge), 127-138.

James Samuel Coleman, 1990. *Foundations of social theory*. (Cambridge Mass: The Belknap Press of Harvard University Press).

Koops, B-J and M. Galič (2017), 'Conceptualising space and place: Lessons from geography for the debate on privacy in public', in: T. Timan, B.C. Newell & B.J. Koops (eds), *Privacy in Public Space: Conceptual and Regulatory Challenges* (Cheltenham: Edward Elgar), 19-46.

Lagouvardou, S., 2018. Maritime Cyber Security: concepts, problems and models. Unpublished Master thesis. Technical University of Denmark. Kongens Lyngby, Copenhagen.

Leovy, J. 2017, Cyberattack cost Maersk as much as $300 million and disrupted operations for 2 weeks. Los Angelos Times. 17 August. Available at: <https://www.latimes.com/business/la-fi-maersk-cyberattack-20170817-story.html> [Accessed 01 December 2023].

Marongiu, P., & Newman, G. R., 1997. Situational crime prevention and the utilitarian tradition. In G. Newman, R. V. Clarke, & S. G. Shoham (Eds.), *Rational choice and situational crime prevention* (Aldershot, U.K.: Ashgate), 115–135.

Mehlkop, G. and Graeff, P., 2010. Modelling a rational choice theory of criminal action: Subjective expected utilities, norms, and interactions. *Rationality and Society,* [online] 22(2), 189–222. https://doi.org/10.1177/1043463110364730.

Moore, R., 2014. Cybercrime: Investigating high-technology computer crime. (Oxon: Routledge).

Naylor, R.T. 2003.Towards a General Theory of Profit-Driven Crimes, *British Journal of Criminology*, vol. 43, no. 1, 81–101. https://doi.org/10.1093/bjc/43.1.81.

Ndlovu, M.D & Mpagalile, JJ 2017. Cybercrime laws in Africa: The need for updated legislation, *International Data Privacy Law*, 7(1), 71-89.

Nigerian Maritime Administration and Safety Agency (NIMASA) 2017, 'Suppression of Piracy and Other Maritime Offences Act 2019: Eplanatory Memorandum'. Available at: <https://rb.gy/hwxo1r> [Accessed 1 December 2023].

Oceans Beyond Piracy., 2020. The State of Maritime Piracy 2020. Available at: <https://obp.ngo/wp-content/uploads/2020/12/The-State-of-Maritime-Piracy-2020.pdf> [Accessed 1 December 2023].

Okafor-Yarwood, I., 2019. Illegal, unreported and unregulated fishing, and the complexities of the sustainable development goals (SDGs) for countries in the Gulf of Guinea. *Maritime Policy*, 99, 414–422. https://doi.org/10.1016/j.marpol.2017.09.016.

Onuoha, F. C., 2013. Piracy and Maritime Security in the Gulf of Guinea: Trends, Concerns, and Propositions, *The Journal of the Middle East and Afri*ca, 4(3), 267-293, https://doi.org/10.1080/21520844.2013.862767

Osinowo, A.A., 2015. Combating piracy in the Gulf of Guinea. Africa Center For Strategic Studies.

Quarshie, H.O. and Martin-Odoom, A., 2012. Fighting cybercrime in Africa. *Computer Science and Engineering*, 2(6), 98-100.

Rediker, M., 1989. Between the Devil and the Deep Blue Sea: merchant seamen, pirates and the Anglo-American maritime world, 1700-1750. (Cambridge: Cambridge University Press).

Regalado, A., 2018, August 2. The biggest cybersecurity crisis of 2017 was a ransomware outbreak you never heard of. MIT Technology Review. Available at: <https://www.technologyreview.com/2018/08/02/241208/the-biggest-cybersecurity-crisis-of-2017-was-a-ransomware-outbreak-you-never-heard-of/> [Membership only].

Ruhl, C., 2023 Rational Choice Theory In Sociology: Definition And Examples, Available at: <https://simplysociology.com/rational-choice-theory.html> [Accessed 1 December 2023].

Security Council Report, 2022. Monthly Forecast. Gulf of Guinea piracy. (31 October 2022). Available at: <https://www.securitycouncilreport.org/monthly-forecast/2022-11/gulf-of-guinea-piracy.php#:~:text=A%20December%202021%20study%20by,generated%20approximately%20%245%20million%20annually> [Accessed on May 28, 2023].

Statista, 2023. Piracy and robbery incidents in West Africa 2016-2021, (24 October). Available at: <https://www.statista.com/statistics/1123280/piracy-robbery-in-west-africa-timeline/#:~:text=The%20highest%20number%20of%20piracy,Africa%2C%20the%20lowest%20amount%20recorded> [Accessed 1 December 2023].

The London School of Economics and Political Science, 2023. What is the blue economy? Available at: <https://www.lse.ac.uk/granthaminstitute/explainers/what-is-the-role-of-the-blue-economy-in-a-sustainable-future/> [Accessed 3 December 2023].

Terra Nova Security, 2023. The chain reaction: Why cyber security in supply chain networks is critical. Available at: <https://terranovasecurity.com/blog/cyber-security-in-supply-chain/> [Accessed 3 December 2023].

United Nations, 2019. High Seas Crime Becoming More Sophisticated, Endangering Lives, International Security, Speakers Tell Security Council | Meetings Coverage and Press Releases. Available at: https://www.un.org/press/en/2019/sc13691.doc.html> [Accessed 14 November 2021].

United Nations Security Council (UNSC), 2019. Letter dated 31 January 2019 from the Permanent Representative of Equatorial Guinea to the United Nations addressed to the Secretary-General. (31 January). Available at: <https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_98.pdf> [Accessed on February 23, 2023].

United Nations Security Council. 2022. Situation of piracy and armed robbery at sea in the Gulf of Guinea and its underlying causes. (1 November). Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/666/09/PDF/N2266609.pdf?OpenElement> [Accessed 1 December 2023].

United Nations Office on Drugs and Crime. 2021. United Nations. 2004. United Nations Convention against Transnational Organized Crime and the Protocols thereto. Available at: <https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf> [Accessed 1 December 2023].

UNODC, n.d. United Nations Convention against Transnational Organized Crime and the Protocols Thereto Available at: <https://www.unodc.org/unodc/en/organized-crime/intro/UNTOC.html> [Accessed 3 December 2023].

Walton H. 2022. The Maersk Cyber Attack - How Malware Can Hit Companies Of All Sizes. Kordia, (11 September). Available at: <https://www.kordia.co.nz/news-and-views/the-maersk-cyber-attack> [Accessed 1 December 2023].

Whitty, M.T., 2018. Do you love me? Psychological characteristics of romance scam victims. *Cyberpsychology, behavior, and social networking*, 21(2), 105-109.

World Bank. 2021. World Development Indicators 2020. Available at: <https://databank.worldbank.org/reports.aspx?source=world-development-indicators> [Accessed 1 December 2023]

Shasha, Z.T., Geng, Y., Sun, H.P., Musakwa, W. and Sun, L., 2020. Past, current, and future perspectives on eco-tourism: A bibliometric review between 2001 and 2018. *Environmental Science and Pollution Research*, 27, 23514-23528.