Scientia Militaria
2023, VOL. 51, NO. 3, 1-88
DOI: 10.5787/51-3-1426

A Critical Reflection on African Maritime Cybersecurity Frameworks

Tefesehet Hailu Sime
Amani Africa Media and Research Services

Abstract

With a coastline of 26,000 nautical miles and 38 out of 55 African states being either coastal or island states, trading activities on the continent are facilitated by over a hundred port facilities in the region, which make up 90 per cent of African seaborne trade. These factors indicate that the continent is dependent on well-run ports, effective protection of its maritime resources, and regulated shipping. Regulating the maritime sector requires new technologies that come at the cost of cyber vulnerabilities. However, in Africa, there are very few legal instruments, both at national and at regional level, specifically addressing the issue of cyberattacks on ships and port facilities.

Given the lack of attention given to maritime security and the lack of collective action from African states, the study on which this article reports, sought to provide a critical reflection on how cyber technology is affecting is affecting the African maritime domain; and the consequences that could manifest should the cybersecurity of ships, ports, and their critical infrastructure continue to be ignored.

The aim of this study was to broaden the understanding of the maritime cybersecurity legal frameworks in Africa by using the 'black letter' methodology, which is a positivist approach described by academics as being the best avenue by which to assess the existence, meaning and application of a defined system of legal principles. In engaging with those conventions, policies, laws, and regulations that are currently guiding the area of maritime cybersecurity, the study sought to identify the gaps in the legal frameworks on the continent and to provide policy recommendations.

Keywords: maritime cybersecurity, Africa, cybercrime, African Union, regulatory framework

Introduction

It is readily apparent that the ever-evolving technological landscape as well as the increasing digitisation, automation, and operational integration in the maritime sector has made the industry vulnerable to cyber threats. The fact that maritime transport is the backbone of international trade and the global economy makes it even more susceptible to cyberattacks. It is because of this importance that cyberattacks have become the premier threat to ports, vessels, shipping companies, and shipbuilding companies in recent years (SAFETY4SEA, 2018). To make matters worse, already existing maritime crimes, such as

piracy and drug trafficking, are being assisted by cybercriminals who are seeking to access sensitive data related to vessel movements and cargo according to a report in the *E&T (Engineering and Technology*) magazine (Bateman, 2013; Newman, 2019; Pasternack, 2013). Nevertheless, such attacks are not always successful, as there have been rare instances where institutions have utilised resilient cybersecurity management systems.

Cyber resilience is needed to enable companies to safely benefit from interconnected information systems, automated ships and offshore operations. Given the growing threat of cyberattacks and the need to create the necessary resilience, different regulations are also being adopted at regional, national, and international level. There are also commercial requirements being introduced to reduce the financial risks associated with cyberattacks, and since 2018, cybersecurity is being evaluated just as any other part of commercial contracts (DNV-Maritime, 2020). This vigilance observed elsewhere does not match the reaction by and preparedness of African states to deal with this piercing issue. However, according to the United Nations Economic and Social Council (ECOSOC) (2009), 92 per cent of African external trade is maritime-based; thus, it is time for the continent to start building a robust cybersecurity management framework.

Another factor necessitating such a framework is the establishment of the Common African Market under the African Continental Free Trade Agreement (also called the AfCFTA agreement) (AU, 2018a), which is expected to boost intra-African and international trade (AU, 2018). With the AfCFTA coming into effect, it was expected that there would be new developments in maritime transport, which would increasingly require new technologies (Reva, 2020). Moreover, with the subsequent construction of new ports and the expansion of existing ports throughout Africa, the Agreement would make the continent even more dependent on well-run ports, regulated shipping, and effective protection of its maritime resources.

Keeping the above factors in mind, the study on which this article reports, explored the threats and consequences of cybersecurity attacks associated with the maritime sector. The study also analysed the United Nations Convention on the Law of the Sea (UNCLOS), as well as the International Maritime Organization (IMO) instruments dealing with maritime cybersecurity. Furthermore, the article presents an assessment of the cyber vulnerability of the African maritime sector by reviewing the legal instruments adopted by the African Union (AU), the Regional Economic Communities (RECs), and the national legislations of African states. Lastly, the article provides conclusions and recommendations to create a robust cybersecurity framework in Africa.

Cyberattacks as a maritime security threat

Although the innovation of ships has undergone centuries of development, sea navigation first started with the use of goat skins to float on water (see Hornell, 1942). Unlike today, sailors in the ancient times used instruments, such as quadrants and astrolabes, in order to use nature to navigate the seas and ultimately reach their destinations (see Bennett, 2017). Today, the industry has come a long way in improving the design of ships, their navigation capabilities, and their interconnected communication with ports as well as off-shore companies (see Safe Seas, Safe Shores, 2018).

Besides human curiosity and the need to establish new colonies and settlements around the world, the most important reason for the development of ships and their navigation capabilities was the desire to find faster trading routes (see Formula, 2019). While the design of a ship, its navigation system and communication instruments continue to improve, what has not changed is the dependency of global trade on maritime transport. In fact, maritime transport currently accounts for nearly 80 per cent of the global trade (UNCTAD, 2018).

It is hard to think of the constantly growing maritime trade without considering the new technologies that seek to enhance operational efficiency and increase the profitability of the maritime industry. This interdependence not only makes maritime trade and technology inseparable, but also pushes the industry to rely heavily on technology. In this regard, although the introduction of the Electronic Chart Display and Information System (ECDIS), the Global Maritime Distress and Safety System (GMDSS), the Global Positioning System (GPS), cloud computing, and artificial intelligence has brought opportunities to the maritime sector, they have also aggravated the risks associated with its cybersecurity.

These technological developments that sought to enhance the navigation safety and security of a ship as well as onshore infrastructures have also increased vulnerabilities (see Akpan et al., 2022). Such electronic systems were made mandatory through different IMO instruments. The operation of an automatic identification system (AIS) became mandatory for all ships from 31 December 2004 under regulation 19(2) of Chapter V ("Safety of Navigation") of the 1980 International Convention for Safety of Life at Sea (SOLAS Convention 1980) (IMO, 1980). Under the same chapter, vessels are required to be equipped with an ECDIS as a computer-based alternative to paper-based navigation charts. Although these instruments are useful for enhancing maritime safety, researchers have also identified repeated and significant flaws in the GPS, AIS and ECDIS systems (Androjna, Perkovič, Pavic & Mišković, 2021). From the assessment of reports about incidents, it can be observed that cybercriminals continue to take advantage of those weaknesses that are associated with navigation systems, safety systems, engine control, and monitoring systems, as well as mooring and ballast water systems (Kochetkova, 2015; O'Dwyer, 2020; Pasternack, 2013; SAFETY4SEA, 2018).

In light of this, the Fair play, BIMCO[1] and ABS Advanced Solutions (2018) Maritime Cyber Survey (2018) found that the navigation systems of ships scored 86 per cent in the rating of the most vulnerable to a cyber threat, followed by the score of the safety system of a ship at 46 per cent. The World Economic Forum (WEF) also reported in its Global Risks Report (2020) that cyberattacks on critical infrastructure, such as shipping, were rated as the fifth biggest risk in 2019 (WEF, 2020). Additionally, there have been 310 reported cyberattacks on ships and ports in 2019, which was a sharp increase from the estimated 120 attacks in 2018, and 50 in 2017 (see Fair Play et al., 2018). Although it was expected by a Naval Dome cybersecurity expert, Robert Rizika, that the number of cyberattacks would exceed 500 in 2020, it was later reported by the Israeli cybersecurity specialist agency

[1] BIMCO = Baltic and International Maritime Council

Naval Dome itself that there had been a 400 per cent increase in attempted hacks since February 2020 (Ovcina, 2020). It was further stated by Naval Dome that the COVID-19 pandemic also contributed to the already existing risks associated with cybersecurity, as people were forced to work from home, and subsequent network access adjustments due to travel restrictions made them more vulnerable to malware attack (Jeffrey, 2020).

It is important to note that, although such cyberattacks are orchestrated via different means, they mostly rely on the lack of training of the crew of a ship as well as the insufficient data protection systems of their victims. Mostly, the attackers gain access to the system or data by 'phishing', which could be done via e-mail, fake websites, or by installing malware. In some instances, the malware attachment or the download link presented by the malware will infect the information technology (IT) system if opened or if the link is clicked, whilst in other instances, the crew will be led through trustworthy-appearing websites to install malware or to submit sensitive or personal data. Case in point is the 2017 Svitzer, where the company was a victim of data theft of over 5 000 e-mails, resulting in the redirecting of personal data to outside addresses and affecting more than 400 employees (Bogle, 2018).

The crew's lack of awareness could also lead to a ransomware attack, which could result in operational interference and the encrypting of the IT system on the ship. Once a malware file attached to an e-mail is accessed by the user, the ransomware could result in denying access to important documents as well as key operational systems. To recover from such restrictions and to regain access to such files or even the system, a ransom might be required. This was the case of Carnival Corp, the world's largest cruise line operator (Cimpanu, 2020).

Cybercriminals also use other methods that target the crew of a ship or port facility staff, which are beyond the control of the crew, most notable jamming the GPS to disrupt the navigation system of the ship and transferring erroneous information to shore-based operating systems. Given its possible consequences, *Fortune* magazine characterised GPS jamming incidents as "a disaster waiting to happen" to the global shipping industry (see Dunn, 2020:n.p.). The dangers of cybercrimes were practically seen in 2014, when Somali pirates were assisted in targeting their victims by using navigational data found online, leading vessels to either to use fake data, so it looked as if they were somewhere else, or to turn off the GPS signal of the ship entirely (Wagstaff, 2014). This gave rise to a different set of security threats for ships at sea and those responsible for their safety and security, such as phishing, ransom or spyware and distributed denial of services.

Hence, given the prevalence of maritime cyber-attacks and the diverse methods that are employed, the industry needs to take serious measures in order to tackle cyber related challenges.

UNCLOS and the SUA Convention

During the earlier negotiations in terms of UNCLOS, the internet was not considered a feasible alternative to traditional modes of warfare and terrorism. As a result, the focus of the Third United Nations Conference on the Law of the Sea conference (1973–1982) inclined towards considering piracy as a major maritime security threat.

When reading the definition of piracy under the UNCLOS, one may wonder whether the definition may also be implemented in a manner that seeks to regulate cybercrimes in the maritime domain. It is therefore important to study the meaning of piracy within those provisions of the UNCLOS that are considered to reflect customary international law (UN, 1982). Article 101 of UNCLOS stipulates that, for an act to be considered piracy:

- there must be an illegal act of violence, detention or depredation;
- the act must be committed for private ends by the crew or the passengers of a private ship or a private aircraft;
- two ships or aircraft must be involved; and
- the act must be committed on the high seas or outside the jurisdiction of any state (Attard, Fitzmaurice, Hamza & Martinez, 2017).

In assessing the above article in the light of cyberattack incidents in the previous decade (i.e. 2010–2019), it is clear that a cyberattack is an illegal act of violence or depredation that can also be committed for private ends. That means that two elements of the definition of piracy could exist in the case of a cybercrime incident, namely violence and depredation. Nevertheless, given that a vessel or a port facility may be targeted by a cybercriminal with only a computer and the right skills from any part of the world, the third and fourth elements of the above definition may not always be fulfilled.

In contrast to UNCLOS, the Convention for the Suppression of Unlawful Acts against the Safety of Navigation (i.e. the SUA Convention) provides for a broader regulatory scope that could be used to regulate and penalise cyberattacks in the maritime domain, as it criminalises offences which do not fall within the definition of piracy under the UNCLOS (Triantafillou, Bardaka Vrettakos & Zombanakis, 2023). When adopting the SUA Convention in 1988, the aim was to address the persisting issues of terrorism and piracy, as well as armed robbery at sea, and its scope has since been broadened by the Protocol of 2005 to the SUA Convention (IMO, 2005, which incorporated accessory offences and offences committed on fixed platforms located on the continental shelf. Due to the difficulties in defining these terminologies, the 1988 SUA Convention does not explicitly use the terminologies. Instead, it uses the term ‘unlawful acts’, which covers both the crime of piracy and maritime terrorism.

A broad interpretation of those elements of crimes that are provided under article 3 of the SUA Convention may be applicable to cybercrimes. For instance, although the provision, which states, “an unlawful act committed with the intention to seize or exercise control over a ship” (UN, 1988). The SUA Convention, art. 3(1)(a) was intended to apply to terrorist acts, it could also be applicable to cybercrimes under those circumstances where a cyber attacker unlawfully and intentionally seizes a ship or directs it to a specific location.

Additionally, if a person "commits an unlawful act with the intention to interfere with the ship's navigation and endangers the safe navigation of a ship" (SUA Convention, art. 3(1)(b)) (UN, 1988), such act will also be considered a crime under the SUA Convention. Even though this provision was not intended to penalise cybercrimes specifically, it could be deemed to apply if a person unlawfully and intentionally attacks the navigational systems of a ship or interferes with or deactivates its AIS, thereby taking control of the ship via a cyberattack (Tanti-Dougall, 2020).

Similarly, it is considered to be a crime "where a person places or causes to be placed on a ship, by any means whatsoever, a device or substance that may endanger or is likely to endanger the safe navigation of that ship" (art. 3(1)(b) (UN, 1988). The phrase 'placing a device' could be interpreted as referring to a bomb, but the word 'device' could also mean any destructive program or chip that allows the attacker to have complete control over the system of the victim. Furthermore, when the drafters of the Convention included the phrase "communication of a false information which is known to be false that endangers the safe navigation of a ship" in art. 3(1)(f) of the SUA Convention, it is hard to contend that they legislated with cybercrimes in mind (UN, 1988).

Considering the wider scope of the SUA Convention explained above, it can be broadly interpreted and be implemented in the case of a cyberattack. In other words, as long as the act falls within the parameters of the offences provided under any of articles 3a–3d of the SUA Convention, cybercrime can be considered an 'unlawful act'. The listed criminal offences under these provisions nevertheless require implementation through national legislation by state parties (James & Raul, 2013).

Of note here is that, unless the offender or the alleged offender is found in the territory of a state party, the incident must occur while the ship is navigating either outside the internal waters or in the territorial sea of a state in order for it to be a criminal offence under the SUA Convention. In such cases, the "state parties are required to establish jurisdiction over the offences committed against or on board a ship flying the flag of the State at the time the offence is committed; or in the territory of that State, including its territorial sea; or by a national of that State" (SUA Convention, art. 6(1)) (UN, 1988). Moreover, when reading the provisions of the SUA Convention dealing with jurisdiction, one can observe that the Convention aims to remove those listed offences from the exclusive jurisdiction of the flag state and allow them to be tried in another contracting state. To this end, the SUA Convention allows a state party to establish its jurisdiction over any offence when –

- such offence is committed by a stateless person whose habitual residence is in that state; or
- during its commission, a national of that state is seized, threatened, injured or killed; or
- the offence is committed in an attempt to compel such state to do or abstain from doing any act.

However, such an assessment should not be considered to be in contradiction to the principle of universal jurisdiction, as the effect of those provisions of the SUA Convention relating to jurisdiction is limited to state parties to the Convention (Hespen, 2016). In

this respect, the Convention puts a positive obligation on state parties either to extradite or to prosecute alleged criminals (see UN, 1988).

IMO Maritime Cybersecurity Regulatory Framework

In the international sphere, the concern for maritime cybersecurity began in 2014 when the IMO considered a proposal to develop voluntary guidelines on cybersecurity practices (IMO, 2014). Subsequently, the IMO adopted the Interim Guidelines on Cyber Risk Management in 2016 (IMO, 2016). In 2017, the interim guidelines were superseded by the IMO Guidelines on Maritime Cyber Risk management. The 2017 Guidelines aim to provide high-level recommendations on maritime cyber risk management in order to facilitate and support safe and secure shipping that is operationally resilient to current and emerging cyber threats and vulnerabilities (IMO, 2017a). In seeking to achieve these objectives, the Guidelines encourages the embedment of a cyber risk awareness culture into all levels of an organisation whilst recommending a holistic and flexible cyber risk management regime that is constantly being evaluated.

In an attempt to make the cyber risk management regime effective and to enhance the cyber risk management framework, the 2017 Guidelines gives recognition to those best practices that seek to provide detailed guidance regarding the implementation of maritime cyber risk management (IMO, 2017a). The recognised practices include:

- the United States National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (the NIST Framework) (NIST, 2017);
- the ISO/IEC 27001 standard on information technology (International Organization for Standardization [ISO], 2017); and
- the BIMCO Guidelines on Cybersecurity On-board Ships (BIMCO, 2020.

Moreover, the IMO Guidelines on Maritime Cyber Risk management suggest the incorporation of key recommendations into existing risk management processes as well as the use of the Guidelines as a complementary instrument to the already established safety and security management practices of the IMO. Amongst those already established safety and security management practices, the main pillar is the International Ships and Port Facilities Security Code (ISPS), which was subsequently incorporated in 2002 under Chapter XI-2 of the SOLAS Convention of 1980 as those special measures that seek to enhance maritime cybersecurity. The ISPS Code is applicable to passenger ships, cargo ships, as well as ships engaged in mobile offshore drilling, port facility serving, and international voyages (IMO, 2002). The Code is also applicable to high-speed passenger crafts and high-speed crafts of 500 gross tonnage. It is also important to note that the reason for its inclusion in SOLAS was to recognise the role of port facilities in maritime security and the need to define mandatory requirements and recommendations that ships and port facilities must follow (Drougkas, Sarri, Kyranoudi & Zisi, 2019).

Besides the Guidelines, the IMO has also adopted Maritime Safety Committee (MSC) Resolution 428(98) (IMO, 2017a) on maritime cyber risk management in safety management systems, which encourages flag states[2] to compel companies to treat cybersecurity management at company level through a safety management system (SMS) as per the requirement provided under the International Safety Management (ISM) Code (Mraković & Vujinoć, 2019). 'Company' is defined under the ISM Code as the owner of the ship or any other organisation or person, such as the manager, or the bareboat charterer,[3] who has assumed the responsibility for operation of the ship from the shipowner and who, on assuming such responsibility, has agreed to take over all the duties and responsibility imposed by the Code (IMO, 1993). As an enforcement mechanism, the Resolution 428(98) also provides a deadline for the requirement to be fulfilled, namely 1 January 2021 (IMO, 2017c). Accordingly, for companies to achieve the compliance that is required by the IMO, they should have assessed their cyber risk exposure before the deadline, and should have implemented those measures that seek to reduce and monitor cyber risks to shipping operations (IMO, 2017c). If companies fail to implement the required measures, their ships could be detained by port state control (PSC), and given that the deadline had passed, such companies would face the first annual verification of the company's document of compliance (Mraković & Vujinoć, 2019).

Overall, it is safe to say that the international IMO cyber risk management framework requires ships and port facilities to have cyber risk management plans and procedures that complement the existing security risk management requirements of both the ISM as well as the ISPS Code.

Cyber threats and vulnerabilities in Africa

With the level of attention that was given to maritime security in the past decade (i.e. 2010–2019), one would assume that there would be enough literature to assess the cyber vulnerability of the maritime domain in Africa. Unfortunately, the only available comprehensive document on the issue of maritime cybersecurity in Africa is the report published by the Institute for Security Studies (ISS) (see Reva, 2020), which highlights the lack of cybersecurity preparedness in the African maritime sector, a sentiment that is also echoed in the title of the report (see Reva, 2020). The report also highlights the lack of Africa-specific research and knowledge on maritime cybersecurity.

The strategic importance of maritime transport for the continent is an already established fact (Kahyarara & Simon, 2018). There is therefore a need for preparation to minimise the risk of a cyber-attack that is likely to target port facilities in particular and the shipping industry in general. So far, except for a cyberattack incident on Transnet, a South African state-owned enterprise in 2021 (see Shabalala & Heiberg, 2021), no cyber incidents that have targeted the maritime industry in Africa have been reported (Reva, 2021). In this

---

2 A flag state is "a state whose flag a ship flies and is entitled to fly" (see *UN 1986, art. 2*).

3 A bareboat charterer is "a contract for the lease of a ship, for a stipulated period of time, by virtue of which the lessee has complete possession and control of the ship, including the right to appoint the master and crew of the ship, for the duration of the lease" (see *UN 1986, art. 2*).

regard, it might be necessary to refer to the 2018 Fair play, BIMCO and ABS Survey, which states that 50 per cent of information regarding cyber incidents have not been shared (BIMCO, 2018). This could mean that there might be unreported cases or cyber phishing incidents that have occurred on the continent but that have gone unnoticed. Taking this into consideration, the maritime cyber incidents that have happened around the globe should alert the African maritime sector and should increase the level of preparedness on the continent by way of further research as well as by implementing important minimum guidelines.

It is also important to take into consideration that, in the hope of improving the poor port efficiency and the inadequate port infrastructure found in Africa, ports on the continent are also being highly influenced by those technologies that are trending across the globe. Transformation of ports is, for instance, being realised through increasingly sizeable investments, the growth of major economic powers, the involvement of private international operators, as well as the emergence of world-class ports (Maury & Féligonde, 2020). Additionally, private investments in African ports totalled $15bn between 2005 and 2019 and public investments amounted to more than $85bn (African Container Shipping, 2021). The heavy Chinese involvement in those port development projects on the continent should also be noted, as China has been supporting the development of 46 ports in sub-Saharan Africa financially, operationally, and technically from 2011–2017 (Devermont, Cheatham & Chiang, 2019). These new technological developments run the risk of further exasperating the vulnerability of the maritime sector unless key cybersecurity measures are taken.

Another factor that is worth considering is the continental project that aims to create a single continental market for goods and services via a comprehensive agreement between member states of the African Union (AU). In addition, the launching of the Belt and Road Initiative (BRI) in 2013 added another piece to the puzzle. The BRI seeks to encourage trade between China and the rest of the world, and is planned to connect points in both the northern and eastern regions of Africa. When the actual operation of the initiative starts, pre-existing protests against the Chinese workforce who are seen as mistreating nationals of the countries where the Chinese are operating could further spread to the maritime sector causing vulnerabilities to non-state actors (Lokanathan, 2020).

In terms of future vulnerabilities in the African maritime sector, landlocked states are also facing imminent vulnerabilities, as the volume of maritime transport on the continent is dominated by a few countries (Rosenberg, 2019). For instance, if major operating ports, such as Tangier (Morocco), Durban (South Africa) or Port Said (Egypt) are targeted by a cyberattack (Maury & Féligonde, 2020), landlocked states that are highly dependent on the ports of these coastal states will also be greatly affected. In particular, landlocked states are greatly affected by geopolitics, as they are not only dependent on political relations with the transit states,[4] but they also rely on peace and stability within such transit states. Transit states can take measures of blocking borders and adopting regulatory impediments to trade if the landlocked states and their transit states are in conflict (Faye,

[4] A transit state is a state with or without a sea coast, situated between a land-locked state and the sea, through whose territory 'traffic in transit' passes (UN, 1965).

McArthur, Sachs & Snow, 2004). According to McArthur (cited in Faye *et al*., 2004), Ethiopia has encountered major difficulties as a result of conflicts with its neighbouring nation, Eritrea. These conflicts have restricted Ethiopian access to the Eritrean port of Assab, which played a critical role in facilitating three-quarters (75 per cent) of its trade without tariffs until 1997.

Although the high seas are open to all nations, including landlocked nations, these rights may face significant practical constraints in such geopolitical scenarios. In a nutshell, the practical implementation of the rights of landlocked states depends on the relations, agreements, and/or the political will of the transit states (Bayehu, 2015).

The African Union Convention on Cybersecurity and Personal Data Protection

The development of continental regulatory initiatives on cybersecurity began in November 2009, after the commitment made by AU ministers in charge of information and communication technology (ICT) in the Oliver Tambo Declaration (AU, 2009). The Declaration requested the African Union Commission (AUC) to "jointly develop with the United Nations Economic Commission for Africa (UNECA), under the framework of the African Information Society Initiative, a convention on cyber legislation …" (AU, 2009: n.p.). Consequently, after passing through consultations, regional workshops that engaged a wide range of African stakeholders as well as different AU Policy Organs, the AU Convention on Cybersecurity and Personal Data Protection (hereafter the Malabo Convention) was adopted on 27 June 2014 at the 23rd ordinary Session of the summit of the AU in Malabo, Equatorial Guinea.

Beyond aiming to harmonise the laws of African states on electronic commerce, data protection, cybersecurity promotion and cybercrime control, the Malabo Convention also seeks to set forth those essential security rules that would not only establish a credible digital environment, but which would also strengthen the existing ICT legislations of AU member states and those of the RECs (see AU, 2014c: art.1–3).

Without addressing the pertinent issues of maritime cybersecurity directly and specifically, the Malabo Convention adopted a holistic approach to cybersecurity governance by imposing obligations on member states to establish, on a national level, those legal, policy and institutional mechanisms related to cybersecurity. In its holistic approach, the Malabo Convention gives a broad definition of 'critical information infrastructure' as "cyber infrastructure that is essential to vital services for public safety, economic stability, national security, international stability, and for the sustainability and restoration of critical cyberspace" (AU, 2014c: art. 1). This definition can also incorporate the maritime sector, as it is considered essential for economic stability, national security, as well as international stability. One could therefore argue that the obligations that are imposed on member states with regard to critical information infrastructures under the Malabo Convention could also be applicable to the maritime sector, as the Convention does not explicitly identify those sectors that should be regarded 'essential cyber infrastructure'. On this premise, member states are not only required to impose severe sanctions in terms

of those cybercrimes and other criminal activities that affect the ICT systems used in critical sectors, but they also have to establish measures that seek to improve the security and management of such systems.

Whether the argument given above is applicable or not, it is readily apparent that the cybersecurity framework of the Malabo Convention does not regulate the maritime sector sufficiently. Additionally, the Malabo Convention came into force in June 2023, nine years after its adoption in 2014 by the AU Head of States and Governments (AU, 2023). It has reached the required fifteenth ratification that was required for its coming into force with the Mauritanian ratification of the Convention (AU, 2023). As a result, the AU Specialized Technical Committee on Communication and Information Communications Technology (STC-CICT) and the AU Peace and Security Council (AU, 2022a) have since decided to call on member states not only to adopt the Malabo Convention, but also to adopt the required measures that would bolster their cybersecurity framework (AU, 2017b).

Since the adoption of the Malabo Convention, the STC-CICT has endorsed a strategy document entitled "A Global Approach on Cybersecurity and Cybercrime in Africa" (AU, 2017b). The recommendation by the STC-CTCT to create an AU Cybersecurity Expert Group (AUCSEG) under the auspices of the Information Society Division was also endorsed by the 32nd Executive Council in 2018 (AU, 2018b). It is important to note that the AUCSEG is a group of 10 cybersecurity experts representing the five African regions, whose specific tasks were identified at the first meeting of AUCSEG in 2019, and includes advising the AUC on cybersecurity issues as well as developing those policies and strategies that seek to establish collaborative ties between AU member states and stakeholders in terms of cybersecurity (AU, 2019a).

A recent development that was publicised by a Peace and Security Council Communique of the 1120th meeting –

[U]nderlines the urgent need for a Common African Position on the application of international law on cyberspace, as well as the need for Africa to actively engage in the process of articulating the rules of international law in this regard (AU, 2022b, paragraph 4).

The communique accordingly requested the AU Commission on International Law (AUCIL) to prepare a draft statement on the application of international law to cyberspace to be submitted to AUCIL for consideration. It further required circulation of the background note and questionnaire prepared by the AUCIL to all member states, and encouraged member states to respond expeditiously to the questionnaire (AU, 2022b, paragraph 6).

Maritime security instruments adopted by the AU and the security architecture

Despite the dependency of African states on the maritime sector and being endowed with a vast amount of marine resources, land-based conflicts have remained the focus of African member states for several years. The attempt to regulate the security of the maritime domain noticeably started in the last decade (i.e. 2010–2019) with the development of a few maritime security instruments.

The first instrument is the 2050 Africa's Integrated Maritime Strategy (2050 AIM Strategy), a document with no legal weight that had the vision "to foster increased wealth creation from Africa's oceans and seas by developing a sustainable thriving blue economy in a secure and environmentally sustainable manner" (AU, 2014a). The 2050 AIM strategy highlights the importance of inter-agency and transnational cooperation in cybersecurity, as well as the benefits and risks of communication technology advancements. The Strategy also gives due emphasis to the nature of cybercrime as being a cross-border issue that needs a united strategy. With that in mind, the strategy recommends that the AU, RECs and Regional Mechanisms (RMs), member states, the private sector as well as civil society work collaboratively in order to improve cybercrimes in Africa (AU, 2014a: paragraph 79). Furthermore, the strategy calls for international cooperation, most notably between the RECs, the RMs and AU member states and the relevant UN organs, in order to deal effectively with cyber threats in the maritime domain (AU, 2014a: paragraph 80).

On the other hand, the African Charter on Maritime Security and Safety and Development (Lomé Charter) is a legally binding document that has not only developed the AU's architecture for maritime security but also the modalities in which to develop the continent's Blue Economy. The scope of the Charter extends to maritime transnational crimes listed under the SUA Convention and the list of crimes encompassed within the Charter also refers to 'other unlawful acts' at sea (Lomé Charter, art. 4(a)) (AU, 2016). The inclusion of other unlawful acts provides a leeway for the Charter to be interpreted as being applicable to cybercrimes as well.

Under the Charter, member states are also required to harmonise their national laws in order to conform to relevant international legal instruments, such as the UNCLOS, SOLAS and the 2005 SUA Protocol. While pointing out these factors, it is also important to note that the Charter is yet to come into force (AU, 2023) and some of its important provisions are pending further discussions before being added as annexes to the Charter (AU, 2019c). The eight draft annexes to the Charter seek to regulate the marine environment as well as the development aspect of maritime security. However, it is surprising that none of the annexes, as they currently stand, address the issue of cybersecurity (see Annexure).

Regional economic communities

Besides being described in Agenda 2063 as "building blocks for continental unity" (AU, 2015:1), RECs are regional groupings of African states formed prior to the establishment of the AU. The RECs were established with the primary purpose of facilitating regional economic integration between members of the individual regions (African Union website, n.d.: n.p.).

If one takes a closer look, the contribution of the RECs to the integration process varies amongst RECs. As Stephen Karangizi highlights, "while some of them have made rapid progress, others have remained rather stagnant" (Karangizi, 2012: 248). Out of 55 African states, 11 hold membership with only one of the RECs, while 35 are members of two RECs, seven are members of three RECs, and one (Kenya) is a member of four of more RECs. For countries, membership of more than one REC means agreeing to implement different regional policies and programmes that may, at times, contradict each other (see Karangizi, 2012: 237).

Efforts to harmonise the legal framework of cybersecurity also differ from one region to another. Considering the variation of the regional frameworks, this section will only discuss those RECs that have an established policy framework in place, including regional frameworks that are beyond the RECs. The East African Community (EAC) for instance, started its efforts in 2001 with the establishment of the EAC task force. It consequently adopted the EAC regional harmonised framework for cyber laws, which is coordinated by the task force itself (see United Nations Conference on Trade and Development [UNCTAD], 2013). Cybercrime and data protection were included under phase one of the framework that was subsequently adopted by the EAC Council of Ministers on Transport, Communications and Meteorology, and is being implemented at national level (UNCTAD, 2013).

Furthermore, although the EAC was the pioneer in adopting the first instrument on cybercrime, the Economic Community of West African States (ECOWAS) has also attempted to harmonise the cybersecurity legal framework in its region by adopting key instruments in 2010 (ECOWAS, 2021). Most notable were the Supplementary Act on Personal Data Protection within ECOWAS (see ECOWAS, 2010a) and the Supplementary Act on Electronic Transactions within ECOWAS (see ECOWAS, 2010b). The importance of these instruments lies not only in their ability to set out the security, privacy and confidentiality obligations of those responsible for processing personal data but also in clearly outlining the conditions for accepting electronic signatures. Following these two instruments, the ECOWAS has since implemented Directive C/DIR 1/08/11 on Fighting Cybercrime within ECOWAS (see ECOWAS, 2011), which prescribes legal provisions for the regulation of cybercrimes within the region (Talabi, 2021).

In addition to these efforts, the ECOWAS was running a project together with the European Union from 2019–2021 called "Organized crime: West African Response on Cybersecurity and Fight against Cybercrime (OCWAR-C)" (OCWAR-C, 2020). The project aimed to enhance cybersecurity as well as to combat cybercrimes in the region. Comparably, the Southern Africa Development Community (SADC) and the Common Market for Eastern and Southern Africa (COMESA) have since developed a model law that seeks to guide member states in drafting their national laws on cybersecurity (COMESA, 2010; SADC, 2013).

All in all, the aspiration to criminalise cybercrimes, to increase cybersecurity capacity, as well as to promote the exchange of information between member states plays a role in creating a communal approach between the RECs.

Unfortunately, some of the RECs are yet to make visible progress in this integration process. Case in point is the Economic Community of Central African States (ECCAS), as it was inactive for several years due to conflicts in the Great Lake area as well as financial constraints (Raemdonck, 2021) The ECCAS held its first regional forum on cybersecurity in 2015, and subsequently adopted the Brazzaville Declaration in 2016 (ECCAS, 2016). The Declaration was adopted with the ambition to harmonise national policies and regulations in the region on matters related to telecommunications, cybersecurity, and those regulatory frameworks that seek to govern cross-border interconnection (ECCAS, 2016). Although it is an important step, the Declaration is a non-binding document with no legal obligation on member states.

Additionally, despite the fact that the Intergovernmental Authority on Development (IGAD) called for a determined, regional and collaborative approach on security-related matters, the region is yet to adopt a specific and binding legal document on cybersecurity. Nevertheless, it is important to note that one of the primary objectives of the IGAD Security Sector Program (IGAD SSP) and the SSP Transnational and Organized Crime Pillar is the prevention and management of emerging and exiting security threats, which include cybercrime (IGAD, n.d.). Likewise, the Arab Maghreb Union (AMU) is yet to adopt either a regional legal instrument or a cooperation agreement that seeks to harmonise the legal framework of its member states on the issue of cybersecurity (Raemdonck, 2021). Although the region has stayed inactive in the integration process for far too long, all of the Northern Africa states are part of the League of Arab States, making them parties to the 2010 Arab Convention on Combating Technology Offences. This Convention is comprised of procedural provisions as well as those legal and judicial mechanisms that seek to enhance cooperation between state parties (Raemdonck, 2021).

That being the case for regional cybersecurity instruments, it is equally important to analyse those regional instruments that seek to regulate the maritime sector and to reinforce its security. Although there are no specific regional instruments dealing with maritime cybersecurity, there are some maritime security instruments that seek to penalise maritime cybercrimes.

The first regional action to address maritime insecurity in the region started with the Djibouti Code of Conduct, which was first adopted in 2009 and subsequently amended in 2017 in order to broaden the scope of the Code (IMO, 2009). The amended document is now called "the Jeddah Amendment to the Djibouti Code of Conduct 2017" (Jeddah Amendment) (IGAD, 2017b). From the 17 state parties to the Code, 12 are African states comprising IGAD, EAC and the SADC.[5] Similarly, in realising that one of the means to resolve the insecurity in the Gulf of Guinea is through regional cooperation, the ECOWAS and ECCAS member states as well as the Gulf of Guinea Commission (GGC) have followed in the footsteps of the Indian Ocean states and have since adopted a regional instrument called the Yaoundé Code of Conduct.

5 Djibouti, Ethiopia, Kenya, Madagascar, Seychelles, Somalia, the United Republic of Tanzania, Comoros, Egypt, Eritrea, Mauritius, Mozambique, South Africa and Sudan are state parties to the Convention.

Both the Jeddah Amendment and the Yaoundé Code of Conduct aim to create regional frameworks that seek to combat piracy and armed robbery at sea along the Gulf of Guinea, in the Western Indian Ocean, and in the Gulf of Aden. Additionally, the Codes not only urge states, shipowners, and ship as well as port operators to take protective measures against transnational organised crime in the maritime domain, but they also encourage coordination, assistance, information sharing and incident reporting among state parties (IMO, 2017b).

The applicability of these regional instruments extends to transnational organised crimes in the maritime domain that are listed in the SUA Convention. Given that the provisions that stipulate the scope of the instruments also extend to other illegal activities at sea, it is not an exhaustive list. It would therefore be reasonable to conclude that cybercrime is also incorporated within the scope of the Jeddah Amendment as well as the Yaoundé Code of Conduct.

Beyond the legal instruments, it is worth mentioning the European Union Program to Promote Regional Maritime Security (MASE), which is working in the Eastern and Southern Africa as well as the Indian Ocean region (ESA-IO). The programme operates in the IGAD, EAC and COMESA regions, and its objective is to enhance maritime security in the ESA-IO region (EU, 2016). Despite the programme being focused on maritime security, its main objective is strengthening and developing the capacity of the ESA-IO region in the implementation of both legal and infrastructural matters for "the arrest, transfer, detention and trial of pirates" (EU, 2016).

Analysis of national legislation

Given the transnational nature of maritime crimes, it is important to assess those legal mechanisms that have been put in place by African states in order to enforce the international as well as regional instruments that they have ratified. In doing so, an extensive online research was undertaken on the national legislation of all African states. The detailed overview of the 55 African states subsequently resulted in a robust collection of pertinent data that have been categorised in terms of national cybersecurity laws, national maritime security laws, as well as those international and regional instruments that have been ratified by these African states. This categorisation effort has given the research two benefits. First, it identified and presented those legal instruments that deal with cybersecurity in general and maritime security in particular. Second, it highlighted the attempts made by these states in combatting cybercrime through national as well as international cooperation.

In light of the data that have been collected, this section will seek to assess the level of preparedness of African states in combating maritime cyber threats by first analysing those instruments that specifically regulate maritime cybersecurity. Following that, the section will review those general instruments that have been incorporated into the national legal frameworks of the states.

With regard to port security, it is important to remember that the IMO instruments were adopted with the aim of addressing the issues of maritime cybersecurity where it has been previously discussed that the cyber domain is already regulated by the 'all-risks approach' of both the ISM and the ISPS Codes. As far as the ISPS Code is concerned, cyber risk is only one risk that needs to be considered from the overall security of a ship or port facility. Accordingly, those states that are signatories of the SOLAS Convention should already have incorporated cyber risks into their risk assessments and should have designed their plans accordingly.

In terms of the security of ships, it is important to note that MSC Resolution 428(98) in effect worked as an enforcement mechanism, as the MSC had designated a specific deadline (1 January 2021) at which time cyber risks had to have been considered and addressed in SMSs of ships, as defined in the ISM Code and subject to verification of the Document of Compliance of the company (IMO, 2017c). This indicates that the ship component of maritime cybersecurity is a well-regulated domain, as the industry has been given a limited window in which to get its security measures properly adapted in order to address cybersecurity risks effectively. In terms of implementation, none of the African states have promulgated instructions for the enforcement of either the IMO guidelines or the resolution on maritime cybersecurity, except for Togo (Togolese Maritime Authority, 2020). Nevertheless, as can be *seen in Figure 1* below, African states, such as Ghana, Nigeria, Sao Tome and Principe, Libya, Mauritania, Seychelles, Cape Verde and the Democratic Republic of Congo, have expressly incorporated both the ISPS and the ISM Codes into their legal framework either by adopting a specific instrument or by incorporating them into their general maritime legal framework.

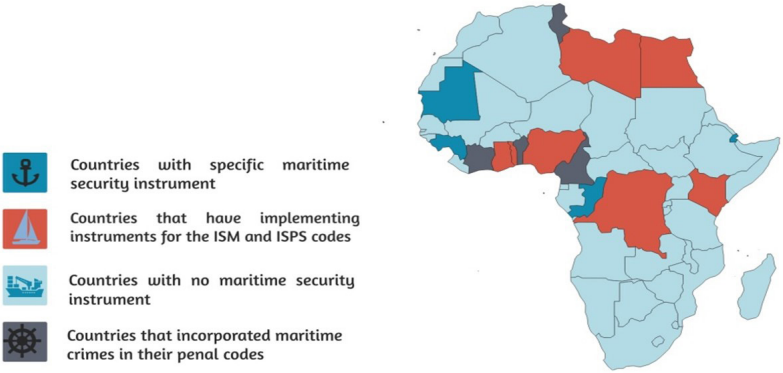

Figure 1: The implementation of the IMO instruments by African states

Source: See the Annexure

The remaining African states – particularly the 41 states that are state parties to the SOLAS Convention – are still required to enforce the 'all-risks approach' that is provided in both the ISM and the ISPS Codes. To this end, it is important to highlight that, although the legal approach followed by African states was beyond the scope of this article, it will be useful for future research endeavours to determine whether these states follow a monist or a dualist approach when it comes to the implementation of these international instruments. For instance, under the Constitution of Namibia, it is stated, "[u]nless otherwise provided by this Constitution or Act of Parliament, the general rules of public international law and international agreements binding upon Namibia under this Constitution shall form part of the law of Namibia" (Republic of Namibia, 1990: art. 144).

That being the case for the implementation of those standards that seek to regulate not only the safe management and operation of ships but also the security of ships as well as port facilities, it is also fundamental to look into the criminal law aspect of maritime cybersecurity. In order to examine the criminal law aspect one should examine the adoption of the SUA Convention by African states. It is clearly illustrated in Figure 2 that, as of May 2022, only Algeria, Côte d'Ivoire, Djibouti, Ghana, Mauritania, Nigeria, the Republic of Congo and Togo are signatories of the 2005 SUA Protocol, while 32 other states are parties to the 1988 SUA Convention.

As discussed previously, if one were to employ a broad interpretation of the SUA Convention, maritime cybercrimes fall within the meaning of those unlawful offences that are specified under the Convention. With this in mind, certain African states, most notably Kenya, Nigeria, Tanzania, and Togo, have expressly incorporated the provisions of the SUA Convention into their maritime security legal framework. In order to regulate and penalise all possible violent crimes that could occur in the maritime domain, these states have not only developed their very own distinct interpretations of maritime crimes, but have also incorporated such interpretations into their domestic legal texts.

On the other hand, it is unfortunate that more than 80 per cent of African states have neither adopted a maritime security instrument nor incorporated provisions related to maritime security into their maritime legal framework. This in turn creates significant complications when it comes to the implementation of the SUA Convention, the Djibouti Code of Conduct, as well as the Yaoundé Code of Conduct, as these instruments require state parties either to prosecute maritime criminals or to extradite them to another state with prosecutorial jurisdiction. Another serious constraint is that some of the penal codes as well as the provisions dealing with maritime security are outdated, and therefore fail to address contemporary security challenges that are faced by the maritime sector (Aden & McCabe, 2021).

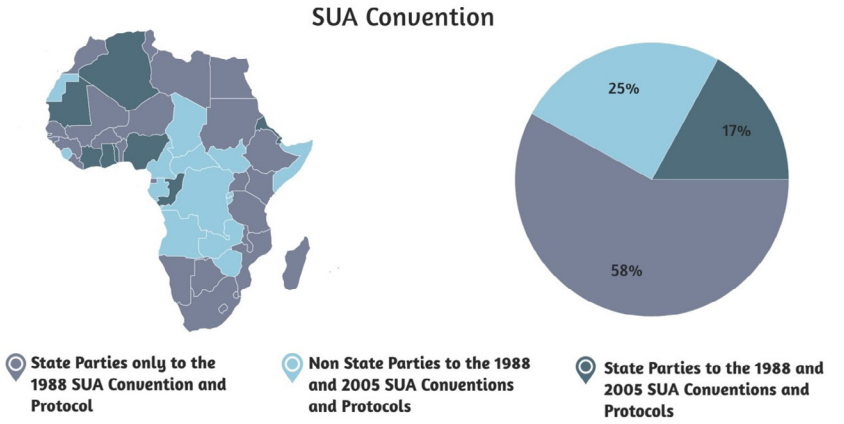

Figure 2: The adoption of the SUA convention by African states

Source: See the Annexure

One may therefore wonder if the general national cybersecurity framework of each African state can be used to fill the regulatory gap that is found in the specific maritime security instruments of these African states. A review of the cybersecurity legislations of the 55 African states indicates that some states have not taken any action in this regard whilst other states have adapted their domestic criminal laws in order to make them applicable to cybercrime. In doing so, most of the instruments adopted by these states are applicable to transport infrastructures, which in turn would include maritime transport. Moreover, it is noteworthy that towards the end of the previous decade (i.e. by 2019), 61 per cent of African states have adopted a variety of cybersecurity as well as cybercrime instruments; with 23 states enacting either a cybersecurity or cybercrime legislation, which would amount to 39 per cent of the continent, while 10 other states had enacted a variety of cybersecurity policies and strategies (*see* the annex). This amounts to 61 per cent of the continent as reflected in Figure 3. Even though there are several states that have either adopted cybersecurity instruments or developed a policy framework, the requirements that have been outlined by the IMO are still far from being met within the region. In this respect, while some countries have already set up the necessary institutions and reached a certain degree of preparation, most of the other states are still at an insufficient level.

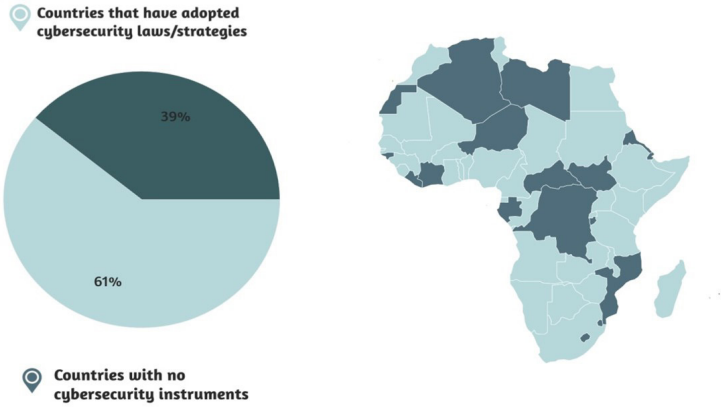

Figure 3: African countries with cybersecurity laws and strategies

Source: See the Annexure

Conclusion and recommendations

Although there are diverse challenges in the maritime sector, African states should come together under the auspices of the AU to resolve the issues that have been discussed in this article. In terms of the research and its findings, the author would like to add that, considering the unique technologies that are used in the maritime sector, there was a need for a research endeavour that also considered the particular vulnerabilities of this sector. Online research was therefore conducted to analyse the national legal and policy instruments of African states and instruments of the RECs dealing with cybersecurity in general and maritime cybersecurity in particular. While an online research was advantageous in terms of speed to access a wide range of documents, it also had limitations when it came to finding national legal instruments of African states, as the legislative documents of certain African countries are not regularly posted on websites of the authorities of such countries. However, considerable effort was made to gather as much of the available information online as possible. The collected data as well as the findings and recommendations provided should therefore be considered a starting point for further research undertakings on the issue of maritime cybersecurity.

Policymaking process

From the data analysis, it was clear that more than half of the African states have adopted either a binding law or a policy on cybersecurity. Many actors are involved in the making of those laws or policies, and for the implementation of the instruments dealing with cybersecurity different interests have to be balanced. However, the implementation process should start at the policy design phase, meaning that at this stage, the final implementation has to be considered.

The same goes for the law-making process of the AU. The law-making process can again be divided into a pre-negotiation phase and a decision-making phase, to which specific challenges apply. The involvement and strengthening of different stakeholders at the earliest possible stage is therefore suggested.

A harmonised regional cybersecurity framework

The lack of a unified approach has led to a regulatory landscape that lacks harmonization, with different national and regional laws across various RECs. To establish minimum standards under the Malabo Convention, it is crucial to address these differences and promote harmonization. The capacity of African States in achieving harmonization and promoting regional cyber stability is very vital, as such this potential need to be utilized. Harmonizing instruments adopted by the regional economic communities at the AU level will not only create a harmonized legal framework but also enhance national instruments and facilitate cooperation in prosecuting cyber criminals.

The level of awareness on maritime cybersecurity

Compared to the previous decade (2010–2019), awareness of general cybersecurity aspects has improved. When it comes to the maritime sector, however, awareness is either at a very low level or even non-existent. Taking into account the level of dependency on information technology, this lack of awareness results in inadequate preparedness in terms of maritime cyber risks. Member states should consider developing focused awareness-raising campaigns aimed at the key stakeholders in the maritime sector. In addition, appropriate and tailored guidance and training on specific maritime cybersecurity aspects should be developed and delivered to the relevant actors of the maritime sector, port authorities, and ship crews.

Fragmented maritime governance context

In the course of undertaking the research, it was observed that several maritime governance stakeholders relevant to the AU member states are found at different levels. It was also noted that their coordination regarding maritime security and the associated risks is inadequate. This inadequacy is ascribed to the lack of a dedicated department dealing with maritime security at the AU level. A harmonising unit should therefore be established by the AU to bring the various stakeholders together to make decisions according to consolidated information and to enhance the legal framework on maritime security matters.

In addition, the Lomé Charter (AU, 2016) and the 2050 AIM Strategy (AU, 2014) are outdated for current maritime challenges. The member states therefore need to revise these instruments. The AU should take the initiative to amend the strategy in a way that would enable member states to integrate cybersecurity into vital governmental infrastructures, involving citizens and other stakeholders in the various infrastructures. The continent would also benefit from a continental organ for the implementation of the strategy and to facilitate information sharing amongst member states.

Minimal consideration of cybersecurity in maritime regulations

From the data collected, it seemed that most of the laws related to maritime security only refer to provisions relating to safety and physical security concepts. Furthermore, as the existing regulatory frameworks are not optimally used and because they are inadequately defined, the implication is a too high dependency on operational stakeholders to identify appropriate courses of action in case of cyber threats that could cause incidents affecting the maritime sector, as well as its ICT infrastructure.

Member states should therefore take appropriate measures in order to add considerations and provisions towards cybersecurity in the national maritime regulatory frameworks. Member states should also work on an in-depth analysis of the current legislative framework to assess whether legislative updates are necessary to make progress in cybersecurity either as part of broader national cybersecurity initiatives or specifically in the maritime sector.

Regarding the AU institutional framework, although different departments are working on maritime issues within the AU, there is no single department or institution that specifically and exclusively deals with maritime security issues. The establishment of a dedicated agency that deals with maritime security within the AU could therefore go a long way in assisting member states, particularly when it comes to developing the type of resilient cyber risk management that has been mentioned earlier and readily discussed in the previous sections. Moreover, a regional maritime enforcement mechanism should be established to regulate the enforcement of the IMO guidelines, resolutions and recognised best practices.

Efforts to implement the holistic approach to maritime cyber risks

At the time of this research in 2021, there was no evidence that the African states were implementing a holistic approach to maritime cyber risks. In addition, efforts at the time of the time only addressed the partial scope of the maritime security range. Consequently, a holistic approach is required to ensure appropriate consideration of all relevant aspects of maritime security. Likewise, a joint effort between maritime ICT providers, maritime operators, port authorities and policymakers is needed to map the cyber risks faced by the maritime sector in Africa clearly.

Moreover, given that cyberspace is mostly controlled by the private sector, cooperation between the public and private sectors is essential to respond appropriately to those contemporary threats that are targeting the cyberspace. It is important for maritime economic operators and stakeholders, to apply sound cyber and information security principles proactively within their organisations and environments. These operators and stakeholders should recognise and manage the actual risks they face appropriately in line with their business objectives and the applicable regulatory context. To this end, it is important to highlight that there is no dedicated agency or department that actively contributes to the cyber policy of the AU. Although the recently established AU Cybersecurity Group of Experts could be of consideration, it is important to note that the expert group lacks institutional, procedural and enforcement powers.

About the Author

Tefesehet Hailu Sime is a researcher with experience in the field of law and international affairs. Currently, she holds a position as a researcher at Amani Africa Media and Research Services. Tefesehet's professional background includes valuable contributions to organizations such as the African Union Commission's Office of the Legal Counsel, the African Union Commission on International Law (AUCIL), and the International Tribunal for the Law of the Sea (ITLOS). Tefesehet holds a Bachelor of Law degree from Addis Ababa University (AAU) and an LL.M in International Maritime Law from the IMO International Maritime Law Institute (IMLI).

References

Aden, M., & McCabe, R. 2021. *Djibouti: Ports, Politics and Piracy*. Edmunds, T., McCabe,

R. & Bueger, C. (eds.). *Capacity Building for Maritime Security: The Western Indian Ocean Experience.* Cham, Switzerland: Palgrave Macmillan, 23 – 248.

Africa Container Shipping. 2021. *Top 10 ports in Africa by volume in TEUs*. Available at: <https://www.africa-container-shipping.com/top-10-ports-africa-port-projects-in-west-africa/> [Accessed 14 May 2021].

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, & S., Michaloliakos, M. Cybersecurity Challenges in the Maritime Sector. Network 2022*, 2,* 123-138. <https://doi.org/10.3390/network2010009>

Androjna, A., Perkovič, M., Pavic, I. & Mišković, J. 2021. AIS data vulnerability indicated by a spoofing case-study. *Applied Sciences*, 11(11):15–50.

Attard, D., Fitzmaurice, M., Hamza, R. & Martinez, N.(Eds.). 2017. *The IMLI manual on international maritime law: Volume III: Marine environmental law and international maritime security law*. Oxford, England Place: Oxford University Press.

AU (African Union) https://au.int/en/recs> [Website], accessed 3 August 2021.

AU (African Union). *Regional Economic Communities*. Available at: <https://au.int/en/recs> [Website], accessed 2 May 2021.

AU (African Union) Website . *Economic Community of Central African States*. Available at: <https://au.int/en/recs/eccas> [Accessed 20 May 2022].

AU (African Union). 1991. Treaty Establishing the African Economic Community. Available at: <https://au.int/en/treaties/treaty-establishing-african-economic-community> [Accessed 16 May 2021].

AU (African Union). 2009. Oliver Tambo Declaration. Available at: <https://au.int/sites/default/files/newsevents/workingdocuments/33025-wd-african_declaration_on_internet_governance_en_0.pdf> [Accessed on 8 June 2021].

AU (African Union) 2014a. *The 2050 Africa's Integrated Maritime Strategy*. Available at: <https://wedocs.unep.org/bitstream/handle/20.500.11822/11151/2050_aims_srategy.pdf> [Accessed 4 April 2021].

AU (African Union) 2014b. Assembly of the Union: Twenty-Third Ordinary Session. Available at: <https://au.int/sites/default/files/decisions/9661-assembly_au_dec_517_-_545_xxiii_e.pdf> [Accessed 4 June 2021].

AU (African Union). 2014c. African Union Convention on Cybersecurity and Personal Data Protection. Available at: <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection> [Accessed 4 May 2021].

AU (African Union). 2015. Agenda 2063. Available at: <https://www.afdb.org/fileadmin/uploads/afdb/Documents/Policy-Documents/Agenda2063_Popular_Version_English.pdf> [Accessed 16 July 2021].

AU (African Union). 2016. *African Charter on Maritime Security and Safety and Development in Africa (Lomé Charter).* Available at: <https://au.int/sites/default/files/treaties/37286-treaty-african_charter_on_maritime_security.pdf> [Accessed 4 July 2021].

AU (African Union). 2017a. A global approach on Cybersecurity and Cybercrime in Africa. Available at: <https://au.int/sites/default/files/newsevents/workingdocuments/31357-wd-a_common_african_approach_on_cybersecurity_and_cybercrime_en_final_web_site_.pdf> [Accessed 17 June 2021].

AU (African Union). 2017b. *African ministers of Communication and Information Technologies reiterate the need for Africa to become actively involved in the dynamics of internet governance, cybersecurity, and cybercrime.* Press release. Available at: <https://au.int/en/pressreleases/20171123/african-ministers-communication-and-information-technologies-reiterate-need> [Accessed 8 May 2021].

AU (African Union). 2018a. Agreement Establishing the African Continental Free Trade Area. Available at: <https://au.int/sites/default/files/treaties/36437-treaty-consolidated_text_on_cfta_-_en.pdf> [Accessed 4 June 2021].

AU (African Union). 2018b. *32nd ordinary session of the Executive Council, 25–26 January 2018.* Available at: <https://au.int/sites/default/files/decisions/33909-ex_cl_decisions_986-1007_e.pdf> [Accessed 20 May 2021].

AU (African Union). 2019a. *African Union Cybersecurity Expert Group holds its first inaugural meeting*. Press release. Available at: <https://au.int/en/pressreleases/20191212/african-union-cybersecurity-expert-group-holds-its-first-inaugural-meeting> [Accessed 20 May 2021].

AU (African Union). 2019b. *Peace and Security Council 850th meeting communiqué*. Available at: <https://archives.au.int/bitstream/handle/123456789/6336/850th%20Meeting%20of%20the%20AUPSC%20on%20Cyber%20Security%2020%20May%202019_E%20.pdf?sequence=1&isAllowed=y> [Accessed 20 May 2019].

AU (African Union). 2019c. Communique of the 858th Meeting of the Peace and Security Council of the African Union. Available at: <https://papsrepository.africa-union.org/handle/123456789/491> [Accessed 25 May 2019].

AU (African Union). 2022a. Communiqué of the 1097th meeting of the Peace and Security Council (PSC) held on 4 August 2022, on Emerging technologies and new media: Impact on democratic governance, peace and security in Africa. Available at: <https://papsrepository.africa-union.org/bitstream/handle/123456789/1700/1097.1.comm_en.pdf?sequence=20&isAllowed=y> [Accessed 16 December 2022].

AU (African Union). 2022b. *Communiqué of the 1120th meeting, held on 9 November 2022, on the Inaugural engagement between the Peace and Security Council and the AU Commission on International Law*. Available at: <https://www.peaceau.org/uploads/1120.comm.1-en.pdf> >[Accessed 16 December 2022].

AU (African Union). 2023. Status List to the African Union Convention on Cyber Security and Personal Data Protection. Available at: <https://dataprotection.africa/wp-content/uploads/2305121.pdf> [Accessed on 29 September 2023].

Bateman, T. 2013. Police warning after drug traffickers' cyber-attack. *BBC*, 16 October. Available at: <https://www.bbc.com/news/world-europe-24539417> [Accessed 25 March 2021].

Bayehu, E. 2015. The rights of land-locked states in the international law: The role of bilateral/multilateral agreements. *Science Publishing Group*, 11(6): 27 - 30.

Bennett, J. 2017. Navigation: A very Short Introduction. Oxford, United Kingdom: Oxford University Press.

BIMCO (Baltic and International Maritime Council). 2020. *The guidelines on cyber security onboard ships.* Available at: <https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf> [Accessed 20 May 2021].

Bogle, A. 2018. Svitzer employee details stolen in data breach affecting almost half of its Australian employees. *ABC News*, 15 March. Available at: <https://www.abc.net.au/news/2018-03-15/sensitive-data-stolen-from-global-shipping-company-svitzer/9552600> [Accessed 6 April 2021].

Cimpanu, C. 2020. World's largest cruise line operator discloses ransomware attack. *ZD Net*, 17 August. Available at: <https://www.zdnet.com/article/worlds-largest-cruise-line-operator-discloses-ransomware-attack/> [Accessed 4 July 2021].

COMESA (Common Market for Eastern and Southern Africa). 2010. Model Law on Electronic Transaction and Guide to Enactment. Available at: <https://web.archive.org/web/20150319055711/http://programmes.comesa.int/attachments/article/78/COMESA%20Model%20Law%20and%20%20Guide%20to%20Enactment%20(fin).pdf>

Devermont, J., Cheatham, A. & Chiang, C. 2019. *Assessing the risks of Chinese investments in sub-Saharan African ports.* Centre for Strategic & International Studies. Available at: <https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/190604_AfricaPorts.pdf> [Accessed 14 May 2021].

DNV-Maritime. 2020. *Maritime cybersecurity: What you need to know*. YouTube, 27 May. Available at: <https://www.youtube.com/watch?v=sz57s7dlmSk> [Accessed 2 May 2021].

Drougkas A., Sarri A, Kyranoudi P. & Zisi A. 2019. *Port cybersecurity: Good practices for cybersecurity in the maritime sector.* European Union Agency for Cybersecurity. Available at: <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector> [Accessed 24 May 2021].

Dunn, K. 2020. Mysterious GPS outages are wrecking the shipping industry. *Fortune*, 20 January. Available at: <https://fortune.com/longform/gps-outages-maritime-shipping-industry/> [Accessed 5 July 2021].

ECCAS (Economic Community of Central African States). 2016. *Declaration de Brazzaville*. Available at: <http://www.ceeac-eccas.org/images/PDF/DISCOURS/DeclarationDeBrazzaville24Nov16.pdf> [Accessed 20 June 2021].

ECOSOC (United Nations Economic and Social Council). 2009. E/ECA/CFSSD/6/6. *Africa review report on transport: Summary*. Available at: <https://sustainabledevelopment.un.org/content/documents/AfricanReviewReport-on-TransportSummary.pdf> [Accessed 24 April 2021].

ECOWAS (Economic Community of West African States). 2010a. Supplementary Act A1SA.1/01/10 On Personal Data Protection Within the ECOWAS. Available at: <https://ictpolicyafrica.org/en/document/z69cbq7b51?page=1&searchTerm=right> [Accessed 19 June 2021].

ECOWAS (Economic Community of West African States). 2010b. Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS. Available at: <https://ccdcoe.org/uploads/2019/10/ECOWAS-10216-Supplementary-Act-on-electronic-transaction.pdf> [Accessed 21 June 2021].

ECOWAS (Economic Community of West African States). 2011. Directive C/DIR.1/08/11 on Fighting Cybercrime within ECOWAS. Available at: <https://www.tit.comm.ecowas.int/wp-content/uploads/2015/11/SIGNED_Cybercrime_En.pdf?ophlfcbiecbaaiec> [Accessed 12 August 2021].

ECOWAS (Economic Community of West African States). 2021. ECOWAS Regional Cybersecurity and Cybercrime Strategy. Available at: <https://www.ocwarc.eu/wp-content/uploads/2021/02/ECOWAS-Regional-Cybersecurity-Cybercrime-Strategy-EN.pdf> [Accessed 3 May 2021].

EU (European Union). 2016. Program to Promote Regional Maritime Security (MASE). Available at: <https://www.eeas.europa.eu/node/8407_en> [Accessed 11 June 2021].

Fair play, BIMCO & ABS Advanced Solutions. 2018. *2018 Maritime Cyber Survey results*. Available at: <https://www.nepia.com/media/977540/Fairplay-and-BIMCO-Maritime-Cyber-Security-survey-2018.pdf> [Accessed 8 August 2021].

Faye, M.L., McArthur, J.W., Sachs, J.D. & Snow, T. 2004. The challenges facing landlocked developing countries. *Journal of Human Development*, 5(1):31–68.

Formula 2019. [Website] History of Navigation at Sea: From Stars to the Modern-Day GPS

Available at: <https://www.formulaboats.com/blog/history-of-navigation-at-sea-from-stars-to-the-modern-day-gps/> [Accessed 25 July 2021].

Handy Shipping Guide. 2020. *As maritime cyber-attacks proliferate international ports warned they are particularly vulnerable*. Available at: <www.handyshippingguide.com/shipping-news/as-maritime-cyberattacks-proliferate-international-ports-warned-they-are-particularly-vulnerable_13084> [Accessed 26 April 2021].

Hespen, I.V. 2016. Developing the concept of maritime piracy: A comparative legal analysis of international law and domestic criminal litigation. *International Journal of Marine and Coastal Law*, 31, 279–314.

Hornell, J. 1942. Floats: A Study in Primitive Water-Transport. The Journal of the Royal Anthropological Institute of Great Britain and Ireland 72(1/2):79–82. <http://www.jstor.org/stable/2844449>

IGAD (Intergovernmental Authority on Development). *Background Security Sector Program*. Available at: <https://igadssp.org/index.php/about-us-main-menu/background> [Website], accessed 13 July 2021].

IGAD-SSP <https://igadssp.org/index.php/components-mainmenu/transnational-organized-crime#:~:text=The%20pillar%20covers%20the%20areas,intellectual%20property%20rights%20related%20crimes%2C> [Website] accessed 12 June 2021.

IMO (International Maritime Organization). 1980. International Convention for the Safety of Life at Sea. Available at: <https://treaties.un.org/doc/Publication/UNTS/Volume%201226/volume-1226-I-18961-English.pdf> [Accessed 2 June 2021].

IMO (International Maritime Organization). 1988. The convention for the suppression of unlawful acts against the safety of maritime navigation. Available at: <https://treaties.un.org/doc/db/terrorism/conv8-english.pdf> [Accessed 8 July 2021].

IMO (International Maritime Organization). 1993. International Safety Management Code. Available at: <https://www.liscr.com/sites/default/files/liscr_imo_resolutions/A.741%2818%29_ISM%20Code.pdf> [Accessed on 19 June 2023].

IMO (International Maritime Organization). 1994. International Safety Management Code for the Safe Operation of Ships and Pollution Prevention. Available at: <https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx> [Accessed 2 August 2021].

IMO (International Maritime Organization). 2002. International Ship and Port Facility and Security Code and SOLAS Amendments. Available at: <https://portalcip.org/wp-content/uploads/2017/05/ISPS-Code-2003-English.pdf> [Accessed 23 August 2021].

IMO (International Maritime Organization) 2004. Ships and Port Facilities Security Code. Available at: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/ILOIMOCodeOfPracticeEnglish.pdf> [Accessed 22 June 2021].

IMO (International Maritime Organization). 2005. Protocol of 2005 to the convention for the suppression of unlawful acts against the safety of maritime navigation. Available at: <://www.refworld.org/docid/49f58c8a2.html> [Accessed 29 June 2021].

IMO (International Maritime Organization). 2009. The Djibouti Code of Conduct. Available at: https://dcoc.org/about-us/> [Accessed 18 June 2021].

IMO (International Maritime Organization). 2009. Djibouti Code of Conduct Available at: <https://www.imo.org/en/OurWork/Security/Pages/DCoC.aspx> [Accessed 14 May 2021].

IMO (International Maritime Organization). 2014. *Meeting summaries: The 94th session of the Maritime Safety Committee*. Available at: <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-94th-session.aspx> [Accessed 2 April 2021].

IMO (International Maritime Organization). 2016. *Interim guidelines on maritime cyber risk management.* IMO Maritime Safety Committee. Available at: <https://www.gard.no/Content/21323229/MSC.1-Circ.1526.pdf> [Accessed 5 June 2021].

IMO (International Maritime Organization). 2017a. *Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.1).* IMO Maritime Safety Committee. Available at: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf> [Accessed 5 June 2021].

IMO (International Maritime Organization). 2017b. The Jeddah Amendment to the Djibouti Code of Conduct. Available at: <https://dcoc.org/about-us/jeddah-amendment/> [Accessed 20 June 2021].

IMO (International Maritime Organization). 2017c. Maritime Cyber Risk Management in Safety

Management Systems (Resolution MSC. 428(98)). Available at: <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf> [Accessed on 28 June 2021].

ISO (International Organization for Standardization). 2017. *ISO/IEC 27001 Standard on Information Technology*. Available at: <https://www.iso.org/isoiec-27001-information-security.html> [Accessed 8 April 2021].

James, K. & Raul, P. 2013. *International maritime security law*. Leiden: Koninklijke Brill NV.

Jeffrey, R. 2020. *More investment in cyber security is needed.* Port Strategy. Available at: <https://www.portstrategy.com/news101/technology/more-investment-in-cyber-security-needed> [Accessed 4 April 2021].

Kahyarara G. & Simon, D. 2018. "Maritime Transport in Africa: Challenges, Opportunities, and an Agenda for Future Research". Available at: <https://unctad.org/system/files/non-official-document/dtltlbts-AhEM2018d1_Kahyarara_en.pdf> [Accessed 7 June 2022].

Karangizi, S. 2012. The Regional Economic Communities. Yusuf, A. A., & Ouguergouz, F. (eds.) In *The African Union: Legal and Regional Framework: A manual on the Pan-African Organization*. Leiden, The Netherlands: Martinus Nijhoff, 231–249.

Kochetkova, K. 2015. Maritime industry is easy meat for cyber criminals. *Kaspersky Daily*, 22 May. Available at: <http://www.kaspersky.com/blog/maritime-cyber-security/8796/> [Accessed 11 October 2022].

League of Arab States. 2010. Arab Convention on Combating Technology Offence. Available at: <https://www.asianlaws.org/gcld/cyberlawdb/GCC/Arab%20Convention%20on%20Combating%20Information%20Technology%20Offences.pdf> [Accessed 20 June 2021].

Lokanathan, V. 2020. *China's Belt and Road Initiative: Implications in Africa*. Observation Research Foundation. Available at: <https://www.orfonline.org/research/chinas-belt-and-road-initiative-implications-in-africa/> [Accessed 6 October 2022].

Maury F. & Féligonde A.. 2020. *Africa's ports: Fast-tracking transformation*. Africa CEO Forum and OKAN Partners. Available at: <https://okanpartners.com/wp-content/uploads/2020/10/Study-Okan-AFC_Ports-in-Africa.pdf> [Accessed 11 May 2021].

Mraković I. & Vujinoć R. 2019. Maritime Cyber Security Analysis – How to Reduce Threats? Transaction on Maritime Science. 13: 132 – 139. Available at: <https://web.archive.org/web/20200212170307id_/https://pdfs.semanticscholar.org/4f49/15b604885029802ff3ca880f67fcb711b157.pdf> [Accessed on 18 August 2021].

Newman, N. 2019. *Cyber pirates terrorising the high seas.* E&T. Available at: <https://eandt.theiet.org/content/articles/2019/04/cyber-pirates-terrorising-the-high-seas/> [Accessed 14 October 2022].

NIST National Institute of Standards and Technology). 2017. *National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity*. Available at: <https://www.nist.gov/cyberframework> [Accessed 8 October 2022].

OCWAR-C (Organised Crime: West African Response). 2020. <https://www.ocwarc.eu/ocwar-c/> [Website], accessed 23 May 2021.

O'Dwyer, R. 2020. *IMO latest to fall victim to cyber-attack*. Smart Maritime Network. Available at: <https://smartmaritimenetwork.com/2020/10/01/imo-latest-to-fall-victim-to-cyber-attack/> [Accessed 10 October 2022].

Ovcina, J. 2020. 400% increase in attempted hacks since February 2020. *Naval Dome*, 5 June. Available at: <https://www.offshore-energy.biz/naval-dome-400-increase-in-attempted-hacks-since-february-2020/> [Accessed 4 April 2021].

Pasternack, A. 2013. To move drugs, traffickers are hacking shipping containers. *Vice*, 21 October. Available at: <https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs> [Accessed 9 October 2022].

Republic of Namibia. 1990. Constitution of the Republic of Namibia. Available at: <http://citizenshiprightsafrica.org/wp-content/uploads/2016/01/1990-Constitution-Amended-1998.pdf [Accessed 10 August 2021].

Raemdonck, N. 2021. Africa as a Cyber Player. EU Institute for Security Studies. Available at: <https://eucd.s3.eu-central-1.amazonaws.com/eucd/assets/FgLaEKYp/digital-dialogue-africa-final.pdf> [Accessed 20 June 2021].

Reva, D. 2020. *Maritime cyber security: Getting Africa ready.* Institute for Security Studies. Available at: <https://issafrica.s3.amazonaws.com/site/uploads/ar-29.pdf> [Accessed 20 May 2021].

Reva, D. 2021. *Cyber-attacks exposed the vulnerability of South Africa's ports.* Institute for Security Studies. Available at: <https://issafrica.org/amp/iss-today/cyber-attacks-expose-the-vulnerability-of-south-africas-ports> [Accessed 5 August 2021].

Rosenberg, M. 2019. *44 land-locked countries without direct ocean access.* ThoughtCo. Available at: <https://www.thoughtco.com/landlocked-countries-1435421> [Accessed 30 May 2021].

SADC (Southern Africa Development Community). 2013. Computer Crime and Cybercrime: SADC Model Law. 2013. Available at: <https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf> [Accessed 16 June 2021].

Safe Seas, Safe Shores. 2018. The Development of Ship Designs. Available at: <https://www.shmgroup.com/blog/development-ship-design/> [Accessed 22 July 2021].

SAFETY4SEA. 2018. *Maersk line: Surviving from a cyberattack*. Available at: <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/> [Accessed 21 March 2021].

Salter, M. & Mason, J. 2007. *Writing law dissertations: An introduction & guide to the conduct of legal research.* WorldCat, Harlow England; New York: Pearson/Longman.

Shabalala, Z. & Heiberg, T. (2021) 'Cyber-attack disrupts major South African port operations'. Reuters 22 July 2021. Available at: <https://www.reuters.com/world/africa/exclusive-south-africas-transnet-hit-by-cyber-attack-sources-2021-07-22/> [Accessed 28 July 2021].

Talabi, D. (2021) Towards a robust consumer protection driven regulatory framework for e- commerce in Nigeria. Unpublished LLM Thesis. University of Pretoria. Available at: <https://repository.up.ac.za/bitstream/handle/2263/82888/Talabi_Towards_2021.pdf?isAllowed=y&sequence=1> [Accessed 30 May 2021].

Tanti-Dougall, R. 2020. *Cyber terrorism: A new threat against the maritime industry.* LexisNexis Legal. Available at: <https://www.lexisnexis.com/legalnewsroom/public-policy/b/public-policy-law-blog/posts/cyber-terrorism-a-new-threat-against-the-maritime-industry> [Accessed 24 October 2022].

Togolese Maritime Authority. 2020. Maritime Cyber Risk Management in Safety Management System. Available at: <https://www.togoregistrar.com/documents/doc_circulars_277.pdf> [Accessed 25 August 2021].

Triantafillou, A., Bardaka, I., Vrettakos, I., & Zombanakis, G. 2023. Maritime piracy: Determining factors and the role of deterrence. *African Security Review*, 32(2), 166 – 183.

Tsimplis, M. & Papadas, S. 2019. Information technology in navigation: Problems in legal implementation and liability. *Journal of Navigation*, 72(4), 833–849.

United Nations Codification Division Publications. <https://legal.un.org/diplomaticconferences/1958_los/> [Accessed 20 August 2021].

UN (United Nations). 1965. Convention on Transit Trade of Land-locked States. Available at: <https://www.jus.uio.no/english/services/library/treaties/09/9-04/land-locked-states.html> [Accessed 5 June 2021].

UN (United Nations). 1982. The United Nations Convention on the Law of the Sea (UNCLOS). Available at: <https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf> [Accessed 3 April 2021].

UN (United Nations). 1986. United Nations Convention on Conditions for Registration of Ships. Available at: <https://unctad.org/system/files/official-document/tdrsconf23_en.pdf> [Accessed on 29 September 2023].

UN (United Nations). 1988. Convention for the Suppression of Unlawful Acts against the Safety of Navigation. Available at: <https://treaties.un.org/doc/db/terrorism/conv8-english.pdf> [Accessed on 228 June 2021].

UNCTAD (United Nations Conference on Trade and Development). 2013. *Harmonizing cyber laws and regulations: The experience of the East African Community.* Available at: <https://unctad.org/system/files/official-document/dtlstict2012d4_en.pdf> [Accessed 24 May 2021].

UNCTAD (United Nations Conference on Trade and Development). 2018. *Review of maritime Transport 2018*. New York, NY. Available at: <https://unctad.org/system/files/official-document/rmt2018_en.pdf> [Accessed 25 August 2021].

Wagstaff, J. 2014. All at sea: Global shipping fleet exposed to hacking threat. *Reuters*, 24 April. Available at: <https://www.reuters.com/article/us-cybersecurity-shipping-idUKBREA3M20820140424> [Accessed 6 July 2021].

WEF (World Economic Forum). 2020. *The Global Risks Report: The Unsettled World.* 15th edition. Available at: <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf> [Accessed 26 April 2021].

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Algeria	Arab Maghreb Union (AMU)	No specific law on maritime security, but there is the Algerian Maritime Code of 1976 amended by Law No. 98-05 of 25 June 1998 and Decree No. 2000-81 of 9 April 2000 establishing the conditions and procedures for the operation of maritime services	Loi n° 16-02 du 14 Ramadhan 1437 – updated the Penal Code to criminalise use of information technologies and communication (ITC) to engage in terrorist acts.	DZ-CERT (Algerian Computer Emergency Response Team)	Project Cyber South – cooperation on cybercrime in the southern neighbourhood region	State party SOLAS, 1974
	Arab League	Presidential Decree No. 97-373 of September 1991 on Accession, subject to reservation, to the Suppression of Unlawful Acts (SUA) Convention, signed on 13 March 1988	Loi n° 18-05 du 10 mai 2018 relative au commerce électronique (en Français).			State Party to the 2005 SUA Convention and Protocol
		Executive Decree No. 08-387 amending Executive Decree No. 04-418 designating the competent authorities in matters of security of ships and port facilities and the creation of related bodies	Loi n° 09-04 du 14 Chaâbane 1430 – rules for preventing and combating offences related to ITC.	Ministry of Post and Telecommunications		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Algeria			Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel (available in French).			
Angola	Economic Community of Central African States (ECCAS)	Law No. 27/12 of 28 August 2012 – the Merchant Navy Law – seeks to regulate all maritime and port activities in a consistent manner, governing matters related to navigational, technical and security rules	Presidential Decree No. 202/11 on the Regulation of Technologies and Services of the Information Society	Ministry of Telecommunications and Information Technologies	Community of Portuguese Speaking Countries (CPLP) Conference on E-Government host	State party to SOLAS, 1974
	Southern African Development Community (SADC)		Law No. 22/11 on the Protection of Personal Data of 17 June (available only in Portuguese)	The Maritime and Port Institute of Angola		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Angola			Republic of Angola Penal Code, 2019 Criminal Code. Article 233–238 deals with forgery of documents, computer data and technical records			
			Regulamento das Tecnologias e dos Serviços da Sociedade da Informação, Decreto Presidencial n.º202/11 (available only in Portuguese).			
			Network and Information Technology Systems Protection Law			
Benin	Community of Sahel–Saharan States (CEN–SAD)	Law n° 2010-11 of 7 March 2011 – maritime code of the Republic of Benin (available in French). Book VI stipulates the penal provisions for maritime crimes and offences	National Digital Security Strategy	Digital Economy Agency	African Union (AU) Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Benin	Economic Community of West African States (ECOWAS)	The Constitution of Benin provides that international law becomes part of the domestic law upon ratification and publication	Law No. 2017-20 on Digital Code in the Republic of Benin (Digital Code) – includes transaction laws, consumer protection laws, data protection and privacy laws	Office Central de Répression de la Cybercriminalité (OCRC)	Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS	State party to the 1988 SUA Convention and Protocol
Botswana (land-locked)	SADC	No specific law regulating the maritime sector	National Cybersecurity Strategy	Ministry of Transport and Communications	Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	State party to the 1988 SUA Convention and Protocol
			Electronic Communication and Transactions Act No. 14/2014	Cybersecurity Operation Center (COC) and National Cybersecurity Advisory Council are proposed		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Botswana (land-locked)						
			Data Protection Act, 2018	Botswana Computer Incident Response Team (BwCIRT)		
			Maitlamo (National ICT Policy) – (2012)			
			Cybercrime and Computer Related Crimes Act			
Burkina Faso (land-locked)	CEN–SAD	No specific law that regulates maritime security	National Cybersecurity Strategy (2019–2023)	National Agency for the Promotion of Information and Communication Technologies (ANPTIC)	Regional workshop on cybercrime/ cyber terrorism in G5 Sahel countries	State party to the 1988 SUA Convention and Protocol
	ECOWAS		National Cybersecurity Plan (2010)	Authority of Regulation Electronic Communications and Posts (ARCEP)		
			Loi n°010-2004/AN Portant Protection des Données àCaractère Personnel (only available in French).	National Information Systems Security Agency (ANSSI)		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Burkina Faso (land-locked)			Loi n°. 61-2008-AN – on the general standards of network and electronic communication services.	Burkina Faso Computer Incident Response Team (CIRT.BF)		
			Loi n°045-2009/AN du 10 Novembre 2009 portant reglementation des services et des transactions électroniques (only available in French).			
Burundi (land-locked)	COMESA	There are 24 Burundian fleets operating in inland waters	Penal Code (2009) – Article 467–476	Regulatory Agency for Telecommunications (ARCT)	Signatory to the African Charter on Maritime Security, Safety and Development (Lome Charter)	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Burundi (land-locked)	EAC		Industrial Property Act No. 1/13 of July 2009, and the Protection of Right of Author and its related Act No. 1/06 of December 2005 both include the protection of software and other electronic or digital formats.			
	ECCAS		The Telecommunications Act No. 1/11 of 4 September 1997 – Articles 10 and 23.			
Cameroon	ECOWAS	Law n° 2000/02 relating to the maritime spaces of the Republic of Cameroon	Strategic Plan for a Digital Cameroon by 2020 (2016).	Computer Incident Response Team (CIRT)	National Cyber Expertise Centre (2015)	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Cameroon		Decree N° 2013/391 of 31 October 2013 on the creation, organisation and functioning of the national committee for monitoring the implementation of the decisions resulting from the Summit of Heads of State and Government of ECCAS, ECOWAS and CGG (Commission of the Gulf of Guinea)	Law n°. 2010/012 relating to cybersecurity and cyber criminality in Cameroon	National Agency for Information and Communication Technologies (ANTIC)	National Committee for monitoring the implementation of the decisions resulting from the Summit of Heads of State and Government of ECCAS, ECOWAS and CGG	
			Loi n° 2010/021 of 21 decembre 2010 Régissant le commerce électronique au Cameroun (in French).			
			Law n° 2010/013 Governing Electronic Communications			
Cape Verde	CEN–SAD	Legislative Decree No. 14/2010 establishing the Maritime Code of Cape Verde	National Strategy on Cybersecurity (2016)	National Centre on Cybersecurity	Cape Verde Maritime Security Services	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Cape Verde	ECOWAS	Law No. 75/IX/2020 granting the government legislative authorisation to amend the Maritime Code	Lei n°8/IX/2017 Lei de Cibercrime – Law on Cybercrime	Penal Code (2004)		State party to the 1988 SUA Convention and Protocol
		Decree No. 5/2004 implementing the International Code for the Security of Ships and Port Facilities (ISPS Code)				
Central African Republic (CAR) (land-locked)	CEN–SAD				United Nations Convention on the Use of Electronic Communications in International Contracts (NY, 2005)	
	ECCAS					
Chad (land-locked)	CEN–SAD					
	ECCAS					

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Comoros	Common Market for Eastern and Southern Africa (COMESA)	No specific law regulating maritime security		Ministry of Transport, Post and Telecommunications, Information and Communication Technologies	AU Convention on Cyber Security and Personal Data Protection – signed not ratified	State party to SOLAS, 1974
	CEN–SAD					State party to the 1988 SUA Convention and Protocol
Côte d'Ivoire	CEN–SAD	Law No. 2017–442 of 30 June 2017 – Maritime Code	National ICT Master Plan (Schéma directeur national des TIC (2017).	Autorité de Régulation des Télécommunications de Côte d'Ivoire (ARTCI)	Regional workshop on cybercrime/ cyber terrorism in G5 Sahel countries	State party to SOLAS, 1974
	ECOWAS		Loi n° 2013–546 du 30 juillet 2013 relative aux transactions électroniques (available in French)	Côte d'Ivoire – Computer Emergency Response Team (CI-CERT)	ECOWAS Directive on Cybercrime and Cyber Security (C/DIR. 1/08/11) (2011)	State party to the 2005 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Côte d'Ivoire			Loi n° 2013–451 relative à la lutte contre la cybercriminalité – contains provisions on substantive criminal law (including those related to illegal access, illegal interception, data and system interference, computer-related fraud and forgery and online child protection), provisions related to the collection of electronic evidence and provisions on criminal procedure law	Maritime Police Service, which is under the direction of the Coast Guard who is responsible for ensuring port security; offshore platforms; the monitoring of lagoon water, maritime waters; and the protection and security of maritime approaches		
			Loi n° 2013–450 du 19 juin 2013 relative à la protection des données à caractère personnel (in French)			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Côte d'Ivoire			L'ordonnance n°. 2012–293 du 21 mars 2012 relative aux Telecommunications et aux TIC (available in French)		Global Forum on Cyber Expertise (GFCE), member	
Democratic Republic of Congo (DRC)	CEN–SAD	Intermenstrual decree n° / CAB / MIN / INT, DEC & AFF. COUT./2013 and n° 002 / CAB / MIN / TVC / 2013 of 29 April 2013 setting the procedures for establishing the security levels of ships and port facilities in the DRC. The Decree takes into consideration the SOLAS Convention and the ISPS Code	Bill – E-Commerce Legislation			State party to SOLAS, 1974
	ECCAS					
	SADC					

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Djibouti	CEN–SAD	Maritime Security Strategy – the document is not available online	Penal Code Livre IV – the Code is based on the colonial French court system and is therefore outdated in terms of contemporary challenges. The existing penal code prevents national jurisdiction over extraterritorial pirates except when the alleged piracy involves an attack on the flag vessel of the Republic of Djibouti	Ministry of Transport –oversees drafting of policy guidelines at government level	Signatory to the African Charter on Maritime Security Safety and Development (Lomé Charter)	State party to the 2005 SUA Convention and Protocol
	COMESA			The Ministry of Transport has under its authority the Maritime Affairs Directorate, the Djibouti Coast Guard and the Djibouti Regional Maritime Training Center (DRTC)	State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Djibouti	Inter-governmental Authority on Development (IGAD)			Maritime Security Committee	Joint Statement, Djibouti–Somalia (2017) – agreement to promote and strengthen the cooperation between the ministries in number of areas, such as regional interconnectivity, terrestrial optical fibre, cyber security, ICT regulations, cross-border signals issues, spectrum management, numbering plan, etc.	
Egypt	CEN–SAD	Law No. 167/1960 concerning system security and discipline aboard ships	Anti-Cyber and Information Technology Crimes Law (Law No. 175/2018) (2018) – punishes those who commit crimes of violating the safety of networks and IT systems	Egyptian Supreme Cybersecurity Council (ESCC)	Cooperation, Belarus–Egypt	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Egypt	COMESA	Law No. 232/1989 concerning safety of ships	Decree on Cybersecurity, Issue No. 17 BIS (b) (2017)	Ministry of Communications and Information Technology	Regional Cybersecurity Summit and FIRST Regional Symposium for Arabic and African Regions, host	State party to the 1988 SUA Convention and Protocol
	Arab League	Law No. 1/1996 concerning specialised ports	National Cybersecurity Strategy 2017–2021 (2018)	The Cybercrime and Data Networks Unit	Memorandum of understanding (MoU), Egypt–India	
			Law No. 15 of 2004 on E-signature and Establishment of the Information Technology Industry Development Authority	Egyptian Computer Emergency Readiness Team (EG-CERT)		
			Penal Code (No. 58) 1937 (in Arabic)	Libya Computer Emergency Readiness Team (Libya–CERT)		
			Law No. 15/2004 on E-Signatures and *Information Technology Industry Development Agency* (ITIDA) (in English)	Egyptian Authority for Maritime Safety (EAMS)		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Equatorial Guinea	ECCAS			Ministry for Transport, the Postal Service and Telecommunications		State party to SOLAS, 1974
				Telecommunications Regulatory Office (ORTEL)		State party to the 1988 SUA Convention and Protocol
Eritrea	CEN–SAD	Proclamation No. 7 Transitional Maritime Code of Eritrea. It is stated by the proclamation that the Maritime Code of 1960 Ethiopia hitherto in force shall, as of 15 September, 1991, serve as the Transitional Maritime Code of Eritrea with the following amendments and substitutions and with all words, phrases, names and dates denoting the Provisional Government of Eritrea, except for the provisions of Article 46(1) …	None	None	None	State party to SOLAS, 1974
	COMESA					

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Eswatini (land-locked)	COMESA	No specific law regulating the maritime sector	Computer Crime and Cybercrime Bill (draft legislation)	Ministry of Information, Communications and Technology	Cooperation agreement, Russia–South Africa	State party to SOLAS, 1974 ()
	SADC					State party to the 1988 SUA Convention and Protocol
Ethiopia (land-locked)	IGAD	No specific law on maritime cybersecurity or maritime security in general. However, there is the 1960 Maritime Code of Ethiopia, which does not address maritime security	Critical Mass Cyber Security Requirement Standard (2017)	Information Network Security Agency (INSA) (2016)	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	State party to SOLAS, 1974
	COMESA	The maritime strategy is undergoing through a drafting process	Criminal Code Proclamation No. 414/2004	Ministry of Innovation and Technology (MinT) (2018)	Cooperation, Ethiopia–Israel – Cooperation between Israel and 7 African countries (Zambia, Ethiopia, Uganda, South Sudan, Rwanda, Kenya, Tanzania) on security and economic matters, including cyber security	State party to the 1988 SUA Convention

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
				Computer Crime Proclamation No. 958–2016 (2016)	Ethiopian Cyber Emergency Readiness and Response Team (Ethio-CERT)	State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment
			Information Network Security Agency Re-establishment Proclamation			
			Telecom Fraud Offences Proclamation No. 761/2012			
			Electronic Signature Proclamation No. 1072/2018			
Gabon	ECCAS					State party to SOLAS, 1974
Gambia	CEN–SAD		Gambia National Cyber Security Policy, Strategies and Action Plan (2020–2024) (2020)	Ministry of Information and Communication Infrastructure (MOICI)	GFCE, member	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Gambia	ECOWAS		Draft Data Protection and Privacy Policy and Strategy (2019)	National Cybersecurity Commission (NCSC)	UNCITRAL Model Law on Electronic Commerce (1996)	State party to the 1988 SUA Convention
			The Information Communication Act (ICA), No. 1 and 2 of 2009		UNCITRAL Model Law on Electronic Signatures (2001)	
			Cybercrime legislation – in progress		Supplementary Act A/SA.2/01/10 on Electronic Transactions within ECOWAS	
Ghana	CEN–SAD	Ghana Maritime Security Act, No 675 of 2004 – incorporates what is provided under the ISPS and International Safety Management (ISM) Code	Ghana National Cyber Security Policy & Strategy (2015)	National Information Technology Agency (NITA)	Budapest Convention – ratified	State party to SOLAS, 1974
	ECOWAS	Ghana Shipping Act, No. 645 of 2003	The Ghana ICT for Accelerated Development (ICT4AD) Policy (2003)	National Cyber Security Centre (NCSC) (2018)	AU Convention on Cyber Security and Personal Data Protection – ratified	State party to the 2005 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Ghana			Electronic Communications Act (Act No. 775) 2009	Police Cybercrime Unit – Criminal Investigation Department (CID), Ghana Police Service	Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	
			Electronic Transactions Act (Act No. 772) 2008	Ghana Computer Emergency Response Team (CERT-GH)	Advisory Mission on Cybercrime and Cybersecurity Policies	
				Ghana Maritime Authority	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member (2016)	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Ghana Maritime Authority					United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce (1996) b) UNCITRAL Model Law on Electronic Signatures (2001)	
					ECOWAS Directive on Cybercrime and Cyber Security (C/DIR. 1/08/11) (2011)	
Guinea	CEN–SAD	Law n° nº L / 95/23 / CTRN / of 12 June 1995, establishing the Merchant Marine Code	Loi n° 037 Relative à la cyber-sécurité et la protection des données à caractère personnel (2016)	Ministère des Postes, Télécommunications et de l'Economie Numérique (MPTEN)	AU Convention on Cyber Security and Personal Data Protection – ratified	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Guinea	ECOWAS	Decree D / 2019/063 / PRG / SGG of 5 February 2019 on the organisation of state action at sea. State action at sea is implemented by the maritime authority and the maritime authority is responsible and competent in all areas where state action is carried out at sea. The fight against illegal maritime activity is amongst the responsibilities	Loi n° 37/2016 Relative à la cyber sécurité	The maritime authority must be involved in the development of all draft legislative and regulatory texts governing the Guinean maritime area		State party to the 1988 SUA Convention and Protocol
			Loi L/2016/037/ AN relative à la cyber–sécurité et la protection des données à caractère personnel			
			Loi sur les transactions électroniques 35/2016 (available in French)	l'Agence Nationale de la Gouvernance Electronique et de l'Informatisation de l'Etat (ANGEIE)		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Guinea-Bissau	CEN–SAD		Law No. 5/2010 – Basic Information and Communication Technology Law (2010) (available in Portuguese)	Ministry of Transport and Communication	AU Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974
	ECOWAS			Autoridade Reguladora Nacional (National Regulatory Authority) (ARN)		State party to the 1988 SUA Convention and Protocol
Kenya	CEN–SAD	No specific law on maritime cyber security	National Cybersecurity Strategy 2014	Kenya Maritime Authority	Signatory to the African Charter on Maritime Security Safety and Development (Lomé Charter)	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Kenya	COMESA	Part XVI of the Marchant Shipping Act – No.4 of 2009 – is dedicated to maritime security. It incorporates crimes provided for under the SUA Convention, which makes it applicable to criminalising cybercrime, particularly sections 370 and 372	Kenya Information and Communication Act, Rev. 2009 (in English) – sections 32 and 64(4)	Kenya National Computer Security Incident Response Team – Coordination Centre (KE-CIRT/CC)	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	State party to the 1988 SUA Convention and Protocol
	EAC	Merchant Shipping (Port State Control) Regulations, 2011 (Cap. 389)	The Computer Misuse and Cybercrimes Act, 2018	Cyber Crime Unit, Directorate of Criminal Investigations – National Police Service	MoU, Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Kenya	IGAD	Shipping (Maritime Security) Regulations, 2004 (L.N. No. 5 of 2004). The Regulations implement provisions of the International Maritime Organization (IMO) International Management Code for the Safe Operation of Ships and for Pollution Prevention (ISM Code) and the International Code for the Security of Ships and of Port Facilities (ISPS Code). The regulations shall apply to passenger ships, large cargo ships, including oil tankers and chemical tankers, mobile offshore drilling units and port facilities. The regulation requires all ships to have a security plan that shall be submitted to the Minister and to be provided with a ship security alert system	The Data Protection Act, 2019	National Computer and Cybercrimes Coordination Committee	GFCE, member	
				Kenyan National Computer Security Incident Response Team (KE-CIRT/CC)	State Party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Lesotho (land-locked)	SADC	No specific law regulating the maritime sector	ICT Policy for Lesotho	Ministry of Communications, Science and Technology		State party to the 1988 SUA Convention and Protocol
			Data Protection Act No. 19 of 2012			
			Lesotho Electronic Transactions and Electronic Commerce Bill 2013			
			Communication Act, 2012			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Lesotho (land-locked)			Article 44(1) (e) of the Communication Act - A person shall not intentionally modify or interfere with the contents of any message sent by means of a communications service f. (f) engage in interception or tracing of communications operations or messages unless authorised by a court of competent jurisdiction			
Liberia	CEN–SAD	Maritime Law (2013 Revision). Date of original text: 1956	Cybersecurity Strategy of the Republic of Liberia – draft	Ministry of Posts and Telecommunications (MOPT)	GFCE, member	State party to SOLAS, 1974
	ECOWAS		National Telecommunication and ICT Policy 2010–2015	Liberia Cyber Crime Prevention and Mitigation Agency (LCCPMA)	UNCITRAL Model Law on Electronic Commerce (1996)	State party to the 1988 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Libya	Arab Maghreb Union (AMU)	No specific law regulating maritime security		National Information Security and Safety Authority		State party to SOLAS, 1974
	CEN–SAD	General People's Committee Decree No. (152) of 1372 FDP on the Implementation of the International Ship and Port Facility Security Code (ISPS Code)				
	COMESA	Libyan Maritime Law of 1953, as amended		Ports and Maritime Transportation Department		State party to the 1988 SUA Convention and Protocol
		Law no. 81 of 1970 on Maritime Ports – article 152 deals with crimes committed by intentionally causing damage to or obstructing maritime navigation tools, piloting and wireless equipment in ports or ships				

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Madagascar	COMESA	No specific law regulating maritime safety and security	Loi n°2014–006 sur la lutte contre la cybercriminalité (Law on Combatting Cybercrime)	Ministry of Posts, Telecommunications and Digital Development) (MPTDN)	State party to the United Nations Convention on the Use of Electronic Communications in International Contracts (NY, 2005)	State party to SOLAS, 1974
	SADC		Law No. 38/2014 Protection of personal data (Only available in French)		State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	State party to the 1988 SUA Convention and Protocol
			Loi n° 14/2015 sur les garanties et la protection des consommateurs (only available in French) – a law on consumer protection			
			Law No. 24/2018 on electronic transaction (available only in French)	Regulatory Authority for Communication Technologies) (ARTEC)		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Malawi (land-locked)	SADC	Inland Waters Shipping Act (Cap.71:01). Only applicable for inland waters	National ICT Policy: An ICT-led Malawi (2013)	Malawi Communications Regulatory Authority (MACRA)	MoU, Malawi–Uganda – Ministry of ICT	State party to SOLAS, 1974
	COMESA		National Cyber Security Strategy	Ministry of Information		State party to the 1988 SUA Convention and Protocol
			National ICT Master Plan (2014–2031)			
			Communications Act 2016 (No. 34 of 2016)			
			Data Protection Act (Bill)			
			Electronic Transactions and Cyber Security Act 2016 (No. 33 of 2016)			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Mali (land-locked)	CEN–SAD	Ordinance No. 02-026-P-RM of 7 February 2002 authorising the accession of the Republic of Mali to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, concluded in Rome on 10 March 1988	Digital Mali 2020: National Strategy for the Development of the Digital Economy	Ministère de la Communication et des Nouvelles Technologies de l'Information	Regional workshop on cybercrime/ cyber terrorism in G5 Sahel countries	State party to the 1988 SUA Convention and Protocol
	ECOWAS		Lois sur la protection des données à caractère personnel – Loi n° 2013-015 du 21 mai 2013 (available in French)	Agencie des Technologies de L'Information et de la Communication (AGETIC)		
			Loi n° 12 2016 relative aux transaction, aux echanges et services électroniques (available in French)	Brigade de Lutte Contre la Cybercriminalité, Brigade d'Investigation Judiciaire		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Mali (land-locked)			Code Penal: Loi n° 01-079 du 20 août 2001 (Penal Code) (2001) – Articles 264–271			
			Loi n°2019-056 Portant Répression de la Cybercriminalité (Law No. 2019-056 on the Repression of Cybercrime) (2019)			
Mauritania	AMU	The Loi n° 2013-029 portant code de la Marine marchande (Marine Merchant Code) – Book V, Chapter 1 deals with ship security. Particularly, articles 153 and 154 provide that ships are required to provide a security document of the navigation instruments, including a document of compliance with the International Safety Management (ISM) and the International Ship and Port Facility Security (ISPS) codes	Ordonnance n° 2006-031 relative aux instruments de paiement et aux opérations du commerce électroniques (available in French)	Ministry of Fisheries and Maritime Economy		State party to the 2005 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Mauritania		Article 2 of the Marine Merchant Code states that the provisions of future international conventions adopted by the Islamic Republic of Mauritania, or providing for it to accede, as well as the amendments to said conventions, or any other international conventions that it would ratify or expect to accede in the future, are fully applicable in their entirety		The Mauritanian Maritime Authority		
Mauritius	COMESA	Piracy and Maritime Violence Act 2011 (No. 39 of 2011). Article 3 States that any person who commits – (a) an act of piracy; or (b) a maritime attack, shall commit an offence and shall, on conviction, be liable to penal servitude for a term not exceeding 60 years	National Cyber Security Strategy 2014–2019	IT Security Unit – Ministry of Technology, Communication and Innovation	AU Convention on Cyber Security and Personal Data Protection – ratified	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Mauritius	SADC	The Piracy and Maritime Violence Act incorporates crimes provided under the SUA Convention, which makes it applicable to criminalising cybercrime, particularly, articles 4 and 5	Cybercrime Strategy 2017–2019	Mauritian Cybercrime Online Reporting System (MAUCORS)	SADC Workshop on Cybersecurity and public key infrastructure (PKI), host	State party to the 1988 SUA Convention and Protocol
		Merchant Shipping (Port State Control) Regulation 2018 (GN No. 114 of 2018)	Data Protection Act No. 20 (2017)	CERT-MU	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	
		Merchant Shipping (International Safety Management) (ISM Code) Regulations 2018 (GN No. 67 of 2018)	Electronic Transactions Act 2000		State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	
			Computer Misuse and Cybercrime Act (2003)	The Government Security Incident Response Team (G-SIRT)	GFCE, member	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Morocco	AMU	No specific maritime security instrument	Decree n. 2-11-509 (2011)- Completes Decree n. 2-82-673 on the organisation of the national defence administration with provisions on cybersecurity and information systems security	General Directorate of Information Systems Security	Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	State party to SOLAS, 1974
	Arab League	Loi du 31 mars 1919 relative au code de commerce maritime modified and completed by the law of 16 July 2010	The 2009 National Strategy for information Society and Digital Economy, and the 2012 National Cyber Security Strategy.	Strategic Committee for the Security of Information Systems	Project Cybersouth – Cooperation on cybercrime in the Southern Neighbourhood Region	State party to the 1988 SUA Convention and Protocol
			Decree n. 2-09-165 (2009) – Decree to implement Law n. 09-08 on personal data protection	National Commission for the Protection of Personal Data	Morocco–NATO (North Atlantic Treaty Organization) talks	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Morocco			Decree n. 2-11-508 (2011) – Decree to establish the National Commission for the Protection of Personal Data	Moroccan Computer Emergency Response Team (maCERT)	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	
			Law n. 07-03 (2003) – adds Chapter X to Book III, Part I to the Penal Code by defining cybercrime, on unauthorised access to information systems and data processing systems	The Moroccan General Directorate for National Security	Declaration of Intent, Spain– Morocco	
			Decree n. 2-15-712 (2016) – on the protection of sensitive information systems and critical infrastructures		GFCE, member	
			Decret relatif a l'échange électronique des données juridiques No 2-13-881 (available in French)		MoU, Malaysia– Morocco	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Morocco			Law 53-05 related to e-signatures and electronic exchange of legal data to facilitate the use of encryption and electronic certification		Security of Information Systems Cooperation, France–Morocco	
			Law No. 09-08 (2009) – Law on personal data protection			
Mozambique	SADC	Decree No. 71/2017 approving the Regulation of the International Code of Protection of Ships and Port Facilities	National Cyber Security Strategy (2016 draft, English)	Ministry of Transport and Communications	AU Convention on Cyber Security and Personal Data Protection – ratified	State party to SOLAS, 1974
			Electronic Transaction Act, Law No. 3/2017 (available in Portuguese)	The National Marine Institute		State party to the 1988 SUA Convention and Protocol
			Lei das Telecomunicacoes, 2004			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Mozambique			National Cyber Security Strategy (2017 draft, Portuguese)		Expressed views to the annual report of the UN Secretary-General on Developments in the Field of Information and Telecommunications in the Context of International Security	
Namibia	SADC	The ISPS and ISM Codes are enforced, as per article 144 of the Constitution	ICT Strategic Plan 2017–2022	Ministry of Information and Communication Technology	AU Convention on Cyber Security and Personal Data Protection – ratified	State party to SOLAS, 1974
			Cyber Security Strategy and Awareness Creation Plan	Proposed National Cyber and Security Incidence Response Team (NCSIRT)		State party to the 1988 SUA Convention and Protocol
			Electronic Transaction, Act No. of 2019 and Nov 2020 (Bill)			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Niger (land-locked)	CEN–SAD	No specific law regulating the maritime domain	Information and Communication Technologies Development Plan (PLAN NICI du Niger) (2004)	High Commission for New Technologies in Information and Communication	Regional workshop on cybercrime/ cyber terrorism in G5 Sahel countries	State party to the 1988 SUA Convention and Protocol
	ECOWAS		Loi n°2017-28 du 3 Mai 2017 relative à la protection des données à caractère personnel, révisé en 2019 (in French)		Cooperation, France–Niger	
			Loi n°2019-03 du 30 Avril 2019, portant sur les transactions électroniques (available in French)			
			Implementation Programme for the ICT Development Plan (2005–2010)			
			Penal Code – article 399			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Nigeria	CEN–SAD	Part XII of the Merchant Shipping Act 2007 deals with application of international conventions and protocols. Regulation 216 provides that, with the commencement of the Act, the listed conventions on maritime safety shall apply. Amongst the listed instruments SOLAS, ISPS and SUA are provided	National Cybersecurity Policy and Strategy	ngCERT – Office of the National Security Adviser	Cooperation, United States–Nigeria	State party to SOLAS, 1974
	ECOWAS	Ports (Related Offences, etc.) Act. An act to create offences related to unauthorised entry and carrying on of illegal transactions within any of the ports and to extend jurisdiction of the chief magistrate courts to the trial of the offences created by the Act. It does however not cover cybercrime or interference	Cybercrimes Act, 2015	Computer Crime Prosecution Unit, Department of Public Prosecutions	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	State party to the 1988 SUA Convention, Protocol and the 2005 Convention

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Nigeria			Electronic Commerce 2011 (Bill)	Nigerian Maritime Administration and Safety Agency	United Nations Convention on the Use of Electronic Communications in International Contracts (NY, 2005)	
			Data Protection Regulation	National Information Technology Development Agency	GFCE, member	
Republic of Congo	ECOWAS	Law n° 30–63 on the Code of the Merchant Marine	Draft Law on the Fight Against Cybercrime	Ministry of Postal Services, Telecommunications, and Digital Economy	AU Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974
		Order n° 2718 of 2 March 2011 setting the procedures to be followed for the implementation of maritime security measures applicable to port facilities		General director of the Merchant Marine – responsible to carry out tasks relating to the application of and compliance with the ISPS Code	United Nations Convention on the Use of Electronic Communications in International Contracts (NY, 2005)	State party to the 2005 SUA Convention and Protocol
		Order No. 6466 establishing a committee for the assessment of the security of ships and port facilities				

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Rwanda (land-locked)		No specific law regulating maritime security	National Cyber Security Policy (2015)	National Cyber Security Authority (NCSA)	AU Convention on Cyber Security and Personal Data Protection	
			ICT Sector Strategic Plan 2018–2024 (2017)	ICT Unit, General Directorate of Defence Policy and Strategy	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	
	COMESA		National Cyber Security Strategic Plan (2015)	Department of Information Technology and Cybercrime Investigations	MoU, Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States	
	East African Community (EAC)		Law n°N. 26/2017 – establishes the National Cyber Security Authority (NCSA) and determining its mission, organisation and functioning	Computer Security Incident Response Team (RW-CSIRT)	Signatory to the UNCITRAL Model Law on Electronic Commerce (1996) and the UNCITRAL Model Law on Electronic Signatures (2001)	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Rwanda (land-locked)			Law No.18/2010 relating to electronic messages, electronic signatures and electronic transactions		GFCE, member	
			Law governing Information and Communication Technologies (N°24/2016 of 18/06/2016)			
Sao Tome and Principe	CEN–SAD	Law No. 13/2007 establishing the Basic Law on Maritime Safety and Prevention of Marine Pollution (available in Portuguese)	Penal Code – article 240: Interference with data processing, incorrect software programming, incorrect or incomplete data, unauthorised use of data, and any other unauthorised intervention	General Regulatory Authority – mandated with implementation of the Basic Law on Telecommunications /3/2004 of 2 July 2004, which defines the necessary conditions for the establishment, management and operation of network telecommunications services	AU Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Sao Tome and Principe	ECOWAS	Decree-Law No. 4/2010 establishing legal measures and competent authorities for the implementation of the International Code of Vessels' and Harbours' protection. (available in Portuguese) It aims at defining the baselines in order to regulate the provisions prescribed in the ISPS Code and the formal establishment of the committee to guarantee the protection of transport carried out in maritime and harbour areas	Lei n°n. º 15/2017 Lei Sobre Cibercrime (Law on Cybercrime)	The National Maritime Authority (AMN)		State party to the 1988 SUA Convention and Protocol
Senegal	CEN–SAD	Law n°. 2002-22 of 16 August 2002 on the Merchant Marine Code (available in French)	National Cybersecurity Strategy 2022) (SNC2022) (2017)	Information and Communications Technology Department) (DTIC)	AU Convention on Cyber Security and Personal Data Protection – state party	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Senegal						
	ECOWAS		Loi n°2008–08 du 25 janvier 2008 sur les transactions électroniques (Available in French)	The National Agency for Maritime Affairs	United Nations Convention on the Use of Electronic Communications in International Contracts (NY, 2005)	State party to the 1988 SUA Convention and Protocol
		Decree n°. 2006-323 of 7 April 2006 establishing the National Marine Emergency Response Plan (PNIUM) (available in French)	Digital Strategy of Senegal 2016–2025)	CERT/CSIRT – To be established by the National Cybersecurity Strategy 2022	Budapest Convention	
		Law n°. 2005-17 of 3 August 2005 authorising the president of the Republic to ratify the African Maritime Transport Charter adopted in Addis Ababa, 15 December 1993	Law n°. 2008-11 on Cybercrime (Available in French)	High Commission responsible for the Coordination of Maritime Safety, Maritime Security and Protection of the Marine Environment (HASSMAR)	Cooperation, Senegal–France	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Senegal		Decree n°. 2006-322 of 7 April 2006 establishing the High Authority responsible for the Coordination of Maritime Safety, Maritime Security and Protection of the Marine Environment (HASSMAR)	Loi n° 2008–12 du 25 janvier 2008 portant sur la Protection des données à caractère personnel		Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	
		Ministerial Order No. 3902 of 14 March 2016 – Establishing and functioning of the National Technical Committee for Maritime Safety and Security			Cooperation, Senegal–the Netherlands	
					GFCE, member	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Seychelles	COMESA	Merchant Shipping (International Code for the Security of Ship and Port Facilities) Regulations [ISPS Code], 2020. Incorporates responsibilities of shipping companies and ships	National ICT Policy (2007)	Department of Information Communications Technology	State Party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	State party to SOLAS, 1974
		Subject to the Merchant Shipping Act and to any other law, SOLAS 1974 shall have the force of law in Seychelles. And as per article 240, the president may, by order published in the Gazette, declare that any convention relating to shipping, other than a convention referred to in section 85 as having the force of law in Seychelles, shall have effect in Seychelles, subject to the conditions, limitations or reservations (if any), stated in the order and the convention shall have effect accordingly	The Seychelles Maritime Safety Administration			State party to the 1988 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Sierra Leone	CEN–SAD	Merchant Shipping (Amendment) Act (No. 5 of 2008). An act to amend the Merchant Shipping Act, 2003 to provide for the licensing of shipping agents and the regulation of their activities and for other related matters	Cyber Security Policy (2016)	Police Cyber Crime Prevention Unit	AU Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974
	ECOWAS	Regulation 251 of the Merchant Shipping Act States that the safety convention shall, unless exempted by this Act, apply to all Sierra Leonean safety convention ships and all other safety convention ships while they are in Sierra Leonean waters	National ICT Policy of Sierra Leone (2009)	CIRT-SL (Cyber Incident Response Team Sierra Leone)	GFCE, member	
			National Cybersecurity and Data Protection Strategy 2017–2022	Sierra Leone Maritime Administration		

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Somalia	CEN–SAD	No specific law regulating maritime security	National ICT Policy & Strategy 2019–2024	Ministry of Posts, Telecommunications and Technology (MPTT)	Joint Statement, Djibouti–Somalia	State party to SOLAS, 1974
	IGAD	Book V of the Maritime Code of 1959 deals with maritime crimes in a very detailed manner; however, it cannot be extended to cybercrime			State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	
South Africa	SADC		National Cybersecurity Policy Framework (NCPF) (2012)	National Cybersecurity Advisory Council (NCAC)	Budapest Convention (Convention on Cybercrime) – signatory	State party to SOLAS, 1974
			Electronic Communications and Transactions Act No. 25 of 2002	ECS-CSIRT – State Security Agency	Represented at the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security	State party to the 1988 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
South Africa			Cyber Crime and Cybersecurity Bill (2016)	National Cybersecurity Hub	Agreement on cooperation, Iran–South Africa	
			Electronic Communications and Transactions Act, updated in 2010 (in English)	South African Maritime Safety Authority Act, 1998	UNCITRAL Model Law on Electronic Commerce (1996)	
			Cyber Crimes Bill (2017)	Cybersecurity Response Committee	MoU and Joint Statement, France–South Africa	
			Protection of Personal Information, Act 4 of 2013		Budapest Convention on Cybercrime	
Sudan	CEN–SAD	No specific law regulating maritime security law	Electronic Transactions Act, 2007	Sudan Computer Emergency Response Team (Sudan CERT)	State party to the 2009 Durban Resolution on Maritime Safety, Maritime Security and the Protection of the Marine Environment in Africa	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Sudan	COMESA	The 2010 Shipping Act does not include maritime security provisions	Cyber Crimes, Act 2007	Ministry of Communication Science and Technology		State party to the 1988 SUA Convention and Protocol
	IGAD					
United Republic of Tanzania	EAC	No specific law on maritime cybersecurity	National ICT Policy	TZ-CERT	Cooperation, Tanzania–Israel	State party to SOLAS, 1974
	Southern African Development Community	Part XVII of the Marchant Shipping Act – No.21 of 2003 – is dedicated to maritime security. It incorporates crimes provided under the SUA Convention, which makes it applicable to criminalising cybercrime, particularly, sections 342 and 343	Cybercrime Act, 2015	Department of Information Communication Technology	MoU for Cyber Security Cooperation, Tanzania–Republic of Korea	State party to the 1988 SUA Convention and Protocol

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
United Republic of Tanzania			Electronic Transaction Act 2015	Tanzania Communications Regulatory Authority (TCRA)	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	
			Data Protection Bill 2013	Tanzanian Ports Authority	GFCE, member	
			The National Payment System Act, 2015		State party to the Djibouti Code of Conduct and the 2017 Jeddah Amendment	
Togo	CEN–SAD	Law n°. 2016-028 of 11 October 2016 on the merchant marine code. The provisions of this code also apply to breaches resulting from maritime, river or lagoon activities observed in waters under national jurisdiction	Policy Declaration of the Digital Economy Sector for 2018–2022 (2017)	Cyber Defence Africa (CDA)	AU Convention on Cyber Security and Personal Data Protection – signatory	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Togo	ECOWAS	Book III of the Merchant Marine Code organises maritime navigation, in particular navigation safety; classification societies; marine casualties and incidents (in accordance with IMO resolutions and the International Convention for the Prevention of Pollution from Ships (MARPOL) 73/78);	Bill on cybersecurity and the fight against cybercrime (2018)	Security Operational Centre (SOC)		State party to the 1988 SUA Convention, Protocol and the 2005 Convention
		Law n°. 2016-004 of 11 March 2016 on the fight against piracy, other illicit acts and the exercise by the state of its police powers at sea (available in French)	Loi sur les transactions électroniques No. 2017-07	Computer Security Incident Response Team (CSIRT)		
Tunisia	CEN–SAD	Code de Commerce maritime, 1984, as amended in 2010	Penal Code – article 199 bis and ter	National Agency for Computer Security (ANSI)	Project Cybersouth – Cooperation on Cybercrime in the Southern Neighbourhood Region	State party to SOLAS, 1974

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Tunisia						State party to the 1988 SUA Convention and Protocol
	Arab League	Law n° 77-28 of 30 March 1977 promulgating the Maritime Disciplinary and Penal Code. This law is applicable only to the persons on board any Tunisian ship, except for war ships and offences concerning the navigation police, and punishes any person embarked on a Tunisian or foreign vessel who in Tunisian territorial waters does not comply with the regulations or orders emanating from the maritime authority, and relating to the water police	Law n°. 2004-5 on cybersecurity – establishes the Agence Nationale de Sécurité Informatique and its mandate; Establishes general rules on the protection of information systems and network security	The Office of Merchant Marine and Ports	Declaration of Intent, Spain–Tunisia	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Tunisia			Electronic Exchanges and Electronic Commerce Law No. 83 of 2000	The National Council for Port and Maritime Transport Security – established by the Decree No. 2004-2534 relating to the creation, composition and operating procedures of the National Council for Port and Maritime Transport Security	GFCE, member – a global platform for countries, international organisations and private companies to exchange best practices and expertise on cyber capacity building	
				National Commission for the Law of the Sea	AU Convention on Cyber Security and Personal Data Protection	
Uganda (land-locked)	COMESA	No specific law regulating the maritime security sector	Computer Misuse Act, 2011	National Information Technology Authority–Uganda (NITA-U)	MoU, Malawi–Uganda	State party to SOLAS, 1974
	IGAD		Electronic Transactions Act, 2011	Uganda National Computer Emergency Response Team/ Coordination Centre (CERT.UG/CC)	Cybersecurity Alliance for Mutual Progress – CAMP Initiative, member	State party to the 1988 SUA Convention

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Uganda (land-locked)			The Data Protection and Privacy Bill, 2015		Cooperation, Uganda–Israel	
			Computer Misuse Act, 2011		MoU, Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States	
					Cooperation, Uganda–Israel	
					Signatory to UNCITRAL Model Law on Electronic Commerce (1996) and UNCITRAL Model Law on Electronic Signatures (2001)	
					GFCE, member	

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Zambia (land-locked)	COMESA	No specific law regulating the maritime sector	National ICT Policy (2006)	Zambia ICT Authority	AU Convention on Cyber Security and Personal Data Protection – signed but not ratified	
	SADC		The Electronic Communications and Transactions Act No. 21 (2009)	Zambia Computer Incident Response Team (zmCIRT)	Cooperation, Zambia–Israel	
			Computer Misuse and Crimes Act No. 13 (2004)		UNCITRAL Model Law on Electronic Commerce (1996)	
			The Cyber Security and Cyber Crimes Act, 2021		UNCITRAL Model Law on Electronic Signatures (2001)	
			Data Protection Act, 2020,			

Country name	Regional grouping	National maritime instruments, acts or regulations dealing with maritime security	General cyber security act or strategy	Authorities of the member state governments with regard to protecting the ICT elements of the maritime sector against cyber attacks	National and international cooperation mechanisms	IMO Resolution MSC.428(98)
Zimbabwe (land-locked)	COMESA	No specific law regulating the maritime sector	National Policy for ICT	Ministry of Information Communication Technology, Postal and Courier Services		
	SADC		Cyber Security and Data Protection Bill (2019)			
			Bill – Electronic Transactions and E-commerce, 2013			
			Bill – Data Protection 2016 (in English)			