SCIENTIA MILITARIA
South African Journal of Military Studies

Volume 51
Number 3
2023

ISSN 2224-0020 (online) | ISSN 1022-8136 (print)

scientiamilitaria.journals.ac.za

IN MEMORIAM

ARTICLES

BOOK REVIEWS

Scientia Militaria

South African Journal of Military Studies

ISSN 2224-0020 (online); ISSN 1022-8136 (print)

The Editor, Scientia Militaria, Faculty of Military Science (SA Military Academy), Stellenbosch University, Private Bag X2, Saldanha 7395, South Africa

Scientia Militaria
Volume 51
Number 3
2023

Click on icon to navigate to articles/reviews

Contents

South African Journal
of Military Science

Scientia Militaria
2023, VOL. 51, NO. 3, i-viii
DOI: 10.5787/51-3-1424

SCIENTIA MILITARIA
South African Journal of Military Studies

South African Journal *of Military Science*

Guest Editorial

As humanity seeks to exploit new frontiers in pursuit of greater wealth, prosperity and well-being, more intensive use of ocean territories and the exploration of more remote areas of the oceans unfold.[1] Population growth, declining land-based resources, technological advances, geopolitics, and climate change alongside growing consumption trends dovetail and compete to harvest the oceans for space, food, and materials. Early in the twenty-first century, several ocean debates took place, rose rapidly to more maturity, and shaped a set of paradigms broadly depicting maritime security, the blue economy, ocean health, and blue justice.[2] While the four paradigms serve as ordering mechanisms for analysing the complexities and competing interests, views and actors at play, operational maritime sectors hold their own demands, difficulties and tribulations. In addition, threats, vulnerabilities and opportunities manifest in each of the ocean sectors to further complexity and cut across each other to a larger or lesser extent. The inherent dynamics of the aforementioned plays out above, on the surface and below the surface of the oceans in visible and invisible ways that affect the myriad of activities depending on the oceans as a stock and flow resource.

The growing use of the oceans embedded in the range of actions undertaken in sectors, such as shipping, renewable and non-renewable energy extraction, harvesting of living resources, operating ports, subsea infrastructure, and monitoring the oceans as an environment has not only expanded in scope, but in complexity as well. In addition, actors operating in the different realms of maritime security, the blue economy, the environment, and justice all depend upon a growing common denominator to operate effectively, efficiently and safely: access to modern technologies and assurances of a safe and secure cyber-operating environment to protect the extensive information flows at play.

In lay terms, maritime cybersecurity entails safeguarding digital systems, networks, and data within the maritime domain from cyber threats. It encompasses measures to prevent unauthorised access, data breaches, and disruptions to navigation, communication, vessel control, and port operations. Maritime cybersecurity is also key to promote the sustainable,

1 JB Jouffray, R Blasiak, AV Norström, H Österblom & M Nyström, 'The Blue Acceleration: The Trajectory of Human Expansion into the Ocean', *One Earth*, 2(1), (2020), 43–54.

2 C Bueger & F Mallin, 'Blue Paradigms: Understanding the Intellectual Revolution in Global Ocean Politics', *International Affairs*, 99(4), (2023), 1719–1739.

safe and productive utilisation of the oceans of the world. Modern technology underpinned by an efficient cyber sector forms the backbone of maritime operations. The cyber nexus is also a vulnerability for functional maritime systems as cyber threats continue to grow as a critical hazard to maritime activities. Threats emanate from activists, criminals and terrorists for personal, economic and ideological gains. The actors and the threats they bring about create complex problems for those dependent upon safe and secure functioning of their technology-based systems, information, and data contained in the virtual and physical assets at play.[3]

Some dependencies that rely heavily on maritime cybersecurity and vulnerable to cyber threats entail the following domains: technological dependency, use of the oceans, supply chain continuity, port operations, prevention of financial loss, trade facilitation and compliance, innovation and digital transformation, and investor confidence.

Technological dependency is relevant for modern maritime operations that rely on advanced technology, including navigation systems, communication networks, and vessel control systems. These technologies are susceptible to cyberattacks that can disrupt navigation, communication, and other vital functions, potentially leading to accidents, collisions, and loss of life.[4] Economic use of the oceans depends on cybersecurity playing a pivotal role in enhancing the productive use of the oceans, and so does safeguarding the maritime industry against cyber threats and ensuring the uninterrupted flow of trade, communication, and operations. Here one finds several ways in which cybersecurity contributes to the economic utilisation of the oceans:

Supply chain continuity underpins the broader maritime industry as the backbone of global trade, and facilitates the movement of goods across continents. Cyberattacks targeting shipping companies, port operations, or logistic networks can disrupt supply chains, leading to delays in shipments and increased costs. Robust cybersecurity measures protect against such disruptions by ensuring the smooth flow of goods and minimising economic losses in a world where time is truly money.[5]

Port operations efficiency resonates with being vital hubs for loading and unloading cargo, and they rely heavily on digital systems for operations, such as vessel tracking, cargo handling, and customs clearance. Cybersecurity measures safeguard these systems against unauthorised access, data breaches, and potential disruptions, allowing ports to maintain high levels of efficiency and productivity.[6]

---

3 MS Karim, 'Maritime Cybersecurity and the IMO Legal Instruments: Sluggish Response to an Escalating Threat?', *Marine Policy*, 143 (2022), 105-138.

4 International Maritime Organisation, *Guidelines on Maritime Cyber Risk Management*. MSC-FAL.1/Circ.3/Rev.2. 7 June 2022.

5 S Kumar & RR Mallipeddi, 'Impact of Cybersecurity on Operations and Supply Chain Management: Emerging Trends and Future Research Directions', *Production and Operations Management*, 31(12), (2022), 4488–4500.

6 I de la Peña Zarzuelo, 'Cybersecurity in Ports and Maritime Industry: Reasons for Raising Awareness on this Issue', *Transport Policy*, 100 (2021), 1–4.

Prevention of financial loss requires dependable protection against cyberattacks that may result in financial losses due to ransom demands, theft of sensitive financial information, or fraudulent activities. By implementing cybersecurity protocols, maritime companies can mitigate the risk of financial losses arising from cyber incidents, protect their assets, and secure investments.[7]

Trade facilitation and compliance follows in the wake of many countries and industry clients requiring compliance with cybersecurity standards, such as the Tallinn Manual 2.0 to ensure secure trade operations, and equally so for maritime trade that remains at the core of world trade.[8] Adhering to set standards enables companies to continue participating in international trade with minimal disruptions caused by cybersecurity-related regulatory issues to ultimately promote economic growth.[9]

Innovation and digital transformation reside at the heart of the maritime industry, and the way it embraces digital transformation to enhance operations, reduce costs, and improve customer experiences. This digital shift however also attracts cybersecurity challenges. By addressing these challenges effectively, the industry can confidently explore and adopt innovative technologies that enhance economic competitiveness under the banner of cybersecurity best practices.[10]

Investor confidence grows when robust cybersecurity practices demonstrate the commitment by a company to safeguard its operations and assets. This fosters investor confidence and encourages investments in the maritime sector, supporting growth and expansion opportunities.[11] As the growing economic landscape of the future, building confidence in technologies that promote cyber efficiency and these technologies being encased in cybersecurity are akin to confidence-building measures.

Being lax, unprepared or even ignorant about maritime cyber risks holds implications for maritime players, their interests and business enterprises. The maritime sector is a current and future cornerstone of the global economy, with shipping and port operations facilitating the movement of goods. Damaging cyberattacks on maritime infrastructure, such as ports, energy installations, and subsea cable networks can disrupt supply chains,

---

7 D Reva, 'Maritime Cyber Security: Getting Africa Ready', *ISS Africa Report*, 29 (2020), 1–16.

8 MN Schmitt (ed.). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge: Cambridge University Press, 2017)

9 O Melnyk, S Onyshchenko, O Onishchenko, O Shumylo, A Voloshyn, Y Koskina & Y Volianska, 'Review of Ship Information Security Risks and Safety of Maritime Transportation Issues', *TransNav: International Journal on Marine Navigation & Safety of Sea Transportation*, 16(4), (2022), 717-722.

10 EP Kechagias, G Chatzistelios, GA Papadopoulos & P Apostolou, 'Digital Transformation of the Maritime Industry: A Cybersecurity Systemic Approach', *International Journal of Critical Infrastructure Protection*, 37 (2022).

11 R Hopcraft, K Tam, JDP Misas, K Moara-Nkwe & K Jones, 'Developing a Maritime Cyber Safety Culture: Improving Safety of Operations', *Maritime Technology and Research*, 5(1), (2023), 1–18.

delay shipments, and result in significant financial losses for businesses and nations. Successful cyberattacks on maritime systems in shipping can compromise vessel stability and navigation, leading to accidents, such as oil spills and environmental damage. Ensuring cyber security is thus crucial to prevent incidents that could have long-lasting ecological consequences.[12] Maritime cyberattacks can be used as a tool by state and non-state actors to undermine national security. Disruption of naval operations, coastal surveillance, or navigation can pose threats to the defence capabilities and territorial integrity of a country.[13] Collectively the threats outlined threaten maritime security, blue economy expectations, the blue environment, and the potential to upset national, regional and even international ocean agendas and expectations.

Heeding best practices is an important risk mitigation measure and necessary for actors to remain in step with the codes and conventions of the International Maritime Organization (IMO) and related international bodies. The latter entities have recognised the significance of maritime cybersecurity by establishing guidelines and regulations to help manage cyber risks. Failure to comply with these regulations not only undermines safety but could also lead to legal consequences and sanctions in an ever-growing maritime community.

Africa is not spared the threat and disruptive consequences of maritime cyberattacks and vulnerabilities. Real and potential, African countries have been subject to and must shield themselves against maritime cyber threats.[14] Awareness and regulatory measures and implementing best practices are important steps for every African coastal state and their maritime entities to combat cybersecurity risks. The continent is utterly reliant on seaborne trade, and houses large landlocked economies and vulnerable populations. The African oceans harbours food resources, data cable networks, energy hubs, critical sea lines of communication and ports as connecting hubs for the overall economy of the continent, its blue economy agenda, and environmental security, and thus requires maritime security and blue justice. The aforementioned matters are also interconnected and operate efficiently thanks to cyber-based connectivity and buttressed by cybersecurity to operate securely, free of threats and – if disrupted – can be corrected speedily.

In a world that has turned irrevocably to enter the oceans as a long lingering frontier, technology is key to maritime operations raising robust cybersecurity as paramount for the safe and productive use of the oceans. In all of this, Africa cannot stand sidelined or idle. The interconnectedness of maritime systems, economic implications, growing environmental concerns, and national security considerations all highlight the urgency of mitigating maritime cyber threats, and African voices must be heard in debates. For this

---

12 M Elgan, 'Maritime Cyber Security: A Rising Tide Lifts All Boats', *Security Intelligence*, 4 November 2021. Available at: <https://securityintelligence.com/articles/maritime-cybersecurity-rising-tide/> [Accessed on 17 August 2023].

13 W Loomis, VV Singh, GC Kessler & X Bellekens, *Raising the Colors: Signalling for Cooperation on Maritime Cybersecurity* (Atlantic Council, 2021).

14 J Cronje & G Martin, 'Experts Warn of Increasing Cybersecurity Threats for the African Maritime Industry', *defenceWeb*, 22 October 2002. Available at: <https://www.defenceweb.co.za/featured/experts-warn-of-increasing-cyber-security-threats-for-the-african-maritime-industry/> [Accessed on 17 August 2023].

Special Issue of *Scientia Militaria*, Volume 51, Issue 3, 2023, the African maritime domain is approached in broad terms, including but not limited to the influence of new technologies and related threats to the African maritime sector, offshore oil and gas sectors, maritime transportation and maritime security, maritime cybersecurity governance, maritime trade and logistics chains, blue economy, African navies, border security and digital leadership.

The articles selected offer an insightful analysis and practical solutions to promote better policy and practice across the continent.

Tefesehet Hailu Sime (African Union Commission) addresses maritime cybersecurity: the need for a regional approach by the African Union and its member states in her contribution. Africa is referred as 'the largest island' on earth with oceans on all sides of the continent and a coastal line of 26 000 nautical miles. On top of that, 38 out of 55 African states are coastal countries or islands, and 90% of African trade is seaborne. These trading activities are facilitated by over a hundred port facilities in the region. The continent is therefore dependent on well-run ports, regulated shipping, and effective protection of its maritime resources. At national and regional level, there are however very few legal instruments specifically addressing the issue of cyberattacks on port facilities. Given the lack of attention that is given to this important aspect of maritime security and the lack of collective action from African states, the article seeks to analyse how cyber technology has affected the maritime domain of Africa as a whole. The article also reports on the consequences that could manifest should the cybersecurity of ships, ports, and their critical infrastructure continue to be ignored. In particular, the article addresses the following questions: to what extent do cyber vulnerabilities of African states extend offshore, and what should be done to address those vulnerabilities? What is lacking from the Convention on Cyber Security and Personal Data Protection adopted by the African Union? If maritime cybersecurity should be given focused attention, what is the task expected by the African Union and its member states? Taking into consideration the importance of this issue and in an attempt to address the research questions, the author sought to engage with policies, laws, regulations and other documents (both national and regional) that are currently guiding the area of maritime cybersecurity. Furthermore, the lack of maritime cybersecurity, and the resultant threats and vulnerabilities are addressed, hypothetical incidents are considered and previous incidents assessed, and current mitigation techniques and initiatives explored. After identifying the gaps in the legal framework adopted at national and regional level, policy recommendations are provided that could be implemented by the African Union and that could assist African states to tackle the challenges resulting from cyberattacks in the maritime domain.

Elsie Tachie-Menson (KAIPTC) covered the topic of maritime crime and cybercrime across the Gulf of Guinea: a hand-in-glove affair. As technology expands and spreads worldwide, the maritime industry and maritime crime are evolving rapidly. Although the increased use of digital technologies has proved beneficial in the effective and timely delivery of activities, such as maritime surveillance, policing, monitoring, and early warning, it also introduced serious drawbacks that affect its network of actors. This amalgamation can be attributed to geographical location, surveillance, and navigation systems of ports, vessels, and other state intuitions. With the emergence of cyber threats,

West Africa is poised to face a dual-pronged threat at its ports and shores, affecting the broader security environment of coastal states as more actors in the maritime domain increasingly use digital technologies. Moreover, these threats demonstrate a path for maritime criminals to evolve into maritime cybercriminals. The central theme of this article is the connection between cybercrime and maritime crimes, and the specific cybercrimes that have found a lucrative avenue in the maritime industry. The author also discusses cybercrime in maritime criminal activities occurring in West Africa and the implications for the maritime and cyber landscape of the region. Finally, she concludes with approaches for dealing with the risks posed by cyber maritime risks.

Chris Myers (Maritime consultant and researcher) contributed with a piece on assessing and managing risk within the African shipping sector. The African shipping sector is a significant enabler of trade within Africa, and of trade between Africa and the world. It sources and integrates technical systems of foreign suppliers and service providers into its vessels, ports, and maritime critical infrastructure that are cyber-enabled. Unfortunately, while providing the required functionality, these technical solutions create security vulnerabilities that place the African shipping sector at risk if security within the maritime cyber domain is taken for granted. Through this article, the author seeks to raise awareness of maritime cybersecurity in the context of the African shipping sector, and propose pragmatic steps to achieve such awareness.

Barend Pretorius and Brett van Niekerk (DUT) wrote on Industrial Internet of Things (IIoT) security for the maritime and related domains, the case of South Africa. The advent of the Fourth Industrial Revolution (4IR) has seen a rapid increase in connected 'smart devices' known as the Internet of Things (IoT). While this 'revolution' is most noticeable in commercial devices, there has been an 'evolution' in industrial devices, known as the IIoT. As Africa, and in particular South Africa, is racing to compete in the 4IR, various sectors, including the transportation sector, are introducing innovative projects. However, IoT and IIoT present cybersecurity risks. Cybersecurity itself is also a key component of 4IR; yet, organisations often neglect to consider the security implications of IIoT. A mixed-methods study was conducted to assess the security implications of IIoT in the South African physical transportation sector. Questionnaires were used with those working in the relevant fields to obtain quantitative data, and qualitative document analysis was conducted on frameworks for IoT and IIoT. The research aimed to evaluate and prioritise cyber threats, vulnerabilities, and appropriate countermeasures to mitigate the security risks associated with implementing IIoT in the transportation sector.

Brett van Niekerk (DUT) made a second contribution on a more specialist theme covering vulnerability of South African commodity value chains to cyber incidents. A commodity value chain can be considered as the 'route' from the source (provider) to the destination (client), including the various modes of transportation. This will often include some form of road or rail transport to a port for export to a destination country. Due to the rise in cybercrime and state-backed cyber operations, these commodity value chains may be disrupted, having a cascading affect down the value chain. Previous research considered this as a form of economic information warfare, and has indicated that state-sponsored cyber operations to disrupt a commodity intentionally would most likely fall below

the threshold of 'use of force' or 'attack' under international law. Subsequently, two pertinent instances of cyber incidents at ports have occurred: the disruption of a major Iranian port, and a ransomware incident at a South African major freight and logistics state-owned enterprise. Following the disruption resulting from the ransomware incident affecting South African freight organisations, there is a need to analyse the vulnerabilities of the sector to malicious cyber interference further. Expanding previous research, the author provides a specific look at the major commodity value chains in South Africa, their possible vulnerability to cyber incidents, and the potential implications thereof. In addition, publicly available information on the responses to the ransomware incident are discussed to gauge national readiness to crisis manage a major disruption to the primary trade mechanisms in the country.

A selection of book reviews by Dries Putter, André Wessels, Leon Steyn, Allan du Toit and Tilman Dedering concludes this special issue of *Scientia Militaria*.

The Guest Editors
Francois Vreÿ and Denys Reva

Scientia Militaria
2023, VOL. 51, NO. 3, ix-x
DOI: 10.5787/51-3-1425

SCIENTIA MILITARIA
South African Journal of Military Studies

South African Journal *of Military Science*

In Memoriam

Prof Ian Liebenberg, 1960-2023

With disbelief and a deep sadness, we heard of the sudden passing of Professor Ian Liebenberg on 11 October 2023. Ian was co-editor of *Scientia Militaria* from 2010 to 2016, and a colleague in the Faculty of Military Science, Stellenbosch University as the Director of the Centre for Military Studies. Since 2020 Ian was Professor in Politics at the University of Namibia. His distinguished academic career spanned the most important years of South Africa's transition and democratic consolidation.

Ian's contribution to the struggle for national liberation and the transition away from authoritarianism was not just academic, but embodied the spirit of dialogue, critique, and activism. Ian participated in the Dakar Meeting of 1987, where the still-banned ANC met with progressive South Africans in search for a democratic alternative in South Africa.

One of the main avenues of Ian's scholarly research concerned our transition away from authoritarian rule towards democratic civil control over the military in post-liberation South Africa. Ian's early work, such as the books he co-edited *The Long March: The Story of the Struggle for Liberation in South Africa* (1994) and *The Hidden Hand: Covert operations in South Africa* (1998) document the political crisis, the dynamics of reform and revolt, and the long haul to democracy. To this essential subject Ian brought the mind of a philosopher, the eye of a sociologist, the language of a political scientist, and the sensibilities of a historian. His education and writing were brought alive in the heart of a humanist.

That this was a deeply personal task was made clear in his first contribution to *Scientia Militaria*, titled 'The quest for liberation in South Africa', where he notes that: "To write an inclusive history of liberation and transition to democracy in South Africa is almost impossible … I will draw on my own work in the field over the past fifteen years as well as other sources … A wide variety of sources and personal experiences inform this contribution ... Also needless to say, one's own subjectivities may arise - even if an attempt is made towards intersubjectivity." This combination of academic discourse and self-reflection was a theme. In his 2019 contribution to *In Different Times: The War for Southern Africa 1966-1989* edited by Ian Van der Waag and Albert Grundlingh, he subtitled his chapter 'An auto-ethnographic exploration of the (citizen) conscript in South Africa' where he recounted an auto-biographical understanding of the times in which he lived. This was not just his own individual experience, but emblematic of the wider socio-political, and perhaps even the universal.

Ian's breadth of thinking and understanding is reflected in the range of contributions of over 100 texts that have included journals such as *Politeia* (also as Guest Editor), *South African Journal of Philosophy* (also as book review Editor), *Journal for Contemporary History, South Africa Public Law, Journal of Public Administration, Society in Transition, Acta Academica, Journal for Transdisciplinary Research in Southern Africa, Journal of Asian and African Studies, Peace Review, Armed Forces and Society,* and *Scientia Militaria* (as Editor since 2009). The nature of his work, Ian's multidisciplinary approach produced many partnerships, joint research and publication ventures. Internationally, these collaborations enlightened on the history of relations between Russia and South Africa from the 1890s, on the participation of Cuba in southern Africa, and on views on national security and defence from the Global South. His book, with Jorge Risquet and Vladimir Shubin, *A Far-Away War: Angola 1975-1989*, is an important scholarly contribution bringing a wider perspective on that conflict, including previously unpublished archival photos, and a comprehensive bibliography for researchers and students.

However, Ian's contribution to research extended well beyond his own publications: Ian was always supportive of young researchers, freely giving advice, feedback and support selflessly and providing encouragement to those submitting articles for the first time. At a time of 'publish or perish' Ian's advice that academic publishing was not about feeding career ambition, but about empowering critical engagement. In a recent email he shared the words of Dietrich Bonhoeffer that "One must take the risk of saying things that are in dispute, provided that vital problems are thereby raised". Ian's life-work and contribution to academia purely reflect this.

His energy, enthusiasm, wit, and stories will long remain with friends, old and new alike. Ian leaves Mariaan and their two children, and our thoughts are with them.

Raymond Steenkamp Fonseca
Stellenbosch University

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.

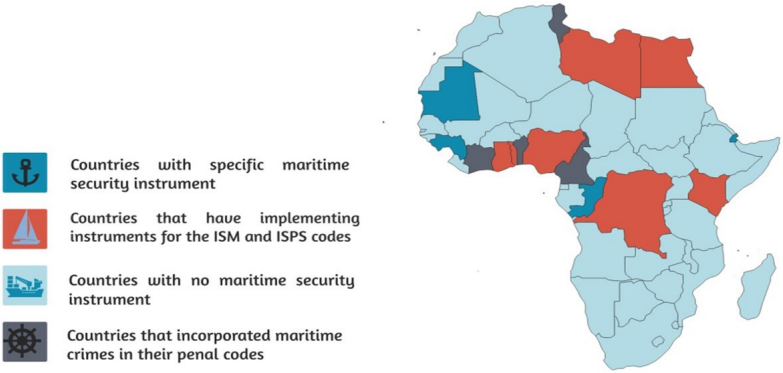


Figure 1: The implementation of the IMO instruments by African states

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).

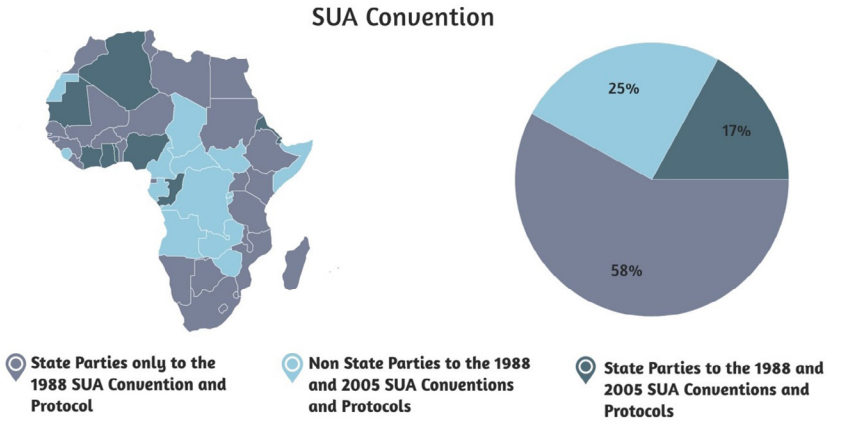


Figure 2: The adoption of the SUA convention by African states

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.

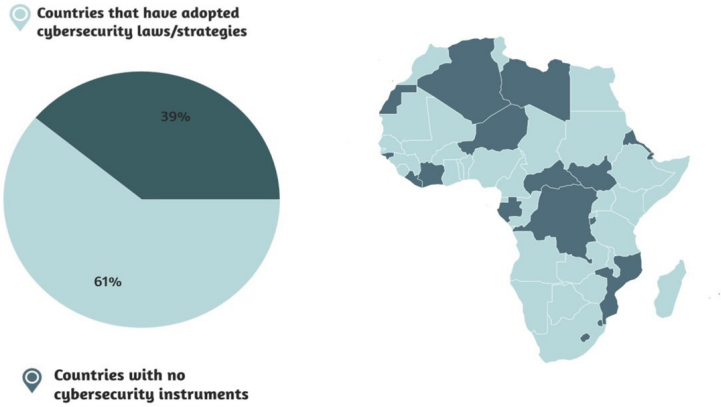


Figure 3: African countries with cybersecurity laws and strategies

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)			

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

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

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

Abstract

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

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

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

Introduction

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

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

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

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

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

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

The Rational Choice Approach and Organised Crime

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The case of cybercrime in West Africa

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

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

Table 1: Respective internet penetration rates of West African states

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

Source: World Bank (2021)

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

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

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

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

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

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

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

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

The case of maritime crime in West Africa

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

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

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

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

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

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

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

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

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

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

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

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

Table 2: Classification of blue crimes

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

Source: Bueger and Edmunds (2017)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

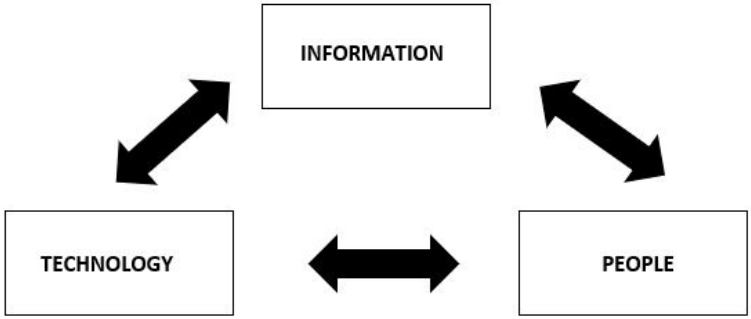


Figure 1: The three elements of cyber operations in the maritime domain

Source: Author's own construct

People

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

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

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

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

Information

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

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

Technology

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

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

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

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

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

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

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

A dual-dimensional approach to addressing maritime cybercrimes

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

Conclusion

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

About the Author

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Scientia Militaria
2023, VOL. 51, NO. 3, 113-132
DOI: 10.5787/51-3-1428

The African Shipping Sector, the Need for and Means to Achieve Effective Cyber Risk Management

Chris Myers
Security Institute for Governance and Leadership in Africa
Stellenbosch University

Abstract

The African shipping sector is a significant enabler of trade within Africa and trade between Africa and the world. African countries are sourcing and integrating technical solutions from foreign suppliers and service providers within their maritime domain. Such technologies are embedded within and enable functionality within transportation systems, port and navigation infrastructure, telecommunications infrastructure, downstream oil and gas infrastructure, and various national defence and security systems. Unfortunately, while providing the required functionality, these technical solutions create security vulnerabilities that place the African shipping sector and national interests at risk if security within the maritime cyber domain is taken for granted. The study on which this article is based firstly sought to identify and deconstruct the technology and associated vulnerabilities within the African maritime domain. Secondly, the research attempted to determine how national strategy and policy could be used to manage these security vulnerabilities to raise awareness of maritime cybersecurity in the context of the African shipping sector and propose pragmatic steps to achieve it.

Keywords: African shipping sector; security vulnerabilities; maritime cyber domain; maritime cybersecurity

Introduction

The international shipping industry is a global enterprise that makes extensive use of cyberspace to conduct its business. With a growing awareness of threats in cyberspace, the industry has become increasingly concerned with the possible disruption of its business by cyber-related threats.

The growing awareness of cyber vulnerabilities and the experience of loss relating to cyberattacks and incidents have prompted the international shipping industry to act and attempt to manage its cybersecurity. These actions are applied throughout the international shipping industry and in all regional shipping sectors.

As a regional element of the international shipping industry, the African shipping sector is connected to the same elements of cyberspace, conducts the same business, and faces the same potential of business disruption from cyber threats as the international shipping industry. It therefore needs to consider the implications of cyber-related threats to its ongoing business.

To this end, the study on which this article is based sought to establish an understanding of the international shipping industry, its associated cyber domain, cybersecurity, the nature of cyber incidents and vulnerabilities, and the effectiveness of the existing cybersecurity practices of the shipping industry. Following that, the article presents a consideration of these elements in the context of the African shipping sector, identifies the potential high-order consequences of cyber threats to the sector, and proposes pragmatic mitigations to manage the cyber risk of the shipping sector.

The international shipping industry

The international shipping industry is the maritime component of the global transportation and logistics system. The United Nations Conference on Trade and Development (UNCTAD) has described the shipping industry as being the "backbone of globalized trade and manufacturing chain". Shipping carries over four fifths of world merchandise trade by volume, and has cargo passing through ports integrated with the value chain and manufacturing networks of global trade. Ships move between the key regions of Africa, the Americas, Asia, Europe, and Oceania (UNCTAD, 2019: 4, 6, 9–14).

The industry has been described as a complex system consisting of independent and rational stakeholders, grouped into sectors that interact in recognisable patterns to ensure the global movement of cargo between nodes within the global maritime and supply chain network (see Raaidi, Bouhaddou & Benghabrit, 2018). Vessels are used to transport cargo between nodes, with the nodes being ports that allow the loading and discharging of cargo from these vessels. Stakeholders include shipping companies, shipping service providers, commodity producers and port authorities, while sectors include international maritime transport, maritime auxiliary services, and port services (Caschili & Medda, 2012: 1–6, 10; Zagan, Raicu, Hanzu-Pazara & Enache, 2017: 221).

Ports are described as important links in the global logistics chain, and as "self-organized ecosystem(s) within a larger self-organized ecosystem of the global shipping industry" within which stakeholders integrate and exchange data to achieve collaborative aims (Alcaide & Llave, 2020: 548; Lind *et al*., 2020: 12–13).

In early 2019, the world shipping fleet comprised of over 95 000 vessels of different designs carrying a range of cargo types (UNCTAD, 2019:4). Vessel designs incorporate a wide range of sub-systems and technologies with a growing trend toward the incorporation of digitised, automated and Internet of Things (IoT) technologies, and the likely future introduction of artificial intelligence (AI), autonomous, and smart shipping technologies (Lambrou, Watanabe & Lida, 2019: 6). The industry makes extensive use of information and communications technologies (ICTs) to achieve global connectivity, and of information technology (IT) to enable the automation of a wide range of ship-borne navigation, communications, and control systems (Boyes, 2013: 57, 59).

The industry is both adaptive and evolving. In 2001, it was predicted that the twenty-first century shipping industry would:

- be required to provide global transport services as part of an integrated logistics service provider;
- build a global information network shared by multiple users within the supply chain; and
- the port would no longer be the terminal of transportation, but rather an element within the "whole transport chain in international trade" (You-Sheng et al., 2001: 23–24).

Since the 2008–2009 financial crisis, shipping companies have changed their business model to affiliate with and then gain ownership of shipping terminals, thereby achieving integration within the onshore logistics infrastructure and associated services (Sheffi & Gray, 2019: 3–4).

Based on this, the international shipping industry consists of three main elements, namely vessels, ports, and associated stakeholders. Together, these form a large and complex internationally displaced industry that routinely exchanges data within the maritime cyber domain while moving cargo within a global supply chain. This constitutes a reliance on cyber connectivity to manage and maintain normal business activities, which will likely increase as its digital transformation process continues and new technologies are adopted within industry.

The number of vessels, ports, and stakeholders connected to and globally active within the maritime cyber domain is significant. All are connected within the same single maritime cyber domain and adopt the same cybersecurity practices. By understanding what the maritime cyber domain is, and which cybersecurity practices the industry has adopted, it should be possible to make an initial assessment of the readiness of the international shipping industry to manage its cybersecurity, and to consider the implications thereof for the African shipping sector.

Defining the maritime cyber domain

The United Kingdom (UK) National Cyber Security Centre (NCSC) describes cyberspace as "a global domain within the information environment consisting of an interdependent network of information system infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers" (NCSC, 2019: 820). This global domain allows a virtual connection and real-time digital data flow to be maintained between geographically remote systems and devices on board vessels, within ports, and used by stakeholders.

This is the "extension of the littoral under the influence of digital technology" where three elements of maritime domain cyber operations interplay, namely information (the data supporting and sustaining maritime operations), technology (computer systems within ports and vessels that are physically and digitally vulnerable), and people (who interact with one another and computer systems). Within this maritime cyber domain, "every intersection of human and machine … the possibility for error, manipulation,

coercion, or sedition" exists, and it is the protection of these intersections and elements of the maritime cyber domain that cybersecurity is intended to achieve (Fitton, Prince, Germon & Lacy, 2015: 2–7, 15).

From this, the maritime cyber domain attack surface[1] will include all intersections between and within individual ports, stakeholders, and vessels, creating a significant and complex threat landscape.[2]

Cybersecurity

The Baltic and International Maritime Council (BIMCO)[3] explains that cybersecurity is "concerned with the protection of IT, Operational Technology (OT), information and data from unauthorised access, manipulation, and disruption". This is achieved using a cyber risk management approach, and the council recommends the development, implementation, and maintenance of a cyber risk management programme to manage cyber risk (BIMCO, 2020:3, 5). The International Maritime Organization (IMO)[4] describes cyber risk management as "the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken" (IMO, 2017b: 3).

Reflecting the concept that the individual cyber and technological vulnerabilities of each system are increased by those of other cyber systems to which they connect (see World Economic Forum [WEF], 2020: 67), BIMCO advises that cyber risk assessments be reviewed periodically to ensure all risks are adequately mitigated (BIMCO, 2020: 5). This is indicative of the dynamic nature of the cyber risk management process required to address a continuously evolving vessel, port, or stakeholder cyber threat landscape effectively, and that cybersecurity threats vary from country to country (Boyes, 2013: 61).

From the above it follows that vessels, ports, and stakeholders connected within the maritime cyber domain wishing to achieve an appropriate level of cybersecurity would require an active cyber risk management system that follows a recognised cyber risk management approach, and which adequately addresses all cybersecurity threats within the specific threat landscape of each organisation.

---

1 The attack surface of the maritime cyber domain comprises all potential points of access into a maritime cyber-enabled system that could be exploited by a cyber threat actor. Effective cybersecurity practice seeks to identify and to eliminate – or at least minimise the size of this attack surface – as far as is reasonably practicable.

2 The threat landscape is the collection of cyber threats observed, known about, or trending in an industry, sector, or amongst a group of cyber users.

3 BIMCO is the largest of various international shipping associations. It represents shipowners of the majority of the world shipping fleet, and its membership includes most industry stakeholders.

4 The IMO is a specialised agency of the United Nations, and responsible for regulating shipping.

To determine the readiness of the shipping industry to address cyber-related security threats definitively, it is necessary to ascertain whether all vessels, ports, and stakeholders have such a cyber risk management system in place. Given the sheer number of organisations globally that constitute the maritime cyber domain, this is clearly an unrealistic task.

Three possible alternatives remain to determine the readiness of the international shipping industry to address cyber-related threats, namely to –

- examine available information relating to maritime cyber incidents and vulnerabilities
- consider the results of maritime industry cybersecurity surveys; and
- consider and evaluate current cybersecurity practices used in the industry, identify their weaknesses and determine of their likely effectiveness in supporting cyber risk management.

Maritime cyber incidents and vulnerabilities

Three sources of information can be considered to determine the nature and extent of cyber incidents and vulnerabilities within the international shipping industry, i.e. public reporting of maritime cyber incidents, maritime losses stemming from cyber incidents, and demonstrations of maritime cyber vulnerability. Each was assessed for viability as a determinant of the readiness of the industry to address cyber-related security threats.

Firstly, an online search of maritime cyberattacks and incidents for the period 2011 to 2020 revealed eighteen such attacks and incidents (see Graph 1 below). While not a comprehensive record of all maritime cyberattacks occurring over that period, these could be considered indicative of the types of incidents and attacks occurring within the maritime cyber domain:

- one caused by outdated software (Wagstaff, 2014);
- six caused by crime (Bestpractice.biz, 2020; Coble, 2020; CyberKeel 2014: 7–8; Gronholt-Pedersen, 2017; *IT News*, 2020; *Seatrade Maritime News*, 2021; Ship & Bunker, 2014);
- two caused by cyberwarfare (CyberKeel, 2014:6; Warrick & Nakashima, 2020);
- four due to data and/or information theft (Beech, 2016; CyberKeel, 2014:7; *Financial Times*, 2016; *IT News*, 2020); and
- five caused by malicious behaviour (Coble, 2020; Offshore Energy, 2018; United States Coast Guard [USCG], 2019a; 2019b).

These attack and incident types appear to correlate with the 2019 threat assessment by the Danish Centre for Cyber Security (CFCS), which found that, within the context of the Danish maritime sector –

- cyber threats were posed to commercial businesses and not maritime operations;
- threats of cyber espionage and cybercrime were high;

- threats of disruption of maritime lines of communication were high during conflict; and
- the threat of cyber activism and cyber terrorism was low (SØfartsstyrelsen, 2019: 3).

However, this information is only of use to demonstrate that some vessels, ports and maritime industry stakeholders did not have effective cyber risk management systems in place, and did not see the need for it. The information therefore does not allow conclusions to be drawn on the readiness of the entire industry to address cyber-related security threats.

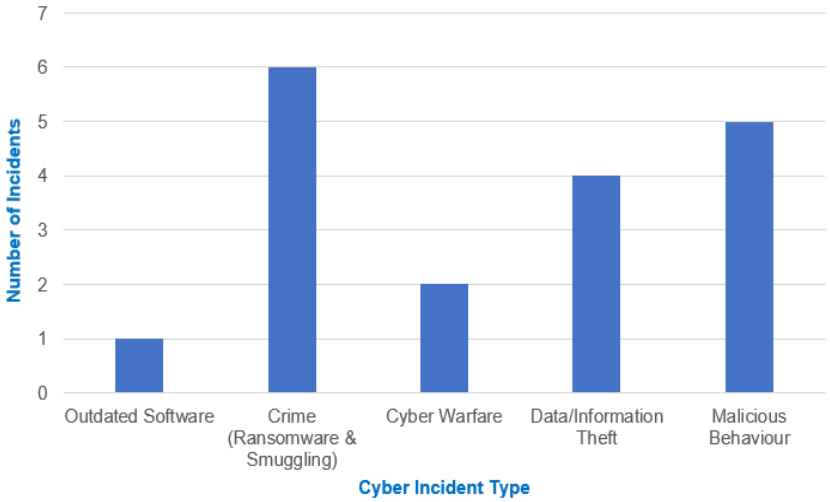


Figure 1: Maritime cyber incidents reviewed for period 2011–2020

Source: Author's own compilation

Secondly, considering open-source information on shipping losses, the Allianz *Safety and Shipping Review*[5] 2020 does not attribute any shipping losses or compromising of safety to cyber threats (Allianz, 2020a: 5–6, 14–15). However, it is of little use to draw meaningful conclusions about cybersecurity readiness of the industry, as the data may be –

- indicative of cyberattacks not causing such losses,
- under-reporting of cyberattacks within the maritime industry (Furness-Smith, 2019: 6–7), and
- caused by the practice of "silent-cyber" where cyber-related losses are treated as losses and not attributed to a cyber incident or attack (Gardner, 2019: 4).

[5] Allianz is one of the largest insurance and financial services groups in the world. Its core business is insurance and asset management. Their annual shipping review reports loss, risk, and safety trends in the shipping industry.

It therefore seems probable that insurers may not be able to attribute maritime losses to cyberattacks or provide meaningful data on such occurrences. As a result, such information also cannot help assess the readiness of the industry to address cyber-related security threats.

Thirdly, demonstrations of vessel cyber vulnerability have frequently been cited as proof of the vulnerability of the industry to cyber risk, such as:

- penetrative tests that have accessed the cyber systems of large container carriers through their corporate websites (CyberKeel, 2014: 9);
- manipulations of the automatic identification systems (AIS)[6] of vessels (Trend Micro, 2013);
- penetration and manipulation of information displayed on the electronic chart display and information systems (ECDIS)[7] of vessels (CyberKeel, 2014: 12);
- penetration and manipulation of the navigation systems, radar systems, and machinery control systems of vessels (Naval Dome, 2020b);
- disruption of global positioning system (GPS) signals of vessels (Grant, Williams, Ward & Basker, 2009: 173–182); and
- penetration of maritime satellite communications systems (Computerworld, 2014; CyberKeel, 2014: 12–13).

However, these only prove the vulnerability of systems used in vessels to cyberattack under controlled and permissive test conditions, provide insight into vessel, port, and stakeholder attack surfaces and possible attack vectors, but do not provide meaningful information on the readiness of the industry to address cyber-related security threats.

While the international maritime industry are subject to cyber vulnerabilities and has experienced cyber incidents, it is challenging to quantify the loss that has occurred from such incidents, the effectiveness of the cyber risk management practices of the industry, or the readiness of the industry to address cyber-related security threats.

Cybersecurity surveys

A range of maritime industry-focused cybersecurity and cyber readiness surveys have been conducted in recent years. The findings from these surveys may indicate the readiness of the shipping industry to address cyber-related security threats. While the results of these surveys are of interest, they only reflect the views of individuals participating in the survey and not the opinion of the entire industry. Furthermore, the cybersecurity knowledge of the individuals surveyed was not always determined beforehand, and respondents' answers might have been technically uninformed, subjective, and self-serving. Additionally, as all surveys were done before implementation and at the start of

[6] AIS is an automatic vessel position tracking system that can provide the user with the position, identity and other information relating to a vessel through the use of transceivers mounted on the vessel.

[7] ECDIS is a geographic information system used by vessels for navigation at sea.

IMO 2021,[8] IMO-mandated cybersecurity risk management systems were not necessarily introduced to and implemented in on-board vessels at the time of each survey.

Given that the shipping industry is a business, another factor to consider is how cyber incidents are rated globally as a business risk. The Allianz global business risk surveys between 2017 and 2021 found cyber threats scored consistently within the top three business risks globally for the period 2017 through to 2020 (Allianz, 2017: 2; 2018: 5, 10–11; 2019, 4, 12–15; 2020a: 4, 8, 9; 2021: 4, 12). This correlates with the findings of the 2019 and 2020 maritime cybersecurity surveys, which found respondents considered cyberattacks a serious threat to maritime organisations (Safety at Sea [SAS] & BIMCO, 2020: 10). While of interest, this gives no measure of the readiness of the industry to address cyber-related security threats, and it is not possible to determine whether the survey results reflect subjective or objective views of the participating respondents.

Maritime cyber risk surveys are therefore neither reliable nor useful indicators of the readiness of the industry to tackle cyber-related threats and should not be used to ascertain the effectiveness of the cyber risk management systems of the industry or the readiness of the entire industry to address cyber-related security threats.

Maritime industry cybersecurity practices and weaknesses

Maritime industry cybersecurity practices can be considered within the context of vessels, ports, and other stakeholders. Each of these practices will be described, and their apparent weaknesses in relation to achieving cybersecurity identified.

Ports and vessels

The IMO 2004 International Ship and Port Facility Security (ISPS) Code[9] addresses specific measures to enhance maritime security. It requires ship and port facility security assessments to be done to address, inter alia, risks associated with radio and telecommunications systems, including computer systems and networks (IMO, 2012: 315–316, 329–330). While cybersecurity is not specifically mentioned, the computer systems and networks described in the Code constitute the cyber-enabled systems of the ships and ports to which the Code applies. From this it is clear that both vessels and ports should already be identifying cyber threats within their vessel and port facility security assessments and be acting to address these. When viewed critically, one can deduce that two key weaknesses exist, namely:

- The ISPS Code does not adequately define and specifically link the terms ‘computer systems’ and ‘networks’ to the maritime cyber domain.
- The ISPS Code does not define ‘telecommunications systems’ in a manner that incorporates digital communications and the connectivity between cyber systems that such technology allows.

[8] IMO 2021 is an IMO resolution intended to address maritime cyber risk management on board vessels.

[9] The ISPS Code is an amendment to the IMO Safety of Life at Sea Convention, and establishes the minimum security arrangements required in ports and on board vessels.

Based on the above, both ship and port facility security plans may fail to identify and address the cybersecurity needs of these systems within their security plans, preventing them from addressing cyber-related security threats effectively.

Additionally, as ports are generally classed as critical infrastructure within the national security management frameworks of their host countries, national regulations and guidance may exist pertaining to their cybersecurity. Such examples include the European Union *Cyber risk management for ports* (European Union Agency for Cybersecurity [ENISA], 2020), and the American *Framework for Improving Critical Infrastructure Cybersecurity* V1.1 (National Institute of Standards and Technology [NIST], 2018). Despite this, two key weaknesses exist, namely:

- While some regulations require ports to manage their cyber risk, this is not the norm internationally and throughout the maritime industry.
- There are no means to determine whether such risks are adequately managed within a port, nor is there universal guidance on how ports should achieve cybersecurity.

Consequently, the level of cybersecurity and specific cyber threats faced by each port will not be known by vessels and stakeholders connecting to the cyber-enabled systems of such ports, thereby compromising their own cyber risk management systems.

Vessels

IMO 2021, consisting of the 2017 IMO resolution (MSC.428 (98) and associated guidelines (MSC-FAL.1/Circ.3), is intended to address maritime cyber risk management of on-board vessels (IMO, 2017a: 1; 2017b: 1). The resolution affirms approved safety management systems to address cyber risk management within the context of the International Safety Management (ISM) Code,[10] and encourages cyber risks be addressed appropriately in the safety management systems (SMSs)[11] of companies no later than the first annual verification of the Document of Compliance of such companies after 1 January 2021 (IMO, 2017a: 1). The guidelines require the adoption of a cyber risk management process that can detect a cyber threat and provide resilience to a company and continuity during and after a cyber event. It can also help the company recover after a cyber event. Recovery is however, dependent upon all relevant stakeholders "[taking] the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping" posed by malicious actions and unintended consequences of benign actions (IMO, 2017b: 1–4).

In principle, this should ensure all vessels would adequately manage their cyber risks once they pass the first annual verification audit of the safety management system (SMS) of the vessel after 1 January 2021. However, several factors are indicative of the possibility that individual vessels may be inadequately protected from cyber threats despite being deemed ISO 2021-compliant, namely:

[10] The ISM Code provides an international standard for the safe management and operation of vessels, and for the prevention of marine pollution.

[11] SMS refers to the vessel safety management system, which is intended to ensure the safe management and operation of a vessel, and the prevention of pollution by said vessel.

- While the IMO guidelines may lead to the development of a security culture that focuses on crew, vessel, and cargo, it lacks the focus needed on cyber- and information security. The findings of the CFCS in this regard may be applicable to the international maritime industry, which suggest an industry-wide need to enhance its existing security culture to include cyber- and information security (Dimakopoulou *et al*., 2019: 11229; SØfartsstyrelsen, 2019: 9).
- The annual SMS verification audit is a compliance audit only and does not test and verify the effectiveness of the cybersecurity management processes adopted within the SMS.
- The audit is performed by marine professionals and not by cybersecurity professionals meaning that failings or weaknesses of the cyber risk management system may be overlooked, and risk assessments and mitigations may be technically weak for their intended purposes.
- The cybersecurity of vessels is maintained on board by seafarers with little or no formal training or expertise in cybersecurity management and they could accidentally compromise security when interacting with the cyber systems of the ship.
- The IMO definition of cyber risk management outlined in their guidance is only an outline of what a successful cybersecurity system requires, namely the IMO 2021-compliant SMS of a vessel may comply fully with the Code but could still fail to address the specific cyber threats of each vessel adequately (Daum, 2019: 3).
- A vessel that is deemed compliant with the IMO guidelines has only satisfied the requirement of 'adequately addressed' cyber risk management within its individual SMS to ensure the safety of its own operations, people, cargo, and environment (GARD, 2020). Such compliance therefore only covers the SMS of a specific vessel, and does not ensure the cyber risk management of other vessels, ports, or stakeholders.

Consequently, the risk exists that the maritime industry may develop a false sense of its own security within the cyber domain once all vessels have achieved IMO 2021 compliance, being compliant with the requirements of the Code while not actually achieving the required outcome of effectively managing their cyber risks.

Classification societies[12] have started offering commercial cybersecurity services to marine clients. To this end, Lloyds Register, Det Norske Veritas – Germanischer Lloyd (DNV-GL), and American Bureau of Ships (ABS) are offering comprehensive cybersecurity services to marine industry clients (ABS Group, 2020; DNV-GL, 2020; Lloyds Register, 2020). Some have gone a step further and started offering a voluntary cyber secure class notation for those customers seeking it (GARD, 2020; SAFETY4SEA, 2018). Both initiatives have weaknesses, namely:

[12] Classification societies promulgate rules for the construction and classification of vessels, supervise their construction, and ensure their continued maintenance and operation in accordance with their rules. They also maintain a register listing vessels and their essential features falling under their rules.

- The concept of classification societies offering cybersecurity services is fundamentally flawed. Such organisations are supposed to be a neutral third party that assesses and reports on the condition of a vessel and its management systems, including the SMS. If they both manage and verify the effectiveness of the cybersecurity management system of a vessel, it would be a clear conflict of interest, and the system will have no external verification of its effectiveness.
- Cyber secure class notation will only serve the interests of a vessel classified accordingly and will only benefit the shipping industry if it becomes an industry-wide requirement for all vessels.

Based on the above, the value of using a classification society to manage and certify the cybersecurity management system of a vessel is questionable until its effectiveness has been verified by an external party. In addition, the benefit of receiving a cyber secure class notation is – at best – only benefitting the vessel holding it and not the industry as a whole.

Commercial companies offer bespoke solutions that might enhance the cybersecurity and support cyber risk management of a vessel. To this end, Naval Dome offers commercial fleets a multi-layered cyber defence solution (Naval Dome, 2020b), and CyberOwl (2020) offers a cybersecurity monitoring and analytics system. Both services, if properly integrated into the intended cyber-enabled systems and associated cybersecurity risk management systems of vessels, could enhance the effectiveness of cyber risk management. Next, original equipment manufacturers (OEM) of marine digital and cyber-enabled and cyber-connected systems are designing cybersecurity measures into their equipment. Examples of this include Inmarsat's Fleet Secure Endpoint (FSE) satellite communications product, which secures networks and devices (Inmarsat, 2020: 22–23), and Wärtsilä incorporating cybersecurity within the design of its proprietary Navi-Planner voyage planning and optimisation system (International Tug & OSV, 2019: 66). However, while this is a pragmatic step toward managing cyber-related threats, the existence of these cybersecurity solutions does not ensure industry-wide readiness to manage threats, because –

- They only focus on cyber-enabled systems fitted to vessels and some cyber-enabled systems within ports, which are unlikely to be used by other stakeholders.
- There is no reliable indication of the portion of the global shipping fleet that have these systems fitted.

These initiatives are therefore likely only to strengthen OEM cyber-enabled systems and support the cyber risk management of those individual vessels and not the entire maritime industry.

Stakeholders

For stakeholders, cyber risk management processes are ordinarily integrated within their business risk management processes (SØfartsstyrelsen, 2019: 3–4) by including management systems that conform to recognised standards, such as the ISO 27001 Information Security Management or the ISO 27002 Security Controls standards. This is largely driven by the business costs associated with non-compliance with national

information security regulations and business interruptions experienced during cyberattacks or incidents, and by organisations adopting a pragmatic approach to risk management (Spin Technology, 2020).

Potential weaknesses exist, namely the management systems and processes associated with these standards, which may –

- be poorly designed, implemented, and managed resulting in their loss of effectiveness;
- exclude the vessel, port, and cyber system connectivity and cyber environment of the stakeholder; and
- be fully compliant with the respective standards but fail to manage the cyber-related threats facing the stakeholder's organisation adequately, as certification is achieved through compliance with the standard and not with the outcomes of the system.

A stakeholder may therefore still be failing to manage the cyber-related risks within the maritime cyber domain despite having their information security management and security control systems certified in terms of the respective ISO standards.

Additional factors

The World Economic Forum (WEF) 2020 *Global Risks Report 2020* identifies several factors relating to international cyber risk that are relevant to the maritime cyber domain, namely:

- The number of people becoming active online is increasing daily (WEF, 2020: 62), and with it, the number of potential cyber threat-actors.
- As organisations increasingly connect and operate within a global digital ecosystem, so their individual level of cyber risk increases when their own vulnerabilities are increased by those of the cyber systems to which they connect (WEF, 2020: 67).
- "Security-by-design" principles are secondary to manufacturers' need to introduce products to the market (WEF, 2020: 63) with many such products being IT and OT systems and "bring your own device" systems that will enter and connect to the maritime cyber domain.
- IoT technology renders all connected systems vulnerable to a large, single cyberattack surface (WEF, 2020: 61–63, 67), so attack vectors may become increasingly difficult to discern when assessing cyber vulnerability.

Considering that maritime industry is integrated within the world economy, these factors would imply that cyber vulnerabilities, threat landscapes, and attack vectors within the maritime industry will continue to evolve and expand rather than diminish.

Additionally, the regulations and policies pertaining to both cyber and information security are globally fragmented (WEF, 2020: 67), and security methodologies differ. This results in a complex regulatory and compliance landscape in which shipping industry stakeholders must perform cyber risk management, possibly resulting in the development of overly complex cyber and information security management systems, policies, and processes that ultimately hamper cybersecurity efforts within these organisations and industry.

The conclusions reached are that cyber threats within the maritime cyber domain are unlikely to diminish but will rather increase in the future. Moreover, individual vessels, ports, and stakeholders have both individual and collective vulnerabilities to defend within an evolving threat landscape while contending with a complex regulatory and compliance landscape. This results in maritime cyber risk management being a necessary and challenging undertaking.

The African shipping industry and cyber risk management

The African shipping sector is an element of the international shipping industry and facilitates the movement of goods during both international and intra-Africa trading.

In terms of international trade, UNCTAD reports[13] that in 2020, of the total international maritime trade done by developing economies, African maritime trade accounted for 11.6% of goods loaded and 6.9% of goods unloaded (UNCTAD, 2021: 3–4). The types of goods passing through African ports are crude oil, other tanker trade (refined petroleum products, gas, and chemicals), and dry cargo (UNCTAD, 2021: 4). Export quantities in all cargo types exceed import quantities (UNCTAD, 2021: 4). While international air freight and export pipelines between Africa and Europe account for limited trade volume, the majority of products are transported by the African shipping sector. Indeed, UNCTAD comments that, for Africa, "maritime transport remains the main gateway to the global marketplace" and that the international trade on the continent – of both coastal and landlocked states – is heavily reliant on shipping and ports (UNCTAD, 2019: 48, 63, 70). As a result, maritime trade is the most significant enabler of African trade within the international economy, and any disruption of this maritime trade is likely to impair economic performance in Africa.

In terms of intra-African trade, the existing African shipping sector, which handled almost a quarter of inter-Africa freight transport in 2019, is expected to more than double the volume of cargo it transports as the 2019 African Continental Free Trade Area (AfCFTA) agreement takes effect. In terms of the maritime element, if this agreement is enforced, the maritime component of the transportation system on the continent could require substantial investment in African ports and vessels to cope with the expected increased volume of trade between African countries (UNCTAD, 2021: 20). Any disruption of maritime trade between African countries in the future could therefore undermine implementation of the AfCFTA agreement and deriving any economic benefit from it.

Like the international shipping industry, the African shipping sector requires access to and use of the maritime cyber domain to perform its business. The shipping industry in Africa is connected to the same elements of cyberspace, conducts the same business, faces the same potential for business disruption from cyber threats, and follows the same potentially ineffective industry cybersecurity practices. The ability of the African shipping industry to sustain maritime trade within Africa and between Africa and the world economies is

[13] Source: UNCTAD secretariat using data sourced from reporting countries, relevant government and port websites, and other undisclosed sources. For 2020, total maritime trade figures were estimated from preliminary data or from the last year of available data.

therefore also at risk of experiencing business disruption or loss from cyber threats, and it is probably relying on potentially ineffective maritime cybersecurity practices to manage this risk (Cronje & Martin, 2021).

A pragmatic approach for safeguarding African maritime trade from cyber threats is required. Such an approach would – as a minimum – entail:

- the enforcement of all existing maritime industry cybersecurity practices by African port and flag state authorities,[14] with such authorities being assisted by trained cybersecurity personnel; and
- categorising ports as critical infrastructure under the respective national legislation, and requiring these ports and associated stakeholders to manage their cyber-related risks effectively by instituting a fit-for-purpose cybersecurity management system.

As always, the challenge would be to develop sensible and pragmatic legislation, supported by guidelines and some form of verification and assurance that each port and associated stakeholder has implemented and is maintaining an effective cyber risk management system.

Conclusion

This article has described the international shipping industry and its associated cyber domain, explained what cybersecurity is, described the nature of maritime cyber incidents and vulnerabilities, considered possible indicators of the readiness of the industry to manage its cyber-related threats, and considered the effectiveness of the existing cybersecurity practices of the industry. Moreover the article considered these elements in the context of the African shipping sector, and identified the potential high-order consequences of cyber threats to this sector, and proposed pragmatic mitigations to manage cyber risk of the sector.

The conclusions drawn were that, while cyber risk management is needed, it is challenging to achieve and, despite efforts by the maritime industry to increase its cybersecurity, multiple weaknesses exist in relation to current cybersecurity practices. Each weakness has the potential to compromise the security of individual vessels, ports, and stakeholders, thereby undermining efforts by the industry to achieve security within the maritime cyber domain. Despite its efforts, the international shipping industry is therefore not yet ready to tackle cyber-related security threats to its activities.

Considering this in relation to the African shipping sector, and taking into account the importance of the maritime industry to intra-Africa and international trade, the weaknesses of current maritime cybersecurity practices in the shipping industry place the sector at risk of disruption by cyber-related threats.

---

[14] Port state authority refers to the authority to inspect ships in national ports to verify compliance with international regulations, manning and other operational requirements. Flag state authority refers to the authority and responsibility to enforce regulations over vessels listed on its registry.

A clear and pragmatic approach for the African shipping sector to manage its cyber risk effectively was described. This approach requires the African shipping sector to embrace and enforce existing maritime industry cybersecurity practices using all available port and flag state authority; addressing the cybersecurity of African ports by declaring them critical infrastructure; and enacting and enforcing legislation requiring them and their associated stakeholders to institute fit-for-purpose cybersecurity management systems within their organisations.

References

ABS Group. 2020. *Maritime cyber security*. Available at: <https://www.abs-group.com/What-We-Do/Safety-Risk-and-Compliance/Cybersecurity/Maritime-Cybersecurity/> [Accessed 30 September 2023].

Alcaide, J. & Llave, R. 2020. Critical infrastructures cybersecurity and the maritime sector. *Transportation Research Procedia*, 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058

Allianz. 2017. *Allianz Risk Barometer: Top business risks for 2017*. Available at: <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2017.html> [Accessed 30 September 2023].

Allianz. 2018. *Allianz Risk Barometer: Top business risks for 2018*. Available at: <https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2018.pdf> [Accessed 30 September 2023].

Allianz. 2019. *Allianz Risk Barometer: Top business risks for 2019*. Available at: <https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html> [Accessed 30 September 2023].

Allianz. 2020a. *Allianz Risk Barometer: Identifying the major business risks for 2020*. Available at: <https://www.allianz.com/en/press/news/studies/200114_Allianz-risk-barometer-2020.html> [Accessed 30 September 2023].

Allianz. 2020b. *Safety and shipping review 2020.* Available at: <https://www.agcs.allianz.com/news-and-insights/reports/shipping-safety.html> [Accessed 30 September 2023].

Allianz. 2021. *Allianz Risk Barometer: Top business risks for 2023*. Available at: <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html> [Accessed 30 September 2023].

Beech, E. 2016. Personal data for more than 130,000 sailors hacked: US Navy. *Reuters*, 24 November. Available at: <https://www.reuters.com/article/us-usa-cyber-navy/personal-data-for-more-than-130000-sailors-hacked-u-s-navy-idUSKBN13J001> [Accessed 30 September 2023].

Bestpractice.biz. 2020. *Four largest shipping companies all hit by cyber attacks*. Available at: <https://bestpractice.biz/four-largest-shipping-companies-all-hit-by-cyber-attacks/> [Accessed 30 September 2023].

BIMCO (Baltic and International Maritime Council). 2020. *The guidelines on cyber security onboard ships, version 4.* Available at: <https://www.bimco.org/news/priority-news/20201223-new-cyber-security-guidelines> [Accessed 30 September 2023].

Boyes, H. 2014. Maritime cyber security: Securing the digital seaways. *Engineering & Technology Reference*, 56–63. https://doi.org/10.1049/etr.2014.0009

Caschili, S. & Medda, F. 2012. A review of the maritime container shipping industry as a complex adaptive system. *Interdisciplinary Description of Complex Systems*, 10(1), 1–15. https://doi.org/10.7906/indecs.10.1.1

Cimpanu, C. 2019. US Coast Guard discloses Ryuk ransomware infection at maritime facility. *ZDNet*, 29 December. Available at: <https://www.zdnet.com/article/us-coast-guard-discloses-ryuk-ransomware-infection-at-maritime-facility/> [Accessed 30 September 2023].

Coble, S. 2020. MSC Data Center closes following suspected cyber-attack. *Infosecurity Magazine.* Available at: <https://www.infosecurity-magazine.com/news/msc-suffers-suspected-cyberattack/> [Accessed 30 September 2023].

Computerworld. 2014. *Satellite communication systems are rife with security flaws, vulnerable to hackers*. Available at: <https://www.computerworld.com/article/2488396/satellite-communication-systems-are-rife-with-security-flaws--vulnerable-to-.html> [Accessed 30 September 2023].

CyberKeel. 2014. *Maritime cyber risks*. Available at: <https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf> [Membership only].

CyberOwl. 2020. *Solutions: Medulla*. Available at: <https://www.cyberowl.io/solutions/> [Accessed 30 September 2023].

Daum, O. 2019. Cyber security in the maritime sector. *Journal of Maritime Law & Commerce*, 50(1), 1–19.

Dimakopoulou, A., Nikitakos, N., Dagkinis, I., Lilas, T., Papachrisos, D. & Papoutsidakis, M. 2019. The new cyber security framework in shipping industry. *Journal of Multidisciplinary Engineering Science and Technology*, 6(12), 11227–11233.

DNV GL. 2020. *Cyber security services.* Available at: <https://www.dnvgl.com/services/cyber-security-services-127179> [Accessed 30 September 2023].

Cronje, J. & Martin, G. 2021. Experts warn of increasing cyber security threats to the African maritime industry. *defenceWeb*, 22 October. Available at: <https://bit.ly/47L13L0d> [Accessed 30 September 2023].

ENISA (European Union Agency for Cybersecurity). 2020. *Cyber risk management for ports.* Available at: <https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports> [Accessed 30 September 2023].

Financial Times. 2016. French submarine maker DCNS hit by data leak, 24 August. Available at: <https://www.ft.com/content/182399f2-69be-11e6-a0b1-d87a9fea034f> [Paid access only].

Fitton, O., Prince, D., Germond, B. & Lacy, M. 2015. *The future of maritime cyber security.* Lancaster University. Available at: <https://eprints.lancs.ac.uk/id/eprint/72696/1/Cyber_Operations_in_the_Maritime_Environment_v2.0.pdf> [Accessed 30 September 2023].

Furness-Smith, G. 2019. Maritime industry must open up about cyber crime. *Phish & Ships*, 34, September. Available at: <https://storage.ning.com/topology/rest/1.0/file/get/3529119427?profile=original> [Accessed 30 September 2023].

GARD. 2020. *International Safety Management Code (ISM Code)*. Available at: <http://www.gard.no/web/updates/content/51838/international-safety-management-code-(ism-code)> [Accessed 30 September 2023].

Gardner, S. 2019. 'Silent' cyber: What is it? And why is it important to the maritime industry? *Phish & Ships*, 34, September. Available at: <https://storage.ning.com/topology/rest/1.0/file/get/3529119427?profile=original> [Accessed 30 September 2023].

Grant, A., Williams, A., Ward, N. & Basker, S. 2009. GPS jamming and the impact on maritime navigation. *The Journal of Navigation*, 62(2), 173–182. https://doi.org/10.1017/S0373463308005213

Gronholt-Pedersen, J. 2017. Maersk says global IT breakdown caused by cyber-attack. *Reuters*, 27 June. Available at: <https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO> [Accessed 30 September 2023].

IMO (International Maritime Organization). 2012. *Guide to maritime security and the ISPS Code.* 2012 edition. Exeter: Polestar Wheatons.

IMO (International Maritime Organization). 2017a. *Guidelines on maritime cyber risk management.* MSC-FAL. 1/Circ. 3. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 30 September 2023].

IMO (International Maritime Organization). 2017b. *Maritime cyber risk management in safety management systems.* MSC.428(98). Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 30 September 2023].

Inmarsat. 2020. *Cyber security requirements for IMO 2021*. Available at: <Inmarsat_Cyber_Security_IMO2021_Requirements.pdf> [Accessed 30 September 2023].

International Tug & OSV. *Voyage planning takes hi-tech turn.* No place: The ABR. 24/4. (July/August 2019).

IT News. 2020. Shipbuilder Austal was hacked with stolen creds sold on dark web, 8 April. Available at: <https://www.itnews.com.au/news/shipbuilder-austal-was-hacked-with-stolen-creds-sold-on-dark-web-546165> [Accessed 30 September 2023].

Lambrou, M., Watanabe, D. & Lida, J. 2019. Shipping digitalization management: Conceptualization, typology and antecedents. *Journal of Shipping and Trade*, 11, 1–17. https://doi.org/10.1186/s41072-019-0052-7

Lind, M., Gardeitchik, J., Carson-Jackson, J., Haraldson, S. & Zuesongdham, P. 2020. Get smart. *Seaways: The International Journal of the Nautical Institute*, July, 12–13.

Loyd's Register. 2020. *Cyber security services: Reducing risk from an evolving threat*. Available at: <https://www.lr.org/en-za/cyber-security/> [Accessed 30 September 2023].

Naval Dome. 2020a. *Solutions: Leading maritime cybersecurity and risk management*. Available at: <https://navaldome.com/solutions.html> [Accessed 30 September 2023].

Naval Dome. 2020b. *The threat: Naval Dome's cyber attack demonstration*. Available at: <https://navaldome.com/threat.html> [Accessed 30 September 2023].

NCSC (National Cyber Security Centre). 2019. *The cyber security body of knowledge, version 1.0*. Available at: <https://www.ncsc.gov.uk/section/education-skills/cybok> [Accessed 30 September 2023].

NIST (National Institute of Standards and Technology). 2018. *Framework for improving critical infrastructure cybersecurity.* Available at: <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf> [Accessed 30 September 2023].

Offshore Energy. 2018. *COSCO Shipping Lines falls victim to cyber attack*. Available at: <https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/> [Accessed 30 September 2023].

SAFETY4SEA. 2018. *DNV GL issues cyber security class notations*. Available at: <https://safety4sea.com/dnv-gl-issues-cyber-security-class-notations/> [Accessed 30 September 2023].

SAFETY4SEA. 2019. *Under-reporting cyber-attacks is a threat to the industry.* Available at: <https://safety4sea.com/under-reporting-cyber-attacks-is-a-threat-to-the-industry/> [Accessed 30 September 2023].

SAS (Safety at Sea) & BIMCO. 2020. *Safety at Sea and BIMCO Cyber Security White Paper 2020*. Available at: <https://bit.ly/3t7T7Eu> [Accessed 30 September 2023].

Seatrade Maritime News. 2021. Antwerp incident highlights maritime IT security risk, 21 October. Available at: <https://www.seatrade-maritime.com/europe/antwerp-incident-highlights-maritime-it-security-risk> [Accessed 30 September 2023].

Sheffi, Y. & Gray, E. 2019. Marine supply chain challenges. *Port Technology International Journal*, 85:3–4.

Ship & Bunker. 2014. *Recent cyber attacks highlight bunker industry vulnerability*. Available at: <https://shipandbunker.com/news/am/171559-recent-cyber-attacks-highlight-bunker-industry-vulnerability> [Accessed 30 September 2023].

SØfartsstyrelsen. 2019. *Cyber and Information Security Strategy for the Maritime Sector 2019–2022.* Available at: <https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information%20Security%20Strategy%20for%20the%20Maritime%20Sector.pdf> [Accessed 30 September 2023].

Spin Technology. 2020. *The financial impact of non-compliance on business*. Available: <https://spinbackup.com/blog/the-impact-of-non-compliance-on-businesses/> [30 September 2023].

Trend Micro. 2013. *Vulnerabilities in global vessel tracking systems.* Available at: <https://www.trendmicro.com/en_us/research/13/j/vulnerabilities-discovered-in-global-vessel-tracking-systems.html> [Accessed 30 September 2023].

UNCTAD (United Nations Conference on Trade and Development). 2019. *Review of maritime transport 2019.* Available at: <https://unctad.org/system/files/official-document/rmt2019_en.pdf> [Accessed 30 September 2023].

UNCTAD (United Nations Conference on Trade and Development). 2021. *UNCTAD's review of maritime transport 2021*. Available at: <https://unctad.org/system/files/official-document/rmt2021_en_0.pdf> [Accessed 30 September 2023].

USCG (United States Coast Guard). 2019a. *Cyber adversaries targeting commercial vessels*. Available at: <https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_004_19.pdf> [Accessed 30 September 2023].

USCG (United States Coast Guard). 2019b. *Cyber incident exposes potential vulnerabilities onboard commercial vessels*. Available at: <https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf> [Accessed 30 September 2023].

Wagstaff, J. 2014. All at sea: Global shipping fleet exposed to hacking threat. *Reuters*, 23 April. Available at: <https://www.reuters.com/article/us-cybersecurity-shipping/all-at-sea-global-shipping-fleet-exposed-to-hacking-threat-idINBREA3M20820140423> [Accessed 30 September 2023].

Warrick, J. & Nakashima, E. 2020. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*, 18 May. Available at: <https://bit.ly/3NfuXig> [Paid access only].

WEF (World Economic Forum). 2020. *The Global Risks Report 2020*. Available at: <http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf> [Accessed 30 September 2023].

You-Sheng, W., Wei-Cheng, C. & Guo-Jun, Z. 2001. *Practical design of ships and other floating structures.* Oxford: Elsevier Science.

Zagan, R., Raicu, G., Hanzu-Pazara, R. & Enache, S. Realities in maritime domain regarding cyber security concept. *Advanced Engineering Forum*, 27 (April 2018), 221–228.

Scientia Militaria
2023, VOL. 51, NO. 3, 133-160
DOI: 10.5787/51-3-1429

IOT and IIOT Security for the South African Maritime and Freight Transport Sectors

Barend Pretorius
University of KwaZulu-Natal

Brett van Niekerk
Durban University of Technology

Abstract

The advent of the Fourth Industrial Revolution (4IR) has seen a rapid increase in connected smart devices known as the Internet of Things (IoT). While this 'revolution' is most noticeable in commercial devices, there has also been an evolution in industrial devices, known as the Industrial Internet of Things. As Africa – and in particular South Africa – is racing to compete in the 4IR, various sectors, including the transport sector, are introducing innovative projects. However, the Internet of Things and the Industrial Internet of Things present cybersecurity risks. Cybersecurity itself is also considered a key component of the 4IR; yet, organisations often neglect to consider the security implications of the Internet of Things.

The current research aimed to evaluate and prioritise cyber threats, vulnerabilities, and risk related to the Internet of Things and the Industrial Internet of Things in the South African physical transport sector. This article focuses on the responses to a questionnaire to obtain quantitative data from those with experience in the related fields. The threats and vulnerabilities of concern are illustrated, and the risks are evaluated based on the perceived impact of such risks and the likelihood of the Internet of Things and the Industrial Internet of Things being compromised. While no clear leaders of risk were found, the top three risks based on the perceived severity and likelihood are unavailability of Internet of Things and Industrial Internet of Things devices and/or networks, damage to reputation, and cyberespionage.

Keywords: critical infrastructure protection, cybersecurity, Industrial Internet of Things (IIoT), Internet of Things (IoT), transport sector security.

Introduction

The Fourth Industrial Revolution (4IR) has seen advances in technologies contributing towards an information-based society; in particular, there has been an increase in the number of connected devices, known as the Internet of Things (IoT) for consumer items and the Industrial Internet of Things (IIoT) within the industrial setting. The IoT has shown potential benefits in agriculture, city management, transportation, business and healthcare. Research on IoT deployments indicates that the IoT shows promise in

addressing or advancing the United Nations' Sustainable Development Goals (Marchant, 2021). However, the IoT also poses risks, particularly regarding cybersecurity. The rapid growth and hyper-connectivity due to the IoT increase the attack surface compared to 'traditional' cybersecurity (Chen, 2016), and the potency of the attacks is increasing (Dooley, 2017). In addition, Townsend (2019) reports that attacks against the IIoT had already begun in 2019, and that organisations were not adequately prepared for them.

The transport sector also is benefitting from the IoT and IIoT, but is also experiencing security challenges. The sector has seen increasing attention from malicious actors in cyberspace (Van Niekerk, 2017), and introducing the IoT and the IIoT may bring with it vulnerabilities, and further increase the attack surface against smart transportation systems (Awan, Memon, Shah & Pathan, 2020; Pretorius & Van Niekerk, 2020). Akpan, Bendiab, Shiaeles and Karamperidis (2022) highlight that limited research has been done on cybersecurity in the maritime sector despite the importance of the sector. In a South African (SA) context, limited studies have been conducted on IoT and IIoT security in the transport sector.

The aim of this study was to investigate the perceptions of IoT and IIoT security in the SA transport sector. In particular, the study sought to evaluate the perceived threats, vulnerabilities, and associated risks of introducing IoT and IIoT to the SA transport sector in order to prioritise the most significant risks. Data were gathered through a close-ended questionnaire, soliciting responses from experts with experience in the sector identified using convenience and snowball sampling.

The article continues with the literature review in the next section, providing an overview of the IoT and the IIoT in general and in the transport sector, and discussing cybersecurity incidents in the sector and those related to the IoT and the IIoT. The methodology section describes the research process in more detail, followed by a presentation of the results. The results are discussed, and the article is then concluded.

Literature review

This section provides an overview of the IoT and the IIoT, followed by a focus of the IoT and the IIoT within the maritime and transport sectors. Specific cybersecurity incidents related to the IoT and the IIoT, in the transport sector, are discussed.

The IoT and IIoT

The IoT can be defined as a "network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment" (Gartner, 2022: n.p.). The term first emerged in 1999, and in the early 2000s the first 'smart' devices were being produced (Marchant, 2021). The IIoT can be considered the intersection between the IoT and traditional operational technology or industrial control systems (Henning, 2017; Pretorius & Van Niekerk, 2020; Sullivan, 2020). In the broader sense, the IoT is revolutionary, as devices not traditionally networked or connected are now becoming so (for example television sets and fridges), whereas the IIoT is evolutionary,

as many industrial systems had already been connected and provided with remote access (Bowne, 2015). Chan (2017) elaborates on some of the differences between the IoT and the IIoT, for instance –

- the IIoT needs to have more interoperability and scalability than IoT as they operate with existing legacy systems and large-scale industrial networks;
- the IIoT requires greater precision than IoT and low latency to cater for real-time monitoring of industrial processes; and
- the IIoT requires greater resilience, reliability and serviceability to be able to operate in harsh environments and minimise downtime than IoT.

While the IoT and IIoT provide many benefits, such as improved productivity and data availability, they also introduce security concerns into the corporate and industrial environments (Marchant, 2021; Sullivan, 2020). Chan (2017) mentions that the IIoT requires more security than commercial IoT due to the placement of IIoT in critical industrial processes. Many connected devices may however contain vulnerabilities, some of which are not disclosed by the manufacturers, something that Solomon (2022) calls "insecure-by-design". Johnson (2017: n.p.) as well as Ku and Weiss (2017) indicate that security IIoT is particularly challenging. Some security concerns in terms of the IoT and the IIoT are authentication, insecure protocols for data transfer, insecure data storage, insecure gateways and interfaces, and supply chain risks relating to vulnerabilities in the IoT and IIoT or in individual components of these (Ku & Weiss, 2017; Sullivan, 2020).

Cybersecurity incidents related to the IoT and the IIoT

A number of cybersecurity incidents have occurred due to insecure IoT and IIoT devices. This section discusses selected incidents to illustrate the range of threats and vulnerabilities relevant to IoT and IIoT devices. The most prominent cybersecurity incident was the Mirai botnet, which was used to conduct a series of DDoS (distributed denial-of-service) attacks word wide in over 160 countries worldwide in 2016 (Forrest, 2016; Kan, 2016; Woolf, 2016). The 100 000 infected IoT devices that targeted the service provider Dyn, were reportedly comprising mostly digital video recorders, CCTV cameras, and home routers from over 160 countries. This was followed by a DDoS attack on a Liberian telecommunication provider, with traffic reportedly reaching 500GB/s. At the time, the series of DDoS attacks were the largest ever recorded, and variants of the Mirai were reported to have spread to 500 000 devices that were compromised due to weak default passwords (Forrest, 2016; Kan, 2016; Woolf, 2016).

In another incident, an undisclosed university suffered a DDoS attack due to IoT and IIoT devices in the network being compromised. The attackers gained control of the devices by using the manufacturer's default passwords, which were then changed and brute force attacks were conducted to compromise other devices. Approximately 5 000 devices, such as smart lightbulbs and connected vending machines, were compromised and then used to conduct a DDoS against the domain name server of the university (Cimpanu, 2017). In 2017, a connected temperature sensor in a fish tank at a casino was used as an entry point into the network and stole 10GB of data (Schiffer, 2017).

Common commercial IoT devices found in a household and in businesses have been compromised and/or concerns were raised about their security. Digital road signage and billboards have been hacked to display messages with warnings about weak default and hardcoded passwords that could be used to compromise such devices (Kovacs, 2014). A fridge has been seen to have sent spam e-mails, and the Federal Bureau of Investigation (FBI) released a warning about insecure baby monitors and toys as well as the risk of smart TVs or entertainment systems with a camera and microphone, which have raised privacy concerns (Chen, 2016; Lomas, 2015; Schiffer, 2017; Starr, 2014; Vaughan-Nichols, 2019). In addition, there have been cases where video conferencing systems have been compromised and large quantities of information stolen from the organisations. This further illustrates the potential use of IoT devices for espionage – if the audio and video could be accessed, the attackers would be able to steal sensitive corporate information (Darktrace, 2016).

IoT or IIoT devices themselves may not necessarily be the entry point. Vendors and third-party services may be compromised in order to gain access to the organisation. A major example of this is the United States (US) market chain Target, where cybercriminals managed to steal 40 million credit-card records in 2013 after entering Target via the Heating, Ventilation and Air Conditioning (HVAC) contractor. This was one of the largest data breaches at the time, and is estimated to have cost Target over US$200 million (Zimmerman, 2017).

The above incidents illustrate a number of vulnerabilities, risks and threats related to IoT and IIoT. These can be seen to include DDoS attacks affecting networks, stolen data, privacy and espionage. Vulnerabilities may include insecure protocols, device authentication, with third parties as well as devices contributing to breaches.

IoT and IIoT in the maritime and related sectors

There are a number of benefits to IoT in the maritime sector, including automation, real-time monitoring, analytics for optimisation, improved communication and connectivity for vessels at sea, which have the potential for cost savings (Burkhalter, 2022; Kapkaeva, Gurzhiy, Maydanova & Levina, 2021; KVH Watch, 2021). The concept 'smart ports' implies enhanced productivity, automation, and intelligent infrastructure based on technologies, such as IoT and artificial intelligence (Min, 2022; Molavi, Lim & Race, 2019). Molavi et al. (2019) also indicate that a measure of a 'smart port' is an interface with intelligent railways. Ayyagari (2018) describes a number of benefits of IoT in railways, which are similar to those in the maritime sector, namely improved monitoring translating into better safety and reliability, predictive maintenance, and analytics to aid optimisation.

Cybersecurity for the transport sector is crucial due to its critical nature. The importance of the sector is highlighted in the *Australian Security of Critical Infrastructure Act (No. 29 of 2018)*, by the US Cybersecurity and Infrastructure Security Agency (CISA) (2020), and also by Theoharidou, Kandias and Gritzalis (2011). Akpan et al. (2022) raise a number of challenges for cybersecurity in the maritime domain, particularly in terms of automated ships due to the large number of systems for navigation, radar, communications, propulsion and the associated industrial control and IT networks. Many of these automated ships with

demonstrated vulnerabilities make cybersecurity of a connected vessel difficult. Similarly, automated ports could also face these challenges, as well as railways and pipelines, which often have interfaces with the maritime sector. Cybersecurity incidents demonstrating the possibly attack methods and consequences are illustrated in the next section.

Cybersecurity incidents in the maritime and related sectors

The number of cybersecurity incidents affecting the transport sector has been increasing from 2008 to 2016, and the majority of the incidents during that period had affected the maritime sector (see Van Niekerk, 2017). This section discusses select incidents to illustrate the types of threats that have been experienced within the sector since 2001.

Port operations have been affected by cybersecurity incidents, such as a DDoS attack disrupting the Port of Houston in 2001 (McCue, 2003). Ransomware affected port operations at Transnet in South Africa in 2021 (Gallagher & Burkhardt, 2021), and the NotPetya affected A.P. Møller-Maersk's port operations globally (Cimpanu, 2018). A major port terminal in Iran was disrupted by a cyberattack in 2020, attributed to a nation-state (Warrick & Nakashima, 2020). Ports have also been disrupted due to signal jamming of global positioning systems (GPSs), such as in an undisclosed European port in 2015 and the Port of Shanghai in 2019; the latter also experienced spoofing of both GPS and Automatic Identification System (AIS) signals (Goward, 2019; Knox, 2015). In addition to operational disruptions, criminals have used cyberattacks to track shipping containers with smuggled goods, as in the Port of Antwerp in 2013 (Dunn, 2013).

In addition to ports, sea-going vessels have also been affected by cyberattacks. A series of oil rigs were affected by cybersecurity incidents, including malware disrupting the navigation systems resulting in the rig drifting off position, and hackers tilting an oil rig in 2014 resulting in a disruption of operations (CyberKeel, 2014; Knox, 2015; Swanbeck, 2015; Wagstaff, 2014). In addition, in 2009, a disgruntled insider at Pacific Energy Resources platforms offshore of Huntington Beach disabled the safety systems of oil rigs (Kravets, 2009).

Delays in passenger rail services have been experienced due to malware (CSX Corporation in 2013), ransomware (San Francisco in 2016), DDoS (Denmark in 2018), and a network intrusion that affected the signals (United States in 2011), indicating a range of threat types that could cause disruptions (Fletcher & Bye, 2022; Miller & Rowe, 2012; Ragan, 2012). One of the earliest attacks against a rail system occurred in Poland in 2008, when a team built a device in order to switch the points on the tram system remotely, resulting in a derailment (Ismail, Sitnikova & Slay, 2015).

Pipelines have also experienced disruptions on the back of cyberattacks, most notably the ransomware infection at Colonial Pipelines in 2021, which resulted in significant social ramifications (Kerner, 2022). In 1999, a disgruntled insider at Gazprom aided attackers with a backdoor, which affected the flow control systems (Miller & Rowe, 2012). Wiper malware rendered corporate computers ineffective at Saudi Aramco in 2012, but did not affect industrial systems (Bronk & Tikk-Ringas, 2013). Between 2011 and 2012, a cyberespionage operation stole operational data from US pipeline organisations (Clayton, 2013).

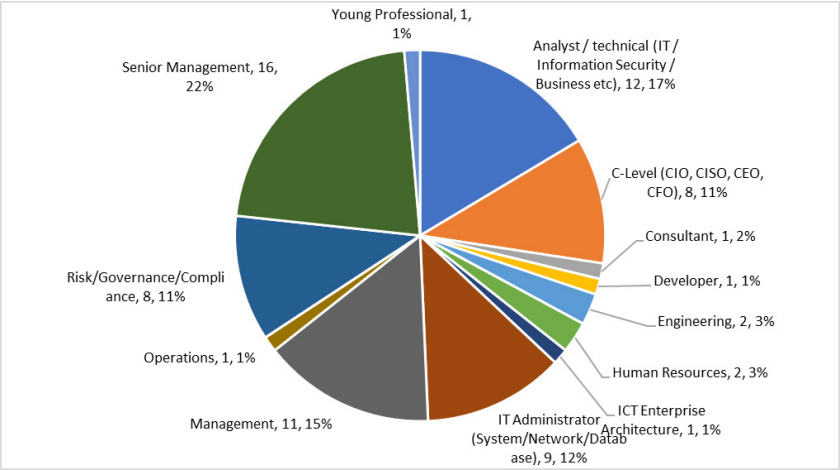
The above incidents illustrate that the transport sector has been affected by numerous threat types, including DDoS, malware, ransomware, signal jamming, as well as other system intrusions. Threat actors include insider threats, state actors, cybercriminals, and individual perpetrators.

Methodology

The current study sought to evaluate the perceptions of IoT and IIoT security within the SA transport sector, particularly to determine whether there are any specific areas of concern. The focus of this article is on the qualitative responses received for the technical factors, namely the threats, vulnerabilities and associated risks of compromised IoT and IIoT. Due to limited information available on individuals who have experience in terms of IoT and IIoT and security in the sector, non-probabilistic sampling was appropriate, and convenience sampling was used and enhanced with snowball sampling. An online questionnaire was distributed to organisations in the transport sector and through professional bodies to solicit responses. This article presents the results of an exploratory analysis of the responses received regarding the technical factors of IoT and IIoT security within the SA transport sector. Limitations of the study arose from the fact that a small population with specialised knowledge was targeted; therefore, the results may not be generalisable outside of the SA transport sector.

Results

This section presents the results from the questionnaire relating to the technology factors influencing IoT and IIoT security in the transport sector of South Africa. A total of 73 responses were received; however, eight of these did not have any experience in terms of either IoT or IIoT, and were therefore excluded, leaving 65 valid responses, as illustrated in Table 1.



Note: CIO = Chief Information Officer; CISO = Chief Information Security Officer

Figure 1: Job profiles of the respondents

The respondents indicated a variety of experience with IIoT, as illustrated in Figure 2. As is evident, the majority of respondents were familiar with IIoT from an IT perspective (38%), followed by security experience (18%) and governance, risk and compliance (17%).

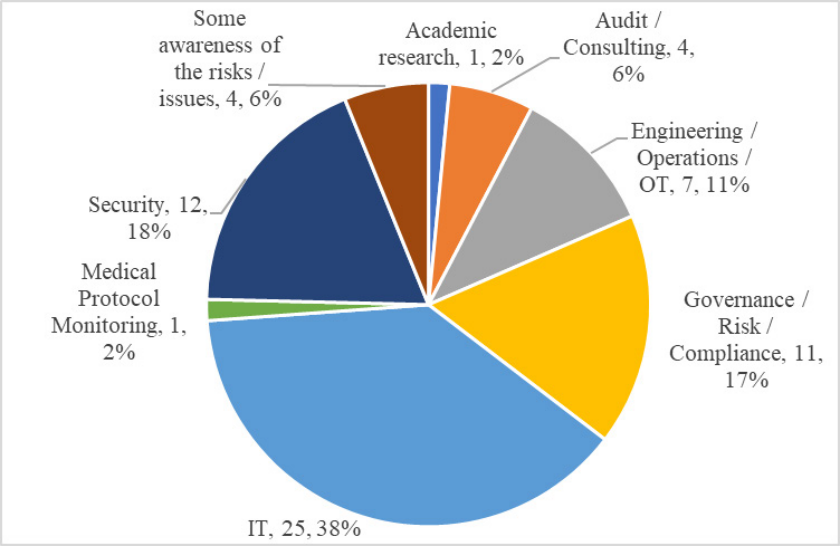


Figure 2: Respondents' experience with IIoT

Figure 3 illustrates the number of years of experience the respondents had with IIoT. The vast majority had less than five years of experience (77%), with 29% having less than one year of experience, and 29% having two to five years of experience. This illustrates the emerging nature of IIoT and its introduction into the environment.

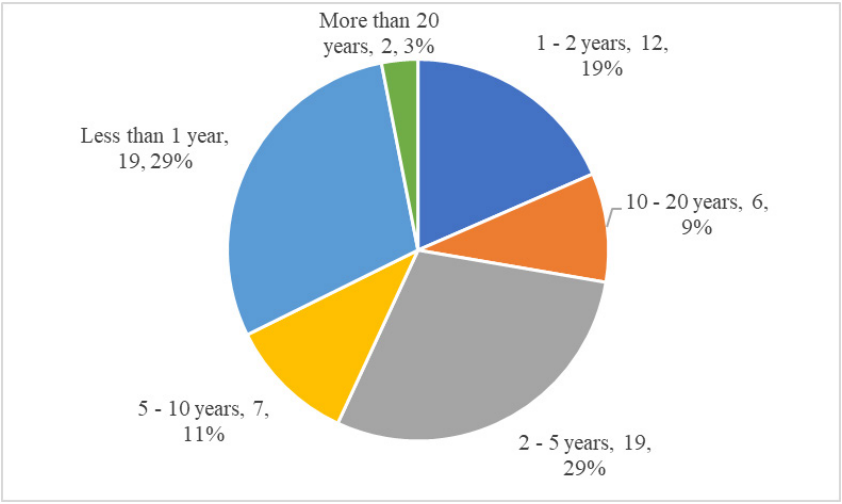


Figure 3: Years of experience with IIoT

Respondents were asked to identify the types of IoT and IIoT present in their environments. Figure 4 illustrates that the vast majority of the respondents had boardroom and/or video conferencing equipment (80%) and CCTV or smart cameras (74%). IIoT is not as prevalent, with ICS and SCADA being indicated the most (60%), followed by vehicle tracking and monitoring (58%). These trends illustrate initial commercial IoT has more penetration in organisations than IIoT.

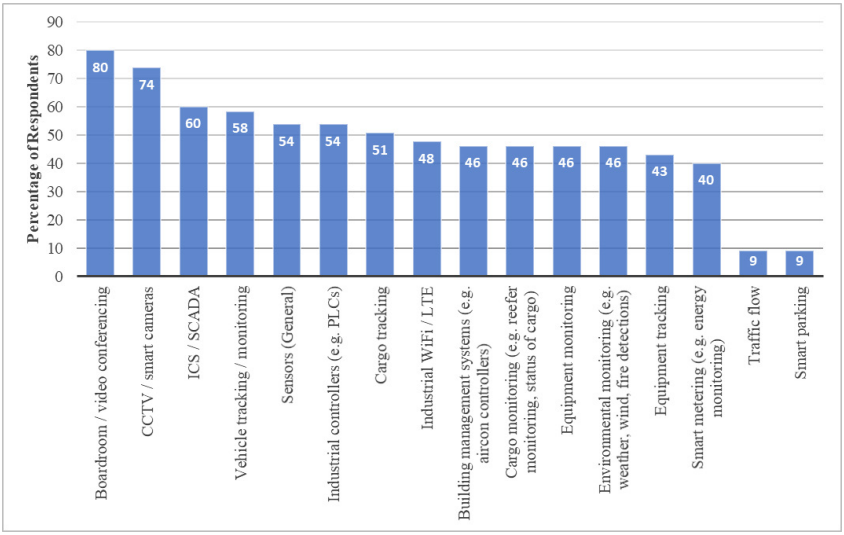


Figure 4: Type of IoT and IIoT devices in the workplace

Perceived IoT and IIoT threats in the South African transport sector

To assess the IoT and IIoT threat landscape with relevance to the SA transport sector, respondents were asked to rate –

- the impact IoT and IIoT will have on the threat landscape;
- the top three perceived threats; and
- whether (at the time) any of the threats had been exploited.

The respondents were asked to rate the impact that IoT and IIoT would have on the threat landscape in the transport sector in South Africa, rating possible threat categories as *Introducing new threats* (5), *Increasing existing threats* (4), a *Slight increase in existing threats* (3), *No change in threats* (2) and *No threat/not relevant* (1). Figure 5 shows the prevalence of responses, and Table 2 provides the descriptive statistics. From the responses, it was noted that the top three threats perceived to be introduced by IIoT are *Remote access*, *Cyber espionage*, and *Signal jamming attacks*. The top threats to be affected by IoT and IIoT (either increasing existing threats or introducing new threats) were *Remote access* with a mean of 4.0, *Cyber espionage* with a mean of 3.9 and *Ransomware* with a mean of 3.8.

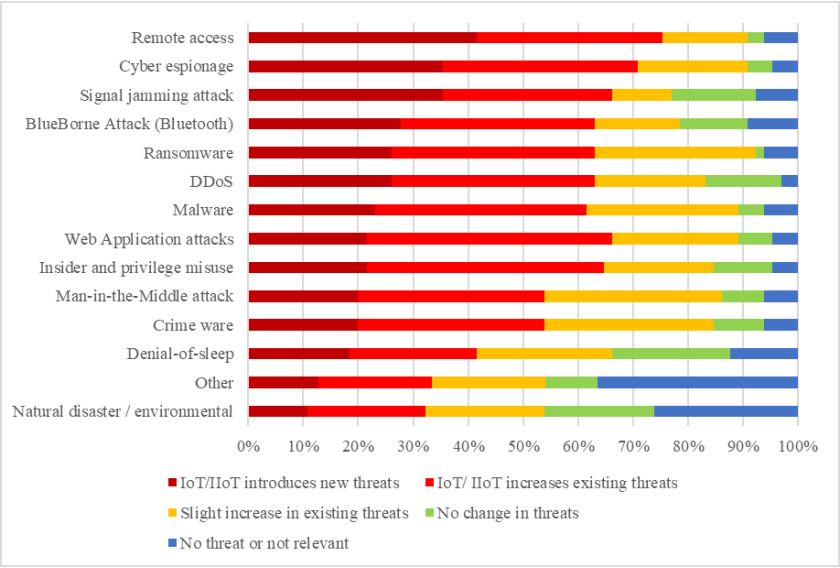


Figure 5: Existing and new threats introduced by IoT and IIoT

Table 2: Frequency and descriptive statistics table of threats

	DDoS	Insider and privilege misuse	Cyber espionage	Web application attacks	Malware	Natural disaster environmental	Crime ware	Denial-of-sleep	Ransomware	Man-in-the-middle attack	Remote access	Signal jamming attack	BlueBorne attack (Bluetooth)	Other
No threat or not relevant	2	3	3	3	4	17	4	8	4	4	4	5	6	23
No change in threats	9	7	3	4	3	13	6	14	1	5	2	10	8	6
Slight increase in existing threats	13	13	13	15	18	14	20	16	19	21	10	7	10	13
IoT/ IIoT increases existing threats	24	28	23	29	25	14	22	15	24	22	22	20	23	13
IoT/IIoT introduces new threats	17	14	23	14	15	7	13	12	17	13	27	23	18	8
Mean	3.7	3.7	3.9	3.7	3.7	2.7	3.5	3.1	3.8	3.5	4.0	3.7	3.6	2.6
Std. deviation	1.1	1.1	1.1	1.0	1.1	1.4	1.1	1.3	1.1	1.1	1.1	1.3	1.3	1.5

Respondents were asked to select three threats from the list in the question that they perceived to be a top threat related to IoT and/or IIoT. The top three threats selected were *Malware,* which was selected by 35 of the respondents*, Insider and privilege misuse* and *Distributed denial of service (DDoS)* was joint second with 29 each and third was *Cyber espionage* with 28. More detailed results are provided in Figure 6.

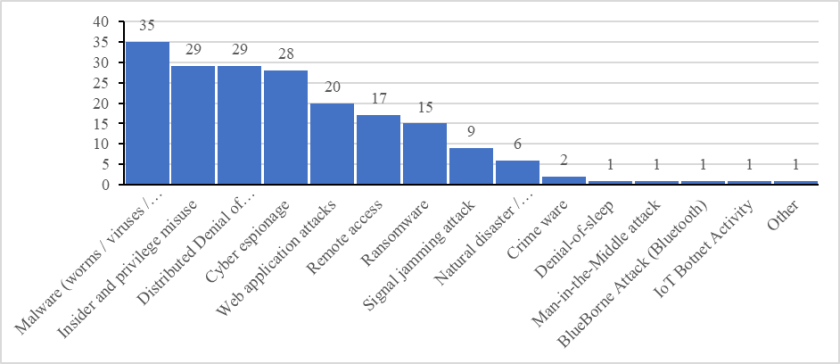


Figure 6: Top three threats related to IoT and IIoT

The respondents were asked to indicate if any of the treats occurred in their organisation's IoT and IIoT environment, and the responses are shown in Figure 7. The largest response showed that respondents were unsure or that a threat might have materialised (36%); followed by an indication that a threat had materialised (29%); while 26% of respondents indicated that they did not have a threat occurring in their IoT and IIoT environment. Some respondents were unable to disclose whether a threat had occurred (9%). The fact that more respondents could confirm a threat than those confirming a threat had not occurred showed that the IoT and IIoT environment in the SA transport sector is susceptible to cyberattacks. The following section discusses the perceived vulnerabilities.

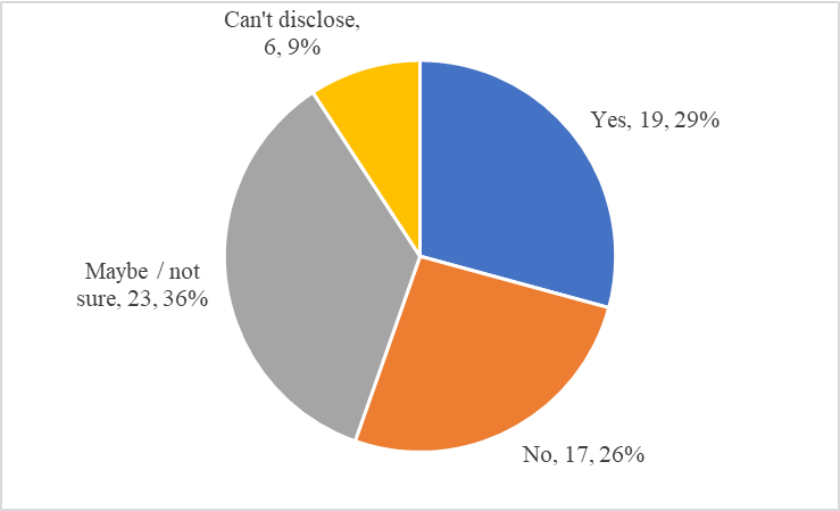


Figure 7: Occurrence of threats

Vulnerabilities related to IoT and IIoT

Respondents were asked to rate a number of vulnerabilities related to IoT and IIoT. Figure 8 and Table 3 show the responses and frequency of the vulnerabilities from Very low (1) to Very high (5) severity. From Figure 8, the top vulnerabilities related to the IoT and IIoT environment in the SA transport sector, ranked on the number of 'Very high' and then 'High' ratings, are:

- *No or delay in Patching / firmware updates*;
- *No or Weak Password*; and
- *Insecure mobile interface*.

From Table 3, the top three vulnerabilities based on the mean of the ratings are:

- *No or delay in Patching / firmware updates* with a mean of 3.8;
- *Insecure Default Settings* with a mean of 3.69; and
- *Insecure mobile interface* with a mean of 3.66.

All of these can be considered a *Medium Risk* moving towards *High*.

The vulnerabilities that appeared to be of least concern are:

- *Lack of physical hardening* and *No privacy protection* both with a mean of 3.3,
- *Insecure network perimeter* and *Insecure network services*, both with a mean of 3.4.

This implies the feedback overall considers most vulnerabilities introduced by IoT and IIoT as *Medium*.

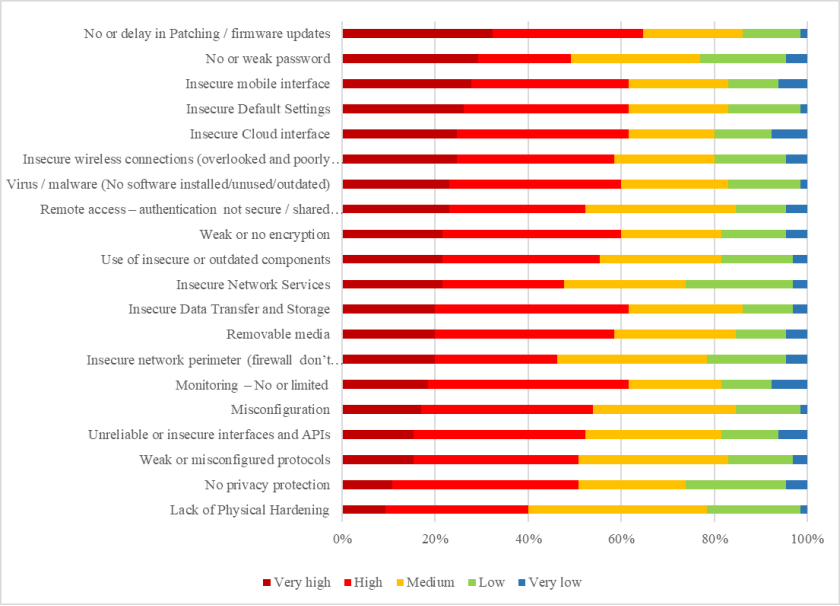


Figure 8: Vulnerabilities related to IoT and IIoT

Table 3: Frequency and descriptive statistics of the vulnerabilities

	Very low	Low	Medium	High	Very high	Mean	Std. deviation	Variance
No or weak password	3	12	18	13	19	3.5	1.2	1.5
No or delay in Patching / firmware updates	1	8	14	21	21	3.8	1.1	1.2
Misconfiguration	1	9	20	24	11	3.5	1	1
Weak or no encryption	3	9	14	25	14	3.6	1.1	1.2
Removable media	3	7	17	25	13	3.6	1.1	1.2
Insecure default settings	1	10	14	23	17	3.7	1.1	1.2
Weak or misconfigured protocols	2	9	21	23	10	3.5	1	1

	Very low	Low	Medium	High	Very high	Mean	Std. deviation	Variance
Unreliable or insecure interfaces and APIs*	4	8	19	24	10	3.4	1.1	1.2
Virus / malware (no software installed/unused/ outdated)	1	10	15	24	15	3.6	1.1	1.1
Insecure wireless connections (overlooked and poorly configured)	3	10	14	22	16	3.6	1.2	1.3
Lack of physical hardening	1	13	25	20	6	3.3	0.9	0.9
Remote access – authentication not secure / shared passwords for vendors	3	7	21	19	15	3.6	1.1	1.2
Monitoring – no or limited	5	7	13	28	12	3.5	1.1	1.3
Insecure network perimeter (firewall don't exist/misconfigured, direct connections to internet)	3	11	21	17	13	3.4	1.1	1.3
No privacy protection	3	14	15	26	7	3.3	1.1	1.2
Insecure network services	2	15	17	17	14	3.4	1.2	1.3
Use of insecure or outdated components	2	10	17	22	14	3.6	1.1	1.2
Insecure data transfer and storage	2	7	16	27	13	3.6	1	1
Insecure cloud interface	5	8	12	24	16	3.6	1.2	1.5
Insecure mobile interface	4	7	14	22	18	3.7	1.2	1.4

Note: API = Application Programming Interface

Risks of unsecured IoT and IIoT (impact)

Respondents were asked to rate risks of IoT and IIoT based on **impact** – *Insignificant* (1) to *Extreme/catastrophic* (5) – and **likelihood** – *Very low* (1) to *Very high* (5). Figure 9 shows the respondents' rating of the impact of compromised IoT and IIoT devices, and Table 4 provides descriptive statistics of the potential impact.

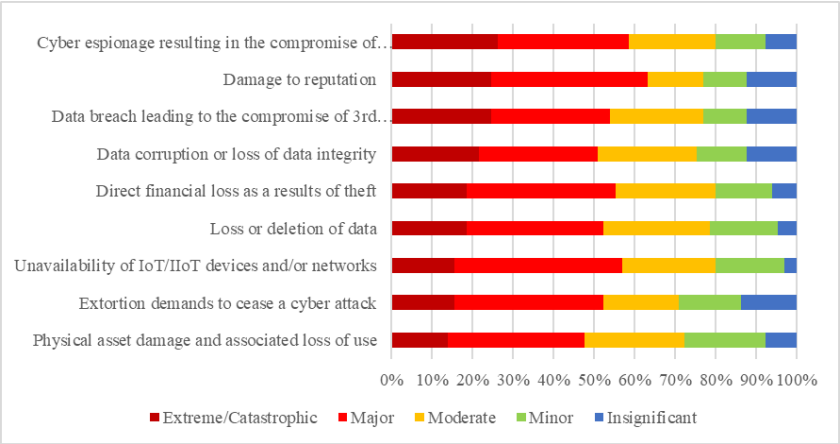


Figure 9: Risk (impact) related to IoT and/or IIoT

From the responses, the top three risks that have the most impact in terms of IoT and IIoT in the transport sector of South Africa are:

- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* with a mean of 3.57;
- *Damage to reputation* with a mean of 3.52; and
- *Unavailability of IoT/IIoT devices and/or networks* with a mean of 3.49.

These are all *Moderate* impacts.

The three risks that are of least concern regarding their potential impact if compromised are:

- *Extortion demands to cease a cyber attack* with a mean of 3.25;
- *Physical asset damage and associated loss of use* with a mean of 3.26; and
- *Data corruption or loss of data integrity* with a mean of 3.35.

Again, these are all *Moderate* impacts, implying that, in general, IoT and IIoT will result in a *Moderate* impact to the organisation if compromised.

Table 4: Frequency and descriptive statistics of risks (impact)

	Physical asset damage and associated loss of use	**Unavailability of IoT/IIoT devices and/or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyber attack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Very low	5	2	3	8	8	5	9	4	8
Low	13	11	11	8	7	8	10	9	7
Medium	16	15	17	16	15	14	12	16	9
High	22	27	22	19	19	21	24	24	25
Very high	9	10	12	14	16	17	10	12	16
Mean	3.26	3.49	3.45	3.35	3.43	3.57	3.25	3.48	3.52
Std. deviation	1.2	1.0	1.1	1.3	1.3	1.2	1.3	1.1	1.3
Variance	1.4	1.1	1.3	1.7	1.7	1.5	1.7	1.3	1.7

For the likelihood of an impact occurring, respondents were asked to rate each category from *Very low* (1) to *Very high* (5). Figure 10 shows the likelihood of the risks due to compromised IoT and IIoT devices ranked according to the most responses for *Very high*, *High*, with *Very low* being the lowest priority. The top three risks by likelihood arranged according to Very high and High responses are *Damage to reputation*, *Cyber espionage*, and *Data breach leading to a compromise of 3rd party*.

Table 5 shows the frequency and full descriptive statistics of the likelihood ratings. From the responses, the top three risks that are rated most likely to occur are:

- *Unavailability of IoT/IIoT devices and/or networks* with a mean of 3.49;
- *Damage to reputation* with a mean of 3.4; and
- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information* with a mean of 3.31.

These are all slightly above *Medium* likelihoods.

The three risks that are rated least likely to occur are:

- *Extortion demands to cease a cyber attack* with a mean of 3.02;
- *Data corruption or loss of data integrity* with a mean of 3.06; and
- *Loss or deletion of data* with a mean of 3.15

Again, these are all *Medium* likelihoods.

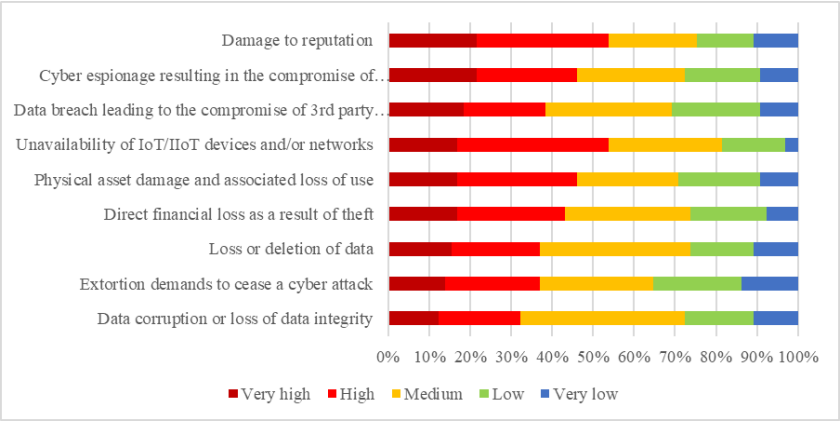


Figure 10: Risk (likelihood) related to IoT and IIoT

Table 5: Frequency and descriptive statistics of risks (likelihood)

	Physical asset damage and associated loss of use	Unavailability of IoT/HoT devices and/or networks	Loss or deletion of data	Data corruption or loss of data integrity	Data breach leading to the compromise of 3rd party confidential information, including personal information	Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information	Extortion demands to cease a cyber attack	Direct financial loss as a result of theft	Damage to reputation
Very low	6	2	7	7	6	6	9	5	7
Low	13	10	10	11	14	12	14	12	9
Medium	16	18	24	26	20	17	18	20	14
High	19	24	14	13	13	16	15	17	21
Very high	11	11	10	8	12	14	9	11	14
Mean	3.25	3.49	3.15	3.06	3.17	3.31	3.02	3.26	3.40
Std. deviation	1.2	1.0	1.2	1.1	1.2	1.3	1.3	1.2	1.3
Variance	1.5	1.1	1.4	1.3	1.5	1.6	1.6	1.4	1.6

The risk for each of the categories is listed in Table 6 and illustrated in Figure 11, taking into account both the mean impact ratings and the mean likelihood ratings. For Table 6, *Risk* is calculated as the product of the mean for *Impact* and *Likelihood*, and has a range of 1 to 25. The highest risk is shown in the top right corner, and the lowest risk is reflected in the bottom left corner.

The top three risks are

- *Unavailability of IoT/IIoT devices and/or networks*;
- *Damage to reputation*; and
- *Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information*.

The three categories presenting the lowest risks for IoT/IIoT are:

- *Extortion demands to cease a cyber attack*;
- *Data corruption or loss of data integrity*; and
- *Physical asset damage and associated loss of use*.

It is also evident from Figure 11 that the risks are clustered together because the mean of the **Impact** and **Likelihood** ratings were all between 3 and 4. There is therefore no distinct category risk posed by IoT and IIoT, but there is a clear risk present.

Table 6: Calculated risk for IoT and IIoT

	Physical asset damage and associated loss of use	**Unavailability of IoT/IIoT devices and/or networks**	**Loss or deletion of data**	**Data corruption or loss of data integrity**	**Data breach leading to the compromise of 3rd party confidential information, including personal information**	**Cyber espionage resulting in the compromise of trade secrets, research and development, and other sensitive information**	**Extortion demands to cease a cyber attack**	**Direct financial loss as a result of theft**	**Damage to reputation**
Very low	6	2	7	7	6	6	9	5	7
Low	13	10	10	11	14	12	14	12	9
Medium	16	18	24	26	20	17	18	20	14

High	19	24	14	13	13	16	15	17	21
Very high	11	11	10	8	12	14	9	11	14
Mean	3.25	3.49	3.15	3.06	3.17	3.31	3.02	3.26	3.40
Std. deviation	1.2	1.0	1.2	1.1	1.2	1.3	1.3	1.2	1.3
Variance	1.5	1.1	1.4	1.3	1.5	1.6	1.6	1.4	1.6

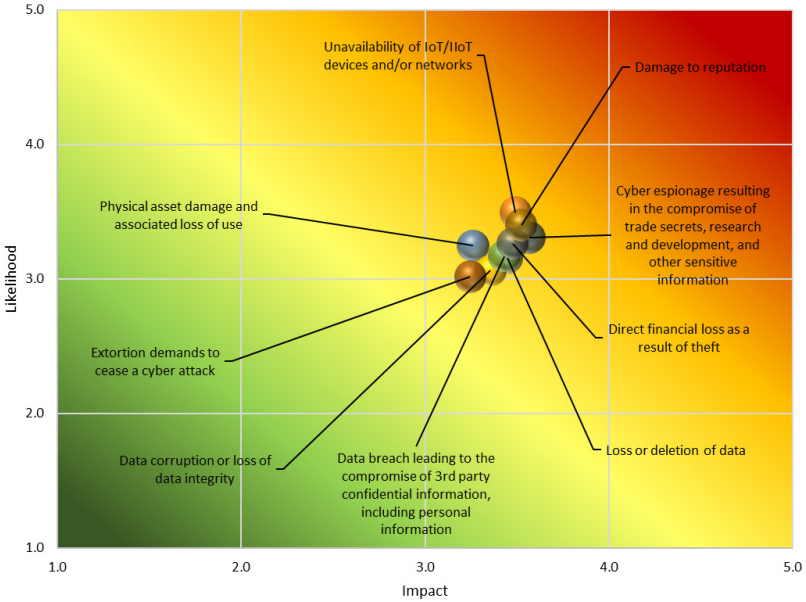


Figure 11: Risk (impact vs likelihood)

Discussion and recommendations

Within the transport sector, there is a prevalence of IoT in terms of smart TVs for boardrooms and CCTV systems, with lower penetration of IIoT. The smart TVs and CCTV systems are of particular note, particularly due to concerns of eavesdropping via the smart TVs, and the use of CCTV systems in the notorious Mirai botnet used to conduct DdoS attacks. Two of the top three perceived risks are therefore aligned to these specific IoT devices: cyber espionage relating to the TVs, and IoT and IIoT and network unavailability relating to the possibility of DdoS due to compromised IoT devices.

Similarly, the top three threats where IoT and IIoT are perceived to introduce new threats are *Remote access*, *Cyber espionage*, and *Signal jamming attacks*. The cyber espionage as described above, and the signal jamming attacks have been reported as discussed in the Literature review above. Remote access is also aligned to incidents that have occurred regarding the IoT that is reported to be prevalent in the sector. When considering the top three threats by the mean of the responses, *Ransomware* replaces *Signal jamming*. An increase in ransomware has been seen, and has negatively affected maritime organisations such as Maersk and Transnet.

When considering the top three threats in general related to IoT and IIoT (compared to being increased by IoT and IIoT), *Malware* was first, followed jointly by *Insider and privilege misuse* and *DdoS*, then *Cyber espionage*. *Cyber espionage* is evidently a recurring theme of concern to the sector. *Malware* has become a common threat related to IoT and IIoT, and *Insider threats* refer to the possibility of insecure rogue devices breaching security. In addition, insider threats were listed as one of the major categories of cyber incidents in 2019 (McKee, 2019). A key recommendation for IoT and IIoT is network segmentation and to include the IoT and IIoT networks in security monitoring in order to detect any abnormalities on the network which could signify the presence of malware, misuse, DdoS, or cyber espionage. Traditional perimeter monitoring security should be updated to ensure the IoT and IIoT environment are catered for.

The perceived vulnerabilities include *No or delay in Patching / firmware updates* and *Insecure mobile interface*, both in the top three based on the number of *Very high* responses as well as the mean of responses. *No or Weak Password* was in the top three based on *Very high* responses, and *Insecure Default Settings* was in the top three based on the mean. All of these perceived vulnerabilities related to the concept of 'insecure by design', where products are provided without sufficient security testing or unacknowledged bugs (Solomon, 2022). These vulnerabilities could allow malicious users the ability to compromise IoT and IIoT devices easily to gain a foothold in a network, and has been demonstrated by a number of incidents. The latter two vulnerabilities can be seen as a 'low-hanging fruit' in that they should be fairly simple to correct by immediately changing the default settings and passwords to secure the devices. A procurement requirement for IoT and IIoT devices that could be included is that the devices must not have hard-coded (i.e. impossible to change) passwords. During project design stage of IoT and IIoT, it is important to consider the patching and the security of such devices, and to conduct adequate security testing well before deploying them to allow for time to make the necessary security adjustments in the interfaces and patching methods if required.

IoT and IIoT present a clear general risk, rated as *Moderate* but leaning towards *High*. While there is no clear risk category that is higher than any other, the top three (*Unavailability of IoT/IIoT devices and/or networks*, *Damage to reputation*, and *Cyber espionage*) signify availability and data theft concerns (which could in turn could have privacy implications). These two categories explain the third, *Damage to reputation*, as an outage of the networks affecting delivery of products or services, or a data breach being discovered, that would lead to reputational damage of the organisation. In terms

of service disruption, the NotPetya incident affecting Maersk and the ransomware at Transnet are prime examples. Overall, the responses align to actual incidents that have been experienced.

As is evidenced from the demographics, IoT and IIoT are still relatively new within the SA transport sector, with 38% of respondents having two years or less of experience, and another 29% having two to five years of experience. It is therefore important to continue similar research, as the environment becomes increasingly established, to assess any changes in the threat landscape (or perceptions thereof). Future research could include an investigation into prevalent industry IoT and IIoT security frameworks in order to propose a dedicated IoT and IIoT security framework for the SA maritime and freight transport sectors.

Conclusion

The IoT and IIoT present benefits to the maritime and related transport sectors; however, IoT and IIoT may introduce vulnerabilities and broaden the attack surface. A number of cybersecurity incidents have been perpetuated through the use of insecure IoT devices. The transport sector, and the maritime sector in particular, have seen increasing cybersecurity incidents; for example, the ransomware incidents that disrupted operations at Maersk and Transnet. It is therefore important to research the potential effect of introducing IoT and IIoT into the environment.

This study investigated the threats, vulnerabilities and risks associated with IoT and IIoT in the SA transport sector. Questionnaires were distributed using convenience and snowball sampling. Remote access, cyber espionage and signal jamming were top threats considered to be introduced along with IoT and IIoT, while malware, insider or privilege misuse, DDoS and cyber espionage were the top threats associated with IoT and IIoT in general. Key vulnerabilities include issues with patching and firmware updates, weak authentication, insecure default settings, and insecure interfaces. While there were no clear leaders of risk, the top three risks based on the perceived severity and likelihood are unavailability of IoT and IIoT devices and/or networks, damage to reputation, and cyber espionage. In general, the responses align to cybersecurity incidents that have already occurred. Recommendations are to ensure that the IoT and IoT devices in existing security controls are considered, that they are on segregated networks, and that security is a key design and procurement consideration for IoT and IIoT devices.

About the Authors

Barend Pretorius holds a Master's degree in Information Systems and a Bachelor of Science (Honours) in Mathematical Statistics. He is studying towards a PhD focusing on the Cyber Security of Industrial Internet of Things and is a Certified Information Security Manager (CISM). He joined Transnet Group in 2014 as a Senior Information Security Analyst and was transferred in 2017 as the Information Security Officer at one of its divisions, Transnet Port Terminals (TPT). He was promoted in 2020 to Senior Manager for ICT Support Service at TPT, responsible for Cyber Security, Networks, Infrastructure,

Cloud and End user computing. In 2022 he was promoted and transferred to Transnet Group where he is currently in the role of Senior Specialist: Information Security & Governance responsible for establishing and maintaining an enterprise-wide information security program, enterprise-wide information security strategy, including an Information Security Management System, ICT Governance, Risk, and Compliance.

Prof Brett van Niekerk (PhD) is an associate professor in the Department of Information Technology at the Durban University of Technology, a non-resident fellow at the Security Institute for Governance and Leadership in Africa (Stellenbosch University), chairs the International Federation of Information Processing Working Group on ICT in Peace and War, and is Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has cybersecurity experience across industry, academia and civil society. He has actively participated in international cybersecurity forums (Global Commission on the Stability of Cyberspace, Paris Call working groups, Carnegie Endowment for International Peace's project on countering influence operations). He is CISM certified, with over 50 academic publications and 20 presentations at industry events.

References

Akpan, F., Bendiab, G., Shiaeles, S. & Karamperidis, S. 2022. Cybersecurity challenges in the maritime sector. *Network*, 2, 123–138.

Australian Government. 2018. *Security of Critical Infrastructure Act 2018*. Available at: <https://www.legislation.gov.au/Details/C2018A00029/Download> [Accessed 25 May 2022].

Awan, J.H., Memon, S., Shah, A.A. & Pathan, K.J. 2020. Proposed framework of smart transportation in Pakistan: Issues, challenges, vulnerabilities, and solutions. *International Journal of Cyber Warfare and Terrorism*, 10(4), 48–63.

Ayyagari, M. 2018. *Five smart ways how IoT is transforming the railways*. CYIENT. Available at: <https://www.cyient.com/blog/rail-transportation/five-smart-ways-how-iot-is-transforming-the-railways> [Accessed 24 June 2022].

Bowne, M. 2015. *IOT vs. IIOT*. Profinet. Available at <http://us.profinet.com/iot-vs-iiot/> [Accessed 14 October 2019].

Bronk, C. & Tikk-Ringas, E. 2013. The cyber attack on Saudi Aramco. *Survival*, 55(2), 81–96.

Burkhalter, M. 2022. IoT at sea: *How the internet of things powers the maritime industry*. Perle. Available at: <https://www.perle.com/articles/iot-at-sea-how-the-internet-of-things-powers-the-maritime-industry-40193572.shtml> [Accessed 24 June 2022].

Chan, B. 2017. *Industrial IoT versus IoT: Do you know the difference?* Strategy of Things. Available at: <https://strategyofthings.io/industrial-iot> [Accessed 14 October 2019].

Chen, P. 2016. *Why security in the Internet of Things is different from cybersecurity*. EDN-Europe. Available at: <http://www.edn-europe.com/blog/why-security-internet-things-different-cybersecurity> [Accessed 12 July 2016].

Cimpanu, C. 2017. *University DDoSed by its own IoT devices*. BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/university-ddosed-by-its-own-iot-devices/> [Accessed 20 February 2017].

Cimpanu, C. 2018. *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack.* BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack> [Accessed 7 September 2018].

Clayton, M. 2013. *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*. The Christian Science Monitor. Available at: <https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage> [Accessed 3 June 2022].

CyberKeel. 2014. *Maritime cyber-risks: Virtual pirates at large on the cyber seas*. Available at: <http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf> [Accessed 24 June 2022].

Cybersecurity and Infrastructure Security Agency. 2020. *Transportation systems sector*. Available at: https://www.cisa.gov/transportation-systems-sector [Accessed 24 May 2022].

Darktrace. 2016. *Darktrace discoveries: Global threat case studies 2016*. Available at: <http://www.informationweek.com/whitepaper/cybersecurity/security/darktrace-discoveries-global-threat-case-studies-2016/383043> [Accessed 14 June 2017].

Dooley, R. 2017. Cyber security at the heart of the Fourth Industrial Revolution, I. *UK Construction Online*, 15 June. Available at: <https://www.ukconstructionmedia.co.uk/features/cyber-security-industrial-revolution/> [Accessed 24 June 2022].

Dunn, J.E. 2013. Hackers planted remote devices to smuggle drugs through Antwerp port, Europol reveals. *Techworld*, 16 October. Available at: <http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggledrugs-through-antwerp-port-europol-reveals/> [Accessed 22 June 2022].

Fletcher, D. & Bye, P. 2022. *Cybersecurity in transit systems*. The National Academies Press. Available at: <https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems> [Accessed 27 May 2022].

Forrest, C. 2016. How the Mirai botnet almost took down an entire country, and what your business can learn. *Tech Republic*, 3 November. Available at: <https://www.techrepublic.com/article/how-the-mirai-botnet-almost-took-down-an-entire-country-and-what-your-business-can-learn/> [Accessed 24 June 2022].

Gallagher, R. & Burkhardt, P. 2021. 'Death Kitty' ransomware linked to South African port attack. *Bloomberg*, 29 July. Available at: <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports> [Accessed 3 January 2022].

Gartner. 2022. *Internet of Things (IoT)*. Gartner Glossary. Available at: <https://www.gartner.com/en/information-technology/glossary/internet-of-things/> [Accessed 24 June 2022].

Goward, D. 2019. GPS jamming and spoofing reported at port of Shanghai. *The Maritime Executive*, 13 August. Available at: <https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai> [Accessed 27 May 2022].

Henning, C. 2017. *7 steps to IIoT*. Profinet. Available at: <http://us.profinet.com/7-steps-iiot/> [Accessed 7 September 2019].

Ismail, S., Sitnikova, E. & Slay, J. 2015. SCADA systems cyber security for critical infrastructures: Case studies in the transport sector. In *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015)*, 425–433.

Johnson, J. 2017. Securing industrial IoT: There is no simple answer. *IIoT World*, 15 June. Available at: <https://www.iiot-world.com/ics-security/cybersecurity/securing-industrial-iot-there-are-no-simple-solutions/> [Accessed 24 June 2022].

Kan, M. 2016. DDoS attack on Dyn came from 100,000 infected devices. *Computer World*, 26 October. Available at: <http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html> [Accessed 31 October 2016].

Kapkaeva, N., Gurzhiy, A., Maydanova, S. & Levina, A. 2021. Digital platform for maritime port ecosystem: Port of Hamburg case. *Transportation Research Procedia*, 54, 909–917.

Kerner, S.M. 2022. Colonial pipeline hack explained: Everything you need to know. *TechTarget*, 26 April. Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [Accessed 6 July 2022].

Knox, J. 2015. *Coast guard commandant on cyber in the maritime domain*. US Coast Guard. Available at: <https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/> [Accessed 27 May 2022].

Kovacs, E. 2014. Default password exposes digital highway signs to hacker attacks. *Security Week*, 6 June. Available at: <http://www.securityweek.com/default-password-exposes-digital-highway-signs-hacker-attacks> [Accessed 24 July 2020].

Kravets, D. 2009. Feds: Hacker disabled offshore oil platforms' leak detection system. *Wired*, 18 March. Available at: <https://www.wired.com/2009/03/feds-hacker-dis/> [Accessed 27 May 2022].

Ku, R. & Weiss, J. 2017. *Integrating security into the IoT strategy in the new converged environment*. Trend Micro.

KVH Watch. 2021. How using dedicated maritime IoT connectivity produces cost savings. *The Maritime Executive*, 27 September. Available at: <https://www.maritime-executive.com/features/how-using-dedicated-maritime-iot-connectivity-produces-cost-savings> [Accessed 24 June 2022].

Lomas, N. 2015. Samsung edits Orwellian clause out of TV privacy policy. *Tech Crunch*, 10 February. Available at: <https://techcrunch.com/2015/02/10/smarttv-privacy/> [Accessed 12 June 2017].

Marchant, N. 2021. *What is the Internet of Things?* World Economic Forum. Available at: <https://www.weforum.org/agenda/2021/03/what-is-the-internet-of-things/> [Accessed 24 June 2022].

McCue, A. 2003. 'Revenge' hack downed US port systems. *ZDNet*, 7 October. Available at: http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/> [Accessed 27 May 2022].

McKee, M. 2019. Insider threats: Manufacturing's silent scourge. *Industry Week*, 25 April. Available at: <https://www.industryweek.com/technology-and-iiot/article/22027503/insider-threats-manufacturings-silent-scourge> [Accessed 24 June 2022].

Miller, B. & Rowe, D.C. 2012. A survey of SCADA and critical infrastructure incidents. Paper presented at the ACM Special Interest Group on Information Technology Education (SIGITE) Research in IT Conference, 11–13 October.

Min, H. 2022. Developing a smart port architecture and essential elements in the era of Industry 4.0. *Maritime Economics & Logistics*, 24, 189–207.

Molavi, A., Lim, G. & Race, B. 2019. A framework for building a smart port and smart port index. *International Journal of Sustainable Transportation*, 14(9) 686–700.

Pretorius, B.H. & Van Niekerk, B. 2020. Industrial Internet of Things security for the transportation infrastructure. *Journal of Information Warfare*, 19(3), 50–67.

Ragan, S. 2012. Railway network disrupted after cyber attack, report says. *Security Week*, 25 January. Available at: <http://www.securityweek.com/railway-network-disruptedafter-cyber-attack-report-says> [Accessed 24 June 2022].

Schiffer, A. 2017. How a fish tank helped hack a casino. *The Washington Post*, 21 July. Available at: <https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/> [Accessed 24 June 2022].

Solomon, H. 2022. Many OT products are 'insecure by design,' say researchers. *IT World Canada*, 22 June. Available at: <https://www.itworldcanada.com/article/many-ot-products-are-insecure-by-design-say-researchers/489735> [Accessed 24 June 2022].

Starr, M. 2014. Fridge caught sending spam emails in botnet attack. *CNET*, 19 January. Available at: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/> [Accessed 10 March 2015].

Sullivan, P. 2020. Critical IIoT security risks cloud IoT's expansion into industry. *Tech Target*, September. Available at: <https://www.techtarget.com/searchsecurity/tip/Critical-IIoT-security-risks-cloud-IoTs-expansion-into-industry> [Accessed 24 June 2022].

Swanbeck, S. 2015. *Coast guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs.* Center for Strategic and International Studies. Available at: <https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities> [Accessed 27 May 2022].

Theoharidou, M., Kandias, M. & Gritzalis, D. 2011. Securing transportation-critical infrastructures: Trends and perspectives. In C.K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush & A. Al-Nemrat (eds.). *Global security, safety and sustainability & e-democracy.* Lecture notes of the Institute for Computer Sciences, Social Informatics and

Telecommunications Engineering, Volume 99. Berlin: Springer, 171-178.

Townsend, K. 2019. Industry is not prepared for the IIoT attacks that have already begun. *Security Week*, 30 May. Available at: <https://www.securityweek.com/industry-not-prepared-iiot-attacks-have-already-begun> [Accessed 24 June 2022].

Van Niekerk, B. 2017. Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (ed.). *Threat mitigation and detection of cyber warfare and terrorism activities.* Hershey, PA: IGI-Global, 68–91.

Vaughan-Nichols, S. 2019. FBI warns about snoopy smart TVs spying on you. *ZDNET*, 3 December. Available at: <https://www.zdnet.com/article/fbi-warns-about-snoopy-smart-tvs-spying-on-you/> [Accessed 24 June 2022].

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-idUSBREA3M20820140424> [Accessed 27 May 2022].

Warrick, J. & Nakashima, E. 2020. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*, 18 May. Available at: <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html> [Accessed 27 May 2022].

Woolf, N. 2016. DDoS attack that disrupted internet was largest of its kind in history, experts say. *The Guardian*, 26 October. Available at: <https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet> [Accessed 9 June 2016].

Zimmerman, G. 2017. Target settles HVAC data breach for $18.5 million. *FacilitiesNet*, 25 May. Available at: <https://www.facilitiesnet.com/hvac/tip/Target-Settles-HVAC-Data-Breach-for-185-Million--39237> [Accessed 24 June 2022].

Scientia Militaria
2023, VOL. 51, NO. 3, 161-186
DOI: 10.5787/51-3-1430

Vulnerability of South African Commodity Value Chains to Cyber Incidents

Brett van Niekerk
Durban University of Technology

Abstract

A commodity value chain can be considered the 'route' from the source (provider) to the destination (client), including the various modes of transportation. This will often include some form of road or rail to a port for export to a destination country. Due to the rise in cybercrime and state-backed cyber operations, these commodity value chains may be disrupted, having a cascading effect down the value chain. Previous research has considered this a form of economic information warfare, and has indicated that state-sponsored cyber operations to disrupt a commodity intentionally will most likely fall below the threshold of a 'use of force' or 'attack' under international law. Subsequently, two pertinent instances of cyber incidents at ports have occurred: the disruption of a major Iranian port, and a ransomware incident at a major South African freight and logistics state-owned enterprise.

Following the disruption resulting from the ransomware incident affecting South African freight organisations, there is a need to analyse the vulnerabilities of the freight transportation sector further, in particular the ports and associated railways in terms of malicious cyber interference. Expanding previous research, this article provides a specific view of the major commodity value chains in South Africa that are supported by the freight transportation infrastructure, their possible vulnerability to cyber incidents, and the potential implications thereof. In addition, publicly available information on the responses to the ransomware incident will be discussed to gauge national readiness in terms of crisis management of a major disruption to the primary trade mechanisms in the country. The article focuses on identifying single points of failure within the commodity value chain, and employs hypothetical scenarios to illustrate possible ramifications of a major incident. The port of Durban is shown to the most critical single point of failure overall. Recommendations include the introduction of a sector-specific computer security incident response team for the freight transportation sector.

Keywords: commodity value chain, critical infrastructure, cyber incident, cybersecurity, maritime security

Introduction

In July 2021, the South African (SA) national freight and logistics organisation suffered a cyber incident that disrupted operations in the container terminals and resulted in freight delays, and *force majeure* was declared at the ports (Gallagher & Burkhardt,

2021; Ginindza, 2021; Njini & Viljoen, 2021). It was estimated that maritime trade contributes between 80% and 90% of the SA economy (Department of Transport [DoT], 2017); however, statistics by the United Nations Conference on Trade and Development (UNCTAD) (2018) show that, at the time, South Africa was losing its prominence in the region based on the liner shipping connectivity index (LSCI). It is therefore imperative that the South African physical freight distributions network be considered in terms of its vulnerability to disruptive cyber incidents, as further significant disruptions will erode the confidence in South Africa as a transport hub. Related to the ports, the railways transport freight between the ports and the source (for export) or destination (for imports).

Problem statement

Trade is the lifeblood of economies, and the majority of the trade is transported through the maritime sector, interconnected with railways. With the severe disruption of SA ports due to a ransomware incident in 2021, the susceptibility of trade routes to cyber interference was demonstrated. There is therefore a need to identify high-level vulnerabilities within the SA freight transportation infrastructure, which supports the nation's major commodity value chains. The objectives of the current study were to –

- conduct an analysis of the physical transport infrastructure supporting the commodity value chains in order to identify critical single points of failure;
- assess the potential impacts of cyber incidents; and
- provide recommendations to mitigate cyber incidents affecting the commodity value chains.

Research design and methodology

The research adopted a positivist standpoint, i.e. a view that the world can be measured. The study therefore analysed the SA freight logistics based on commodity value chains, i.e. the ports, customs, railways and related infrastructure to transport various commodities between the source and destination within the country. In particular, single points of failure are identified at a high level. In the field of critical infrastructure protection, single points of failure are components of a broader system where there is no redundancy, and any failure of this component will result in a severe disruption across the system (Moore, 2018). The contribution of commodities to the national gross domestic product (GDP) and measurements of the throughput of various components of the freight transportation infrastructure (ports and rail routes) are used to calculate potential single points of failure. Hypothetical scenarios are employed to illustrate potential impacts of cyber incidents on the commodity value chains.

The study was limited to a high-level strategic setting, and consequently did not provide in-depth coverage of specific technologies or technical vulnerabilities. The high-level premises can be generalised to apply the analysis to other nations, even though the focus was on the SA situation.

Layout of the article

The article presents a discussion of the SA freight transportation and commodity value chains next, followed by an overview of cybersecurity for physical transportation and commodity value chains. An assessment for potential disruption of the SA freight and maritime environment due to cyber incidents follows to conclude the article.

South African freight transportation and commodity value chains

Overview of value chains

A value chain can be defined as a "system of interdependent activities, which are connected by linkages" (Porter & Millar, 1985:n.p.). In a freight transportation context, commodity value chains can then be considered to contain, but are not limited to, the following processes that enable the transportation of various commodities between the source and destination within the country or internationally (Loomis, Singh, Kessler & Bellenkens, 2021):

- vessel management and navigation;
- piloting and berthing at the ports;
- loading and offloading cargo from vessels;
- customs processes;
- information technology (IT) systems to manage the port and cargo in the port precinct;
- loading and offloading cargo from trains and trucks;
- access control for trucks;
- switching and control of railways;
- toll booths for major roads; and
- dispatch and receiving processes at the source and destination respectively.

Figure 1 provides a high-level conceptualisation of a hypothetical commodity value chain from the point where the commodity is being dispatched from the source, until the time it is received at the destination.

Freight transportation and commodity value chains in South Africa

In South Africa, there are nine key commodities that contributed 42.9% of the national GDP in the 2020–2021 financial year, namely (in order of contribution): agriculture (~12.5%), containers (~12%), automotive (~7%), liquid fuels (~6%), coal (~3%), iron ore (~1.5%), manganese (~1%), chrome and magnetite (~0.5%) (Transnet, 2021a). Of these, the top four commodities contribute approximately 37% of the GDP.

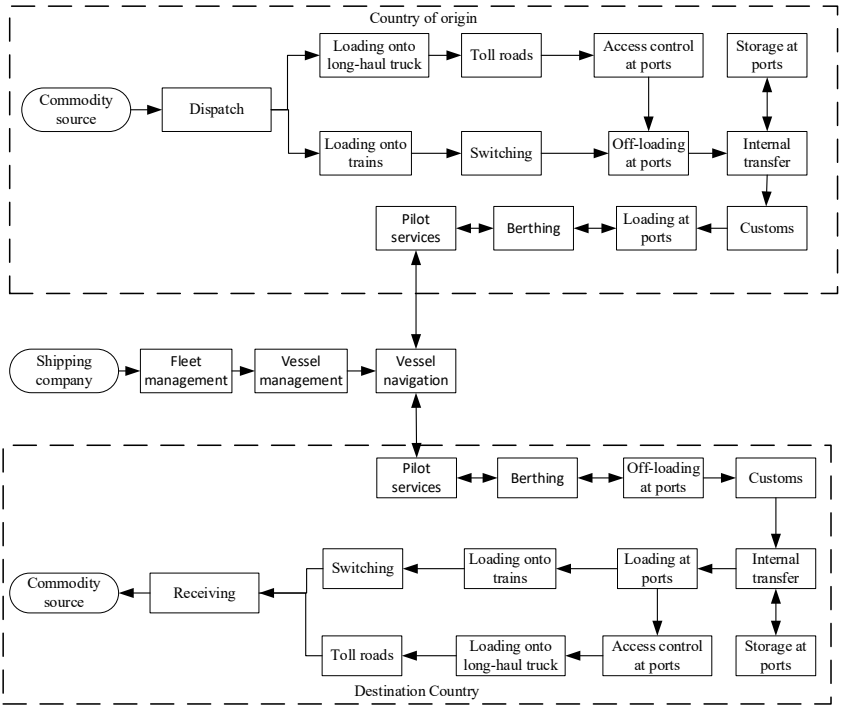


Figure 1: High-level perspective of a value chain

Table 1 below provides an overview of the commodities at and capacities of the SA ports. In addition to the data below, each port has a focus on specific mineral or agricultural products. For mineral bulk, Port Elizabeth handles manganese; Richards Bay deals with numerous mineral products, but primarily coal; and Saldanha handles iron ore and steel products. Wheat and maize are transported through Durban and East London; fresh produce is handled at Cape Town; and Durban handles woodchips, soya bean meal, and animal feed (Transnet Port Terminals [TPT], 2013a).

Table 1: Commodity capacities for South African ports

	Agricultural bulk	Break bulk	Mineral bulk	Automotive	Containers
Cape Town	1.5 mtpa	1.5 mtpa			1.4 TEU
Durban	1.4 mtpa	1.6 mtpa		520 000 FBUs	3.6 TEU
East London	0.76 mtpa	0.21 mtpa		139 000 FBUs	
Ngqura					2.0 TEU
Port Elizabeth			6 mtpa	158 000 FBUs	0.4 TEU

	Agricultural bulk	Break bulk	Mineral bulk	Automotive	Containers
Richards Bay			28 mtpa		
Saldanha		3.0 mtpa	63 mtpa		

Note: mtpa = million tons per annum; FBUs = fully built-up vehicle; TEU = twenty-foot equivalent unit

Source: TPT (2013a)

Key IT systems for the ports include Navis Sparcs N4, General Cargo Operating System (GCOS), and electronic data interchange (EDI). Navis focuses on the container terminals and was first introduced in 2007 before being implemented at other terminals. Navis provides integration with the rail freight since 2012. There is a single instance of Navis for all terminals (TPT, 2013c). The main function of Navis is to keep track of the cargo containers on vessels and in the yards to allow them to be fetched and moved efficiently, and the system can provide some optimisation of routing and stowing (Navis, 2021). GCOS is developed and supported in-house and focuses on multi-purpose terminals and the automotive terminals. EDI is a common standard method of exchanging computer-to-computer information (TPT, 2013b).

While TPT provides cargo-handling services, Transnet National Port Authority (TNPA) provides navigation and port services, including lighthouses and dredging. The berthing infrastructure at SA ports includes 19 berths servicing containers, 36 dry-bulk berths, 29 break-bulk berths, and 13 liquid-bulk berths (Transnet National Ports Authority [TNPA], 2010).

There is approximately 31 000km of rail track, which translates to approximately 21 000km of rail routes across South Africa (Transnet, 2021b). Key links and commodities transported by rail compared to road freight transportation are illustrated in Table 2. As is evident, other than the Sishen–Saldanha and Ermelo–Richards Bay links, road freight carries more that rail (Department of Transport [DoT], 2017).

Table 2: Comparison of rail and road transportation across key routes

Route	Commodities	Rail (MT)	Road (mt)
Ermelo–Richards Bay	Coal, steel, timber, chrome	78	0
Sishen–Saldanha	Iron ore, lead	62	0
Gauteng–Durban	Containers, steel, cars, coal, manganese, fuels, perishables	24	44
Gauteng–Cape Town	Cars, grains, containers, perishables, cement, steel	11	15
Durban–Pongola	Containers, fuel, chemicals, timber	5.2	7

Route	Commodities	Rail (MT)	Road (mt)
Gauteng–Musina	Foods, fuels, vehicles, cement, perishables, beverages	4.5	12

Note: MT = rail tonne; mt = road tonne

Source: DoT (2017).

Figure 2 below illustrates the major corridors in South Africa, with the major ports indicated as filled circles, and the various corridors indicated by the colouring as per the legend. As is evident, certain ports service specific corridors, with the exception of Richards Bay, which services both the North and North East Corridors. The Cape Corridor is serviced by four ports. In addition to the freight rail, there are the pipelines to transport liquid fuel, primarily between the port of Durban and the economic hub in Gauteng (and some surrounding areas). The pipelines carry refined products, crude oil, gas, and aviation fuel. In 2019 and 2020, the pipelines carried approximately 17 750 million litres, which dropped to 13 067 million litres in 2021 (Transnet, 2021c).

Figure 2: Major commodity corridors in South Africa

Source: Adapted from TFR (2021)

Generally, the freight rail contributes more to the GDP and revenue than the ports for break-bulk and mineral bulk. For liquid fuel, the pipelines are the major contributors, and the port terminals are the major revenue producers for containers (Transnet, 2021a). Even though the major revenue contribution by ports is through containers, they are still vital to be able to export and import other commodities, as their failure could render the railways and pipelines ineffective.

In an international context, South Africa is the world's sixth largest coal-exporting country (Mining Technology, 2020), the top supplier of chromium and manganese, the third largest supplier of Titanium minerals, the sixth largest for iron ore, and one of the major suppliers of a number of other minerals and gemstones (United States Geological Survey [USGS], 2020). This implies that South Africa might become a target of cyber operations should some country wish to disrupt the supply of certain mineral commodities.

Given the overview of the commodities and value chains in general and specific to South Africa, the next section focuses on cybersecurity for physical transport infrastructure.

Cybersecurity of physical transport infrastructure

This section discusses the classification of the physical transportation sector as critical infrastructure nationally and internationally, and reasons for targeting commodity value chains. It also provides an overview of previous notable cyber incidents affecting transportation systems globally.

Physical transportation as critical infrastructure

The US Cybersecurity and Infrastructure Security Agency (CISA) considers the transportation system sector as one of the 16 critical infrastructures, and indicates seven subsectors. Of relevance to this article are the maritime transportation system, the freight rail system, and pipelines (CISA, 2020). Previous works on critical infrastructure protection, such as Ware (1998), Nickolov (2005) and Macaulay (2008) have all considered the transportation sector as critical. Theoharidou, Kandias and Gritzalis (2012) highlight that the transport sector is particularly important for the economy. They further emphasise the interdependencies that exist with other critical infrastructure sectors. The *Australian Security of Critical Infrastructure Act (No. 29 of 2018)* explicitly considers a number of ports as critical, and in subsequent updates, of which the *Security Legislation Amendment (Critical Infrastructure Protection) Act (No. 33 of 2022)* is the latest, explicitly incorporates cybersecurity considerations as well as recognition of interdependencies amongst critical infrastructure.

From an SA perspective, section 16 of the *Critical Infrastructure Protection Act (No. 8 of 2019)* specifies that infrastructure is eligible for declaration as critical if its operation is "essential for the economy, national security, public safety and the continuous provision of basic public services", and if the loss or impairment of the infrastructure will have severe negative consequences for the country, society (in terms of safety and the law), or national security. As described above, the trade of commodities represents over 40% of the GDP; therefore, significant disruptions of the transportation sector will have a severe impact on the ability to trade in these commodities, resulting in negative impacts on the economy.

The *Critical Infrastructure Protection Act*, however, has only one reference to cybersecurity, in that at least one member of a Critical Infrastructure Council should have knowledge of cybersecurity. There is also no specified representative from the Department of Communications and Digital Technologies (DCDT), which has the mandate for the national Cybersecurity Hub (see DCDT, 2020). The National Cybersecurity Policy Framework focuses on critical information infrastructure and the establishment of sector computer security incident response teams (CSIRTs). Said framework called for the establishment of the above-mentioned Cybersecurity Hub as well as a National Cybersecurity Advisory Council (State Security Agency [SSA], 2015). At the time of writing (2022), limited sector CSIRTs have been established, and none for the transportation sector. There is no consideration of the interdependencies of various critical infrastructures in either the Critical Infrastructure Protection Act or the National Cybersecurity Policy Framework. A dated cyber security policy from 2009 however indicates the relevance of cybersecurity to critical information infrastructure, suggesting that the coordination of responses to cyber incidents against critical infrastructure is the mandate of a national CSIRT and a government CSIRT (Department of Communications [DOC], 2009); however, this does not seem to have been retained explicitly by later documents.

Physical transportation and commodity value chains as a target

For the purposes of this article, the focus is on two threat actor types: cybercriminals and nation states. Given the value of cargo and payments being made for physical transportation, cybercriminals have an opportunity to achieve large pay-outs through scams targeting the transportation sector. Ransomware is likely to be the most disruptive. The incident at the SA freight organisation Transnet illustrated the potential impact. This and other examples of incidents are discussed in more detail below.

State actors are motivated by geopolitical reasons, and targeting commodity value chains could be used to gain (or maintain) a competitive advantage in international trade over a commodity (Van Niekerk, 2019). From an international law perspective, targeting a specific terminal or rail line to affect limited commodities will not constitute an act of war, compared to disrupting major power generation or stock exchanges (Van Niekerk & Ramluckan, 2019). The targeting of commodity value chains by cyber operations was specifically proposed by Van Niekerk (2019) as a form of economic information warfare. Traditionally, economic warfare can be conducted through a number of tactics, including blockades, the disruption of supply chains, disrupting supporting infrastructure, or degrading, exploiting or corrupting economic information (Deakin, 2003; Lambert, 2017). As Lambert (2017) notes, almost immediate commodity price fluctuations may occur due to deficiencies or excesses in supply as a result of globalisation. It is therefore feasible for nations to employ a timed cyber operation to affect global supply of a commodity in order to gain a strategic advantage, such as being able to gain market share due to the disruption of a competing nation (Van Niekerk, 2019).

Cyber operations can target various points along a commodity value chain in order to cause disruptions. Focusing on a single point of failure within the commodity value chain will maximise the impact of the cyber operation to disrupt the commodity supply

(Van Niekerk, 2019). For cybercriminals, this will put pressure on the organisation to pay the ransom, and for nation states, this will result in longer recovery times to allow them to benefit from their strategic objectives. To affect a commodity value chain, a cyber operation could target the source (extraction, refinement, or manufacturing of a commodity), the transportation (rail, road, maritime and pipelines), or the human decision-making processes at corporate or national level.

To target the source or transportation, the cyber operations will need to target industrial processes containing cyber-physical systems, such as supervisory control and data acquisition (SCADA) systems. In such a scenario, a cyber incident may affect conveyer belts, gantry cranes, refineries, switching on the railways, sea-going vessels, or other related equipment. Analysis by Van Niekerk (2017) and Van Niekerk and Ramluckan (2019) indicated that – given the number of cyber incidents affecting industrial processes and the transportation sector – it is feasible, although still rare, for cyber operations to cause sufficient physical disruption. With increased digitisation, the Industrial Internet of Things (IIoT) is becoming pervasive and is being introduced into the transport sector (for example, automated ports). The IIoT provides opportunities for organisations to improve operational efficiencies, but also introduces security risks that can be exploited by malicious cyber actors (Pretorius & Van Niekerk, 2020).

In addition to the industrial processes that directly degrade the operational capability of the infrastructure, a cyber incident affecting the supporting enterprise IT infrastructure and decision-making information could cause disruptions in commodity supply. For example, deleting legitimate orders, injecting false orders, or changing order quantities, could not only cause conflict between suppliers and consumers, but could also result in surplus or shortages of supply. Scheduling systems could be corrupted so that insufficient equipment or transportation would be available when needed, or equipment does not undergo required maintenance. Corrupting other business information to alter decision-making or corrupting individuals directly to make poor decisions could also have a long-term degrading effect (Van Niekerk & Ramluckan, 2019). A cyber incident affecting the broader enterprise IT network could potentially achieve several of the above-mentioned consequences by denying executives and operations personnel access to the systems they need to make decisions or conduct daily operations.

The sections below will reflect a discussion on a number of cyber incidents to illustrate the susceptibility and consequences of these incidents in the transportation sector.

Maritime cybersecurity incidents

Of the 51 cyber incidents targeting physical transportation sector analysed by Van Niekerk (2017), 25 affected the maritime subsector, and eight resulted in denial of services or disruption of operations.

Notable incidents affecting port and vessel operations globally include:

- In 2001, a hacker used vulnerable servers in the Port of Houston to conduct a denial-of-service attack, which crashed the servers and disrupted port operations (McCue, 2003).
- In 2009, safety systems on three oil rigs were disabled by a disgruntled employee (Kravets, 2009).
- Royal Navy NavyStar/N* systems aboard warships were infected by the Conficker worm (Kirk, 2009; Page, 2009).
- In 2012, organised crime monitored shipping containers they were using by gaining unauthorised access to cargo systems operated by Australian Customs (CyberKeel, 2014).
- An oil rig navigation system was infected with malware, resulting in it drifting off position (Knox, 2015; Swanbeck, 2015).
- In 2013, smugglers used remote access devices to gain unauthorised access to systems in the Port of Antwerp to monitor their containers (Dunn, 2013).
- In 2014, hackers tilted an oil rig off East Africa, stopping operations for a week, and malware rendered another oil rig unseaworthy for almost three weeks (CyberKeel, 2014; Wagstaff, 2014).
- In 2015, operations at a European port were disrupted for 12 hours due to the GPS signals being jammed (Knox, 2015).
- The NotPetya ransomware worm severely disrupted global operations of Maersk, including affecting port operations. The incident was estimated to have a 300 million dollar impact (Greenberg, 2018).
- It was reported that in 2017, at least 20 vessels experienced potential GPS and AIS spoofing in the Black Sea (Hambling, 2017).
- In 2019, irregular GPS and Automatic Identification System (AIS) readings as well as GPS jamming were reported at the Port of Shanghai (Goward, 2019).
- In 2020, operations at the Shahid Rajaee terminal in Iran were disrupted by a cyberattack, attributed to an Israeli response to an alleged Iranian cyber operation against an Israeli water system (Warrick & Nakashima, 2020).
- In 2021, SA port terminal operations were disrupted by ransomware (Gallagher & Burkhardt, 2021; Ginindza, 2021; Njini & Viljoen, 2021).

Of the 14 incidents described above, seven affected port operations, six affected vessels, and one affected both. Two of these incidents were in Africa, illustrating that the continent is also affected by maritime cybersecurity incidents. In addition to the above, incidents of traditional cybercrime affecting maritime organisations, such as scams, phishing attempts and fraudulent bank account changes were reported. Some instances of cyber espionage were also apparent (Meland et al., 2021; Park, Shi, Zhang, Kontovas & Chang, 2019; Van Niekerk, 2017). There have been additional instances of ransomware impacting on the IT networks of shipping companies and ports; however, these affected corporate services and functionality (including bookings), but not operational systems (Meland et al., 2021; Park et al., 2019). There have been instances of researchers demonstrating possible vulnerabilities in on-board systems, such as the Electronic Chart Display and Information Systems, Voyage Data Recorders and satellite communication, as well as possible attacks, such as spoofing GPS and AIS (Van Niekerk, 2017). Reports of spoofed locations for warships have been reported since 2020 (Harris, 2021).

From the incidents described, it is possible to affect both the systems of the ports to disrupt operations, or to disrupt vessel navigation nearby a port to make navigation hazardous. Berthed vessels could be rendered unseaworthy by malware, thereby blocking berthing places in a port. While this article focuses on a high-level perspective of whether cyber incidents could affect commodity value chains, two incidents are worth a more detailed discussion due to the scale of the disruptions: the NotPetya ransomware affecting Maersk, and the Transnet ransomware incident. For Maersk, the incident disrupted at least 17 terminals across three continents, trucks had to be turned away at the terminals, and cranes were not operational. Systems on board ships were not affected, but the terminals were unable to process the EDI files to determine the cargo that needed to be loaded or unloaded from the vessels. The organisation had to rebuild over 4 000 servers and 45 000 personal computers, including 150 domain controllers, and reinstall 2 500 applications. Luckily, a single domain controller in Ghana survived, as it was offline due to a power outage (Cimpanu, 2018; Greenberg, 2018).

In the Transnet case, the incident occurred with very bad timing. It was a week after major protests had disrupted rail operations, and was also at a key time for exporting citrus fruit (Ash, 2021; Smith, 2021; Toyana, 2021). As with the Maersk incident, it was difficult to track containers in the ports, and some ships opted to reroute elsewhere as the incident continued for a week, and some manual operations and booking were in put in place (Ash, 2021). There were also concerns that employee salaries would not be paid, resulting in threats of employees striking. Combined with the protests, there was an approximately 12-day impact on truck freight (Toyana, 2021).

Rail cybersecurity incidents

Railways are increasingly being affected by cyber incidents, including DDoS (distributed denial of service), data breaches, malware and ransomware (Macola, 2021), and threat actors include both cybercriminals and state actors (Fletcher & Bye, 2022).

- In 2008, tram carriages were derailed in Poland after a teenager had built a device to switch points of the tram lines remotely (Ismail, Sitnikova & Slay, 2015; Leyden, 2008).
- In 2013, train delays resulted from a malware infection at the CSX Corporation, (Miller & Rowe, 2012).
- In 2011, a network intrusion at a United States (US) railway affected signals over two days resulting in train delays (Ragan, 2012; Sternstein, 2012).
- In 2016, a passenger rail service in San Francisco was disrupted for two days as many systems were taken offline as a precautionary measure during a ransomware incident (Fletcher & Bye, 2022).
- A Danish train operator suffered disruptions in 2018 due to a DDoS attack, which prevented the purchase of tickets (Fletcher & Bye, 2022; Hill, 2018).

- In 2022, multiple claims emerged that hacktivists called 'Cyber Partisans' affected Belarussian Railways to delay Russian troop movements; these include ransomware attacks against databases and disrupting its ticketing services (Greenberg, 2022), and affecting traffic control systems (Smeets & Achberger, 2022). This was followed by similar claims from the Anonymous collective (Paganini, 2022).
- A ransomware attack affected ticking systems in Italy in March 2022 (Goodman, 2022).

In addition to interference in the maritime industry, examples of scams, fraudulent changes to bank accounts, ransomware, and cyber espionage are available (Fletcher & Bye, 2022); however, these did not affect operations. In 2016, security researchers demonstrated that railway systems are vulnerable, referring to collision avoidance systems and other control systems that could provide a means for cyber operators to derail trains (Pauli, 2016). Reports in 2022 indicated that railway safety systems are still vulnerable (Zukowski, 2022). While many of these incidents do not specifically involve freight rail, the possibility of remotely affecting signals, switching points, and other controls indicate that disruptions to freight rail are possible.

Pipeline and liquid fuel cybersecurity incidents

Key cyber incidents impact on liquid fuel organisations and pipelines include:

- In 1999, flow control systems at Gazprom were reportedly accessed by attackers using backdoors and with aid of a disgruntled insider (Miller & Rowe, 2012).
- From December 2011 to June 2012, 23 pipeline operators in the United States had operational documentation stolen in an apparent cyber-espionage campaign (Clayton, 2013).
- In 2012, the Saudi Aramco oil company was affected by a 'wiper' malware called Shamoon that corrupted files and computer hard drives to make them unusable. Approximately 30 000 computers were affected, and it took the company two weeks to recover. There were however no indications that industrial systems were directly affected (Bronk & Tikk-Ringas, 2013).
- In 2021, shortly after the Saudi Aramco incident, Qatari RasGas was affected by malware on its corporate network (Mills, 2012).
- In May 2021, Colonial Pipelines (United States) was affected by ransomware. While the pipeline systems were not infected, they were shut-down to prevent infection. The incident resulted in the declaration of a state of emergency by the US president, panic buying of petrol and shortages of aviation fuel (Kerner, 2022).

A notable point in terms of the above incidents is that reports indicate pipeline control systems were accessed remotely, and that the ransomware at Colonial Pipelines did affect operations indirectly, with noticeable social impact in the surrounding areas.

Other relevant cyber incidents

In addition to the cyber incidents described above, a few others are relevant to the discussion in this article:

- malware affected the monitoring of process in an SA chemical plant (Cusimano, 2010);
- the Stuxnet worm affected the control systems, particularly the centrifuges at an Iranian nuclear enrichment facility (Zetter, 2014);
- a cyber incident resulted in an explosion at a German steel mill (Cohen, 2021);
- parts of the Ukraine power grid was shut down by a cyber operations (Greenberg, 2017); and
- a key Israeli toll road was affected by malware (Ashford, 2013).

These incidents indicate that processing facilities that could form part of a value chain, but outside of the transportation infrastructure, are also susceptible to cyber disruption. When a key processing facility is unable to produce the commodity for shipment, then the transportation infrastructure cannot generate revenue for the commodities.

Initiatives and best practices for transportation cybersecurity

Industry and government initiatives internationally have focused on strengthening cybersecurity for physical transportation. In particular, the American Transportation Security Agency (TSA) (2022) released a cybersecurity toolkit for surface transportation in 2021 with a number of guiding documents. A multi-national project in Europe, 4SECURAIL (2022), seeks to develop cybersecurity for the railway sector. The International Maritime Organization (IMO) (2019) provides guidelines for managing cybersecurity within this sector. In 2021, the Atlantic Council's Cyber Statecraft Initiative released a report on maritime security, which considered the lifecycle of ships, key aspects of ports, and the cargo lifecycle (Loomis et al., 2021).

While only a few initiatives have been mentioned, it is important to note that there are dedicated programmes and initiatives addressing the challenges and providing guidance.

Analysing the susceptibility of South African commodity value chains to cyber incidents

This section combines the information in the previous two sections to illustrate possible points of failure within the commodity value chains in South Africa.

In Table 1 above, it was shown that agricultural commodities are primarily handled by Cape Town (50% of capacity) followed closely by Durban. The container sector is mostly handled by Durban with 49% of the handling capacity, followed by Ngqura with 27%. Durban handles the vast majority of the automotive sector with 64% handling of cargo. Saldanha is responsible for the vast majority of the mineral bulk with 65% of capacity and handles the majority of the iron ore. This is followed by Richards Bay with 29%, handling the majority of the coal and servicing two of the major rail corridors. Saldanha handles the majority of break bulk (48%), followed by Durban (24%).

The top two rail routes depicted in Table 2 service coal and iron ore, but do not exhibit any major alternative road transportation. This indicates the considerable impact a failure of those rail routes will have on the respective commodities. The third major rail route,

between Gauteng and Durban, only carries 36% of the cargo and the road carries the majority. In addition, there are two routes between Durban and Danskraal, giving a degree of redundancy. The major ports, rail routes, and their approximate influence on the GDP is illustrated in Table 3 and Figure 2. The word 'influence' is chosen as the railways contribute more than the ports for many mineral and bulk commodities; however, the ports are a major means of exporting, therefore without them the railways will be significantly less effective.

Table 3: Key ports and rail routes for major commodities

Commodity	Key port		Key rail route	Approx. port impact on GDP (%)
	Port	Approx. cargo handled (%)		
Agriculture	Cape Town	50		
Containers	Durban	50	Gauteng–Durban	~6
Automotive	Durban	64		~4.2
Coal	Richards Bay	~100	Ermelo–Richards Bay	3
Iron ore	Saldanha	~100	Sishen–Saldanha	1.5
Liquid fuels	Durban	~100		

Source: Author's own compilation based on data in Tables 1 and 2

From the above, it is evident that the port of Durban is the most critical: it has an impact of at least 10% of the GDP, and dominates the automotive, container and liquid fuel commodities, with meaningful impact on the agricultural and break-bulk commodities. Richard's Bay handles the majority of coal, of which South Africa is sixth highest exporter in the world, and services two major rail routes. It has an impact of approximately 3% of the GDP. Saldanha handles the majority of iron ore (of which SA is the sixth largest producer) and break-bulk, with an impact approximately 1.5% of the GDP. Cape Town handles approximately half the agricultural bulk, which is listed as a key factor in Transnet's economic recovery plan (Transnet, 2021a).

Two systems that are mentioned for SA ports are relevant to the incidents: Navis and EDI. EDI was specifically mentioned in the above example of the NotPetya infection of the Maersk systems. Both the Maersk and Transnet examples indicated that container tracking and moving were hindered by the cyber incidents, which is the function the Navis systems also performs. As indicated above, there is a single instance of the system managing all container terminals across the country. A localised cyber incident could therefore potentially affect the ability of the entire country to manage container shipments. It should be noted that the Navis system itself does not need to be targeted directly, but if the localised network is degraded due to a cyber incident or if the Navis system is taken offline as a precautionary measure (as in the Colonial Pipelines incident), the impact will be the same as when the system is targeted.

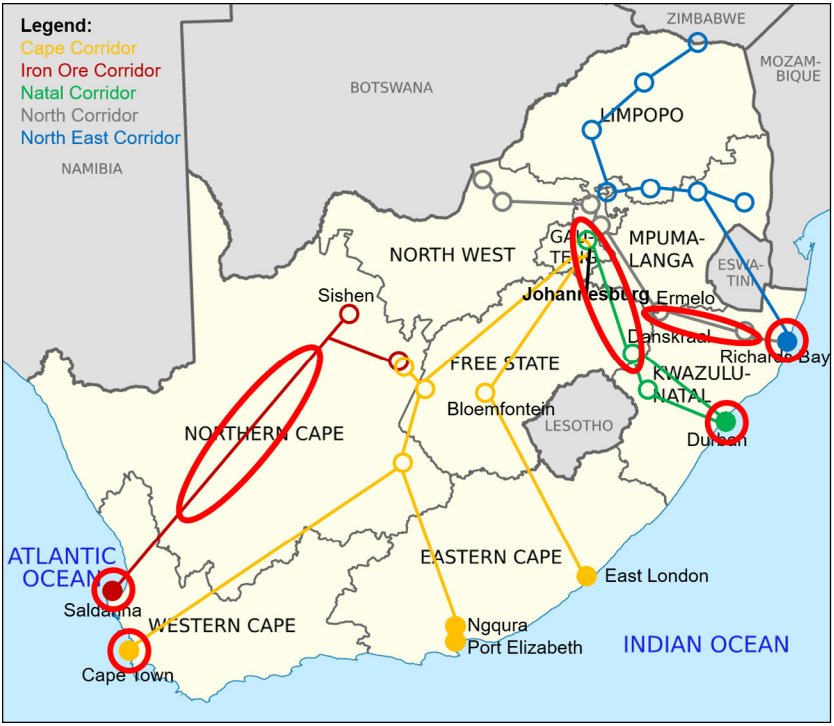


Figure 3: High-level single points of failure in rail and maritime transportation

Source: Adapted from TFR (2021)

Hypothetical examples

To illustrate the potential susceptibility, two hypothetical examples are used: one considering a cybercrime incident and the second, a more targeted state actor scenario. The two scenarios are presented, and then a comparative analysis is provided.

Scenario 1: Cybercrime

For this scenario, an evolution of ransomware attacks, known as a 'triple extortion attack' is considered. Triple extortion uses three methods to maximise the success of forcing the target to pay the ransom, namely ransomware, and the threat of leaking exfiltrated data, enhanced with either DDoS or directly extorting clients or customers based on the exfiltrated data (Snowden, 2021). The scenario will take a worst-case approach to illustrate what is possible. The first stage is the initial infection, which will exfiltrate data and then update to deploy the ransomware. The ransomware affects the servers managing the network, disrupting key services – such as train scheduling, container tracking, and berthing for vessels – resulting in delays as each vessel request needs to be verified. Some

services – such as the website, external EDI with organisations, and booking portals – are at this stage still unaffected. This phase however causes major disruptions for containers vessels and transportation, delays for bulk commodities, and reputation damage for the organisation and nation. The port of Durban was particularly hard hit, being one of the largest terminals, and trucks were backed up on the roads causing discontent and inconvenience for surrounding residents.

The second phase then launches a DDoS attack to hinder the remaining services – such as booking and EDI – further disrupting the ability of the organisation and clients to engage with one another. This causes further reputational damage due to the worsening situation, and the inability to make bookings threatens the future operation of the commodity value chains.

The third phase threatens to release exfiltrated data, initially private to the organisation. Even if the organisation has recovered from the ransomware and DDoS, this phase is still a significant threat. If unsuccessful, extortion attempts against client organisations are attempted, with the potential to release contracting and preferential rate information (if any), or labour brokering information. The release of this information will cause discontent, and clients react strongly against the organisation. The compromise of the data leaks to the media, possibly from one of the clients, triggering an investigation under the national privacy laws. The reputation of the organisation is shattered, eroding international and local confidence in its ability to deliver services and protect customer data. Many shipping organisations will therefore choose to use alternative commodity corridors into the continent.

Scenario 2: State actor

This scenario considers a more targeted and persistent attack focusing on a specific commodity. Nation A has discovered deposits of iron ore and is trying to strengthen its market share for the commodity. To facilitate this, Nation A endeavours to use cyber operations to degrade the ability of competing nations to export iron ore. As South Africa is of similar international standing for providing the commodity, it is one of the countries targeted. The cyber operation is stealthy, and disrupts computers and industrial control systems throughout the iron ore value chain. In particular, power distribution to the mines at Sishen, the port of Saldanha, and the connecting railways are affected. Industrial control systems at the conveyor belts and loading equipment are affected to induce erratic behaviour making the equipment unusable, and, the switching of the tracks are disrupted causing a derailment. The key bottleneck will be the port of Saldanha, as well as its associated rail route. The focus is on disrupting these, where different areas can be affected at different times to create a prolonged effect. This affects the iron ore supply, which in turn affects commodity pricing, allowing Nation A to gain additional market share as well as making it possible for Nation A to sell at a higher price. Once Nation A has established itself as a supplier of iron ore by disrupting South African and other suppliers, the cyber operations cease.

Scenario comparison

The cybercrime scenario gives rise to a broader outcome, which could affect multiple commodities. Here, the goal is to force the organisation into paying, therefore as much pressure as possible will be leveraged: an increase in the number of commodities that are affected translates into more pressure. The implications are far-reaching, particularly in terms of reputational damage of the organisation targeted, and especially for South Africa as a major destination for trade into Africa. This will have both short- and long-term impacts on the national economy and, by extension, on society. By comparison, a state actor will aim to be stealthier and more precise to achieve a specific objective. The reputational damage will be more limited, particularly if multiple nations are targeted. In addition, the cyber operation is likely to be more persistent until the objectives are achieved or the operation can no longer be continued. It is possible that an emerging state actor would use apparent cybercriminal tactics causing more widespread 'collateral' damage, as the tools and/or services can be procured more easily than developing a dedicated in-house process to target specific cyber-physical systems, and using more readily available code will aid in avoiding attribution.

Summary and recommendations

The article has illustrated some critical value chains for which there is limited redundancy, and can be particularly susceptible to disruption via cyber operations. In addition, these routes contribute to the GDP as well as significant proportions of international supply of the commodities. The port of Durban features as a key entry point into the country, and major disruptions of the port could have significant economic consequences for South Africa but could also disrupt global shipping around the continent. The ports of Richards Bay (coal) and Saldanha (iron ore) are also important, along with associated rail routes. The port of Cape Town is important for the growth of the agriculture sector. Two hypothetical scenarios reflecting cybercrime and cyber operations illustrated the potential for disruption of trade corridors in the country. However, while these scenarios are hypothetical, it should be noted that South Africa has already experienced a similar scenario in 2021, and other ports have experienced disruption due to activities in cyberspace.

From the literature it is apparent that, compared to other nations, South Africa does not yet have sufficient formalised structures in place nationally or within the sector to respond to and recover from major cyber incidents, and there appears to be a disjuncture between cybersecurity and critical infrastructure protection. As South Africa is a one of the top suppliers of raw materials and has notable automotive and agricultural sectors, it is imperative that measures be taken to strengthen cybersecurity in the transportation sector. Recommendations for improvement are provided in the section below.

This study was limited to the strategic setting, and consequently did not consider specific technologies or technical vulnerabilities. While the scenarios and discussion focused on South Africa, the high-level premises can be modified to apply to other nations.

Recommendations

Measures to improve cyber resiliency for the freight transportation sector can be implemented or enhanced at national, sectoral and organisational levels. The recommendations considered here were drawn from existing incidents, best practices, and the analysis of the South African (SA) scenario. At a national level, the relevant legislation needs to be reviewed and updated regularly. In particular, cybersecurity needs to feature more prominently in the *Critical Infrastructure Protection Act (8 of 2019)*. In addition, there needs to be greater integration of the National Cyber Security Advisory Council and the Critical Infrastructure Council. A specific agency can be established, similar to the US Cybersecurity and Infrastructure Security Agency.

At a sector level, it is imperative to establish a sector-based computer security incident response team (CSIRT) or a similar facility to aid in responding to incidents and reducing response and recovery time. In addition, the CSIRT could perform other functions, such as distributing alerts, coordinating with other sectors, and facilitating coordination within the physical transport sector. A set of frameworks and standards for cybersecurity best practice within the sector (or for each sub-sector) should be established. Alternatively, existing international frameworks could be adopted formally. In this endeavour, it will be important to engage with international forums and working groups developing cybersecurity best practices for physical transportation. Specialist skills or job profiles for cybersecurity professionals in the sector should be identified, for example industrial control system security.

At an organisational level, there also needs to be engagement with the relevant national and international forums, and particular collaboration with sector cybersecurity functions. Organisations should be responsible for ensuring there is adequate staffing with the necessary general and specialist cybersecurity skills. The specific skill set and job profiles required can be drawn from the sector recommendations. In addition, the organisations should be responsible for conducting strategic and technical risk and vulnerability assessments on their segments of value chains to identify single points of failure and critical assets, and should then implement appropriate security control measures according to sector best practices. It will be important to implement cyber crisis response exercises for organisations to understand their roles in a national cyber crisis, particularly one involving the transport sector.

From an academic perspective, future research could provide more detail on the specific technical vulnerabilities that may be present within the transportation sector, and could consider the level of cybersecurity awareness amongst employees. These future studies could be integrated with the strategic perspective to provide a more holistic view of cybersecurity in the sector.

Conclusion

Cybersecurity threats have affected the physical transport sector, and the maritime sector was hit particularly hard. The current considered the susceptibility of commodity SA supply chains to disruptions from cyber incidents at a strategic level, with the aim of

identifying key areas that may prove to be a single point of failure. SA ports have already experienced a significant cyber incident in 2021; therefore, the feasibility has already been demonstrated. The port of Durban is of particular importance, as it handles close to 50% of container and automotive cargo, as well as a notable percentage of other commodities. The ports of Richards Bay and Saldanha are important for certain bulk commodities, as are the associated rail routes. Cape Town is important for the agricultural sector.

Two hypothetical scenarios illustrated that cybercriminal activity may be more damaging and might affect multiple commodities. Targeted state-backed operations could however limit the effect on specific commodities, but be more persistent in the disruption. It is recommended that national laws be updated to foster good alignment with cybersecurity and critical infrastructure protection. The sector should also engage with relevant forums to implement or adopt best practice frameworks or standards to improve resiliency of the sector.

About the Author

Prof Brett van Niekerk (PhD) is an associate professor in the Department of Information Technology at the Durban University of Technology, a non-resident fellow at the Security Institute for Governance and Leadership in Africa (Stellenbosch University), chairs the International Federation of Information Processing Working Group on ICT in Peace and War, and is Editor-in-Chief of the International Journal of Cyber Warfare and Terrorism. He has cybersecurity experience across industry, academia and civil society. He has actively participated in international cybersecurity forums (Global Commission on the Stability of Cyberspace, Paris Call working groups, Carnegie Endowment for International Peace's project on countering influence operations). He is CISM certified, with over 50 academic publications and 20 presentations at industry events.

References

4SECURAIL. 2022. *Formal methods and CSIRT for the railway sector*. Available at: <https://www.4securail.eu/> [Accessed 15 June 2022].

Ash, P. 2021. Cargo ships give SA a wide berth in wake of cyber attack. *Time Live*, 27 July. Available at: <https://www.timeslive.co.za/news/south-africa/2021-07-27-cargo-ships-give-sa-a-wide-berth-in-wake-of-cyber-attack/> [Accessed 1 June 2022].

Ashford, W. 2013. Cyber attack shuts down Israeli toll road tunnel. *Computer Weekly*, 28 October. Available at: <https://www.computerweekly.com/news/2240207924/Cyber-attack-shuts-down-Israeli-toll-road-tunnel> [Accessed 15 June 2022].

Australian Government. 2018. *Security of Critical Infrastructure Act 2018*. Available at: <https://www.legislation.gov.au/Details/C2018A00029/Download> [Accessed 25 May 2022].

Australian Government. 2022. *Security Legislation Amendment (Critical Infrastructure Protection) Act 2022.* Available at: <https://www.legislation.gov.au/Details/C2022A00033> [Accessed 25 May 2022].

Britannica. 2023. *Anonymous*. Britannica. Available at: <https://www.britannica.com/topic/Anonymous-hacking-group> [Accessed 30 November 2023].

Bronk, C. & Tikk-Ringas, E. 2013. The cyber attack on Saudi Aramco. *Survival*, 55(2), 81–96.

Carman, N. 2023. The use of labour brokers. Labour Guide. Available at <https://labourguide.co.za/general/the-use-of-labour-brokers> [Accessed 30 November 2023].

Cimpanu, C. 2018. *Maersk reinstalled 45,000 PCs and 4,000 servers to recover from NotPetya attack.* BleepingComputer. Available at: <https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack> [Accessed 7 September 2018].

CISA (Cybersecurity and Infrastructure Security Agency). 2020. *Transportation systems sector*. Available at: <https://www.cisa.gov/transportation-systems-sector> [Accessed 24 May 2022].

Clayton, M. 2013. *Exclusive: Cyberattack leaves natural gas pipelines vulnerable to sabotage*. The Christian Science Monitor. Available at: <https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage> [Accessed 3 June 2022].

Cohen, G. 2021. *Throwback attack: A cyberattack causes physical damage at a German steel mill*. Industrial Cybersecurity Pulse. Available at: <https://www.industrialcybersecuritypulse.com/throwback-attack-a-cyberattack-causes-physical-damage-at-a-german-steel-mill/> [Accessed 16 June 2022].

Cusimano, J. 2010. DCS virus infection, investigation and response: A case study. Presentation to Industrial Control Systems Joint Working Group (ICSJWG) Fall Conference, 25–28 October, Seattle, WA.

CyberKeel. 2014. *Maritime cyber-risks: Virtual pirates at large on the cyber seas*. Available at: <http://www.cyberkeel.com/images/pdf-files/Whitepaper.pdf> [Accessed 2 November 2016].

DCDT (Department of Communications and Digital Technologies). 2020. *Cybersecurity Hub Project.* Available at: <https://www.dcdt.gov.za/cybersecurity-hub-project.html> [Accessed 25 May 2022].

Deakin, R.L. 2003. Economic information warfare: Analysis of the relationship between the protection of financial information infrastructure and Australia's national security. Unpublished MA dissertation, Queensland University of Technology.

DOC (Department of Communications). 2009. *Cybersecurity Policy of South Africa*. Available at: <https://www.ellipsis.co.za/wp-content/uploads/2011/02/CYBER-SECURITY-POLICY-draft.pdf> [Accessed 26 September 2022].

DoT (Department of Transport). 2017. *Chapter 7: Freight transport*. Available at: <https://www.transport.gov.za/documents/11623/39906/7_FreightTransport2017.pdf/a3f7cb55-8d77-4eea-b665-4c896c95a0d8> [Accessed 20 May 2022].

Dunn, J.E. 2013. Hackers planted remote devices to smuggle drugs through Antwerp port, Europol reveals. *Techworld*, 16 October. Available at: <http://news.techworld.com/security/3474018/hackers-planted-remote-devices-to-smuggledrugs-through-antwerp-port-europol-reveals/> [Accessed 2 November 2016].

E-International Relations. 2021. Positivism, Post-Positivism and Interpretivism. 25 September. Available at: <https://www.e-ir.info/2021/09/25/positivism-post-positivism-and-interpretivism/> [Accessed 30 November 2023].

Fletcher, D. & Bye, P. 2022. *Cybersecurity in transit systems*. The National Academies Press. Available at: <https://nap.nationalacademies.org/catalog/26475/cybersecurity-in-transit-systems> [Accessed 27 May 2022].

Gallagher, R. & Burkhardt, P. 2021. 'Death Kitty' ransomware linked to South African port attack. *Bloomberg*, 29 July. Available at: <https://www.bloomberg.com/news/articles/2021-07-29/-death-kitty-ransomware-linked-to-attack-on-south-african-ports> [Accessed 3 January 2022].

Ginindza, B. 2021. Transnet 'cyber attack' causes logistics logjam from road to freight and ports. *IOL*, 23 July. Available at: <https://www.iol.co.za/business-report/economy/transnet-cyber-attack-causes-logistics-logjam-from-road-to-freight-and-ports-56f6bd97-c5ef-4d65-90d6-c41d0fe290e2> [Accessed 17 May 2022].

Goodman, M. 2022. Italian railways attacked by ransomware: Ticket sales stopped. *Research Snipers*, 24 March. Available at: <https://researchsnipers.com/italian-railways-attacked-by-ransomware-ticket-sales-stopped/> [Accessed 28 March 2022].

Goward, D. 2019. GPS jamming and spoofing reported at port of Shanghai. *The Maritime Executive*, 13 August. Available at: <https://www.maritime-executive.com/editorials/gps-jamming-and-spoofing-at-port-of-shanghai> [Accessed 27 May 2022].

Greenberg, A. 2017. How an entire nation became Russia's test lab for cyberwar. *Wired*, 20 June. Available at: <https://www.wired.com/story/russian-hackers-attack-ukraine/> [Accessed 15 June 2022].

Greenberg, A. 2018. The untold story of NotPetya, the most devastating cyberattack in history. *Wired*, 22 August. Available at: <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/> [Accessed 27 May 2022].

Greenberg, A. 2022. Why the Belarus railways hack marks a first for ransomware. *Wired*, 25 January. Available at: <https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/> [Accessed 27 May 2022].

Hambling, D. 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon. *New Scientist*, 10 August. Available at: <https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon/> [Accessed 27 May 2022].

Harris, M. 2021. Phantom warships are courting chaos in conflict zones. *Wired*, 29 July. Available at: <https://www.wired.com/story/fake-warships-ais-signals-russia-crimea/> [Accessed 27 May 2022].

Hill, M. 2018. Danish railway company DSB suffers DDoS attack. *Infosecurity Magazine*, 14 May. Available at: <https://www.infosecurity-magazine.com/news/danish-railway-ddos-attack/> [Accessed 27 May 2022].

IMO (International Maritime Organization). 2019. *Maritime cyber risk*. Available at: <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> [Accessed 15 June 2022].

Ismail, S., Sitnikova, E. & Slay, J. 2015. SCADA systems cyber security for critical infrastructures: Case studies in the transport sector. In *Proceedings of the 10th International Conference on Cyber Warfare and Security (ICCWS 2015).* Reading: ACPI, 425–433.

Kerner, S.M. 2022. Colonial pipeline hack explained: Everything you need to know. *TechTarget*, 26 April. Available at: <https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know> [Accessed 2 June 2022].

Kirk, J. 2009. Virus attacks Ministry of Defence. *CIO*, 19 January. Available at: http://www.cio.co.uk/news/3460/virus-attacks-ministry-of-defence/> [Accessed 19 October 2010].

Knox, J. 2015. *Coast guard commandant on cyber in the maritime domain*. US Coast Guard. Available at: <https://mariners.coastguard.blog/2015/06/15/6152015-coast-guard-commandant-on-cyber-in-the-maritime-domain/> [Accessed 27 May 2022].

Kravets, D. 2009. Feds: Hacker disabled offshore oil platforms' leak detection system. *Wired*, 18 March. Available at: <https://www.wired.com/2009/03/feds-hacker-dis/> [Accessed 27 May 2022].

Lambert, N.A. 2017. Brits-Krieg: The strategy of economic warfare. In G. Perkovich & A.E. Levite (eds.). *Understanding cyber conflict: 14 analogies.* Washington, DC: Georgetown University Press, 123–146.

Leyden, J. 2008. Polish teen derails tram after hacking train network. *The Register*, 11 January. Available at: <http://www.theregister.co.uk/2008/01/11/tram_hack/> [Accessed 27 May 2022].

Loomis, W., Singh, V.V., Kessler, G.C. & Bellenkens, X. 2021. *Raising the colours: Signalling for cooperation on maritime cybersecurity.* Washington, DC: Atlantic Council.

Macaulay, T. 2008. *Critical infrastructure*. Boca Raton, FL: CRC Press.

Macola, I.G. 2021. Is cybersecurity in rail more important now than ever? *Railway Technology*, 29 April. Available at: <https://www.railway-technology.com/analysis/is-cybersecurity-rail-important-now-ever/> [Accessed 27 May 2022].

McCue, A. 2003. 'Revenge' hack downed US port systems. *ZDNet*, 7 October. <http://www.zdnet.com/article/revenge-hack-downed-us-port-systems/> [Accessed 27 May 2022].

Meland, P.H., Bernsmed, K., Wille, E., Rodseth, O.J. & Nesheim, D.A. 2021. A retrospective analysis of maritime cyber security incidents. *TransNav: The International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3), 519–530.

Miller, B. & Rowe, D.C. 2012. A survey of SCADA and critical infrastructure incidents. Paper presented at the ACM Special Interest Group on Information Technology Education (SIGITE) Research in IT Conference, 11–13 October, Alberta.

Mills, E. 2012. Virus knocks out computers at Qatari gas firm RasGas. *CNET*, 30 August. Available at: <https://www.cnet.com/news/privacy/virus-knocks-out-computers-at-qatari-gas-firm-rasgas/> [Accessed 3 June 2022].

Mining Technology. 2020. *Coal giants: The world's biggest coal producing countries*. Available at: <https://www.mining-technology.com/analysis/featurecoal-giants-the-worlds-biggest-coal-producing-countries-4186363/> [Accessed 31 May 2022].

Moore, M.R. 2018. Exploring critical infrastructure single point of failure analysis (SPFA) for data center risk and change management. Unpublished PhD dissertation, Northcentral University.

NAVIS. 2021. *N4 Terminal Operating System*. Available at: <https://www.navis.com/en/products/terminal-operations/n4-terminal-operating-system#> [Accessed 26 September 2022].

Nickolov, E. 2005. Critical information infrastructure protection: Analysis, evaluation and expectations. *Information and Security*, 17:105–119.

Njini, F. & Viljoen, J. 2021. Transnet declares force majeure at SA ports over cyberattack. *News24*, 27 July. Available at: <https://www.news24.com/fin24/companies/transnet-declares-force-majeure-at-sa-ports-over-cyber-attack-20210727> [Accessed 17 May 2022].

Paganini, P. 2022. The anonymous hacker collective claims to have breached the Belarusian railway's data-processing network. *Security Affairs*, 27 February. Available at: <https://securityaffairs.co/wordpress/128486/hacktivism/anonymous-breached-belarusian-railways.html> [Accessed 18 March 2022].

Page, L. 2009. MoD networks still malware-plagued after two weeks. *The Register*, 20 January. Available at: <https://www.theregister.com/2009/01/20/mod_malware_still_going_strong> [Accessed 27 May 2022].

Park, C., Shi, W., Zhang, W., Kontovas, C. & Chang, C. 2019. Cybersecurity in the maritime industry: A literature review. In *Proceedings of the International Association of Maritime Universities (IAMU) Conference.* Tokyo: IAMU, 79–86.

Pauli, D. 2016. Irked train hackers talk derailment flaws, drop SCADA password list. *The Register*, 4 January. Available at: <http://www.theregister.co.uk/2016/01/04/irked_train_hackers_talk_derailment_flaws_drop_scada_password_list/> [Accessed 27 May 2022].

Porter, M.E. & Millar, V.E. 1985. How information gives you competitive advantage. *Harvard Business Review*, July. Available at: <https://hbr.org/1985/07/how-information-gives-you-competitive-advantage> [Accessed 10 September 2018].

Pretorius, B.H. & Van Niekerk, B. 2020. Industrial Internet of Things security for the transportation infrastructure. *Journal of Information Warfare*, 19(3), 50–67.

Ragan, S. 2012. Railway network disrupted after cyber attack, report says. *Security Week*, 25 January. Available at: <http://www.securityweek.com/railway-network-disruptedafter-cyber-attack-report-says> [Accessed 2 November 2016].

RSA (Republic of South Africa). 2019. *Critical Infrastructure Protection Act 2019*. Available at: <https://www.gov.za/sites/default/files/gcis_document/201911/4286628-11act8of2019criticalinfraprotectact.pdf> [Accessed 25 May 2022].

Smeets, M. & Achberger, B. 2022. Cyber hacktivists are busy undermining Putin's invasion. *The Washington Post*, 13 May. Available at: <https://www.washingtonpost.com/politics/2022/05/13/cyber-attack-hack-russia-putin-ukraine-belarus/> [Accessed 27 May 2022].

Smith, C. 2021. SA ports in crisis as Transnet cyberattack creates 'total nightmare' for exporters. *Fin24*, 28 July. Available at: <https://www.news24.com/fin24/companies/sa-ports-in-crisis-as-transnet-cyberattack-creates-total-nightmare-for-exporters-20210728> [Accessed 1 June 2022].

Snowden, N. 2021. *Triple extortion ransomware: A new challenge for defenders*. MORPHISEC. Available at: <https://blog.morphisec.com/triple-extortion-ransomware-a-new-challenge-for-defenders> [Accessed 10 June 2022].

SSA (State Security Agency). 2015. National Cybersecurity Policy Framework. *Government Gazette*, 39475. Available at: <https://www.gov.za/sites/default/files/gcis_document/201512/39475gon609.pdf> [Accessed 25 May 2022].

Sternstein, A. 2012. *Hackers manipulated railway computers, TSA memo says*. NextGov. Available at: <http://www.nextgov.com/cybersecurity/2012/01/hackers-manipulated-railway-computers-tsa-memo-says/50498/> [Accessed 27 May 2022].

Swanbeck, S. 2015. *Coast guard commandant addresses cybersecurity vulnerabilities on offshore oil rigs.* Center for Strategic and International Studies. Available at: <https://www.csis.org/blogs/strategic-technologies-blog/coast-guard-commandant-addresses-cybersecurity-vulnerabilities> [Accessed 27 May 2022].

Theoharidou, M., Kandias, M. & Gritzalis, D. 2011. Securing transportation-critical infrastructures: Trends and perspectives. In C.K. Georgiadis, H. Jahankhani, E. Pimenidis, R. Bashroush & A. Al-Nemrat (eds.). *Global security, safety and sustainability & e-democracy.* Lecture notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Volume 99. Berlin: Springer, 171-178.

Toyana, M. 2021. Transnet cyberattack puts employees' salaries at risk while backlogs at ports mount. *Daily Maverick*, 26 July. Available at: <https://www.dailymaverick.co.za/article/2021-07-26-transnet-cyberattack-puts-employees-salaries-at-risk-while-backlogs-at-ports-mount/> [Accessed 28 July 2021].

Transnet. 2021a. *Annual results announcement for the year ended 31 March 2021*. Available at: <https://www.transnet.net/InvestorRelations/AR2021/2021%20ANNUAL%20RESULTS%20PRESENTATION.pdf> [Accessed 24 May 2022].

Transnet. 2021b. *Transnet Freight Rail 2021.* Available at: <https://www.transnet.net/InvestorRelations/AR2021/Transnet%20Freight%20Rail.pdf> [Accessed 24 May 2022].

Transnet. 2021c. *Transnet Pipelines 2021*. Available at: <https://www.transnet.net/InvestorRelations/AR2021/Pipelines%202021.pdf> [Accessed 24 May 2022].

Transnet National Port Authority. 2010. *Transnet National Port Authority*. Available at: <https://www.transnetnationalportsauthority.net/> [Accessed 3 June 2022].

Transnet Port Terminals. 2013a. *Commodity overview*. Available at: <https://www.transnetportterminals.net/Commodities/Pages/default.aspx> [Accessed 20 May 2022].

Transnet Port Terminals. 2013b. *ICT at Transnet Port Terminals*. Available at: <https://www.transnetportterminals.net/About/Pages/ICT.aspx> [Accessed 20 May 2022].

Transnet Port Terminals. 2013c. *Navis Sparcs N4*. Available at: <https://www.transnetportterminals.net/About/Pages/Navis.aspx> [Accessed 20 May 2022].

TSA (Transportation Security Agency). 2022. *Surface Transportation Cybersecurity Toolkit*. Available at: <https://www.tsa.gov/for-industry/surface-transportation-cybersecurity-toolkit> [Accessed 15 June 2022].

UNCTAD (United Nations Conference on Trade and Development). 2018. *Maritime trade and Africa*. Available at: <https://unctad.org/press-material/maritime-trade-and-africa> [Accessed 17 May 2022].

UNCTAD (United Nations Conference on Trade and Development). 2021. Review of Maritime Transport 2021. Available at: https://unctad.org/publication/review-maritime-transport-2021> [Accessed 30 November 2023].

USGS (United States Geological Survey). 2020. *Mineral commodity summaries 2020*. Available at: <https://pubs.usgs.gov/periodicals/mcs2020/mcs2020.pdf> [Accessed 31 May 2022].

Van Niekerk, B. 2017. Analysis of cyber-attacks against the transportation sector. In M.E. Korstanje (ed.). *Threat mitigation and detection of cyber warfare and terrorism activities.* Hershey, PA: IGI-Global, 68–91.

Van Niekerk, B. & Ramluckan, T. 2019. Economic information warfare: Feasibility and legal considerations for cyber-operations targeting commodity value chains. *Journal of Information Warfare*, 18(2), 31–48.

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-idUSBREA3M20820140424> [Accessed 27 May 2022].

Ware, W.H. 1998. *The cyber posture of the national information infrastructure*. Santa Monica, CA: RAND Institute.

Warrick, J. & Nakashima, E. 2020. Officials: Israel linked to a disruptive cyberattack on Iranian port facility. *The Washington Post*, 18 May. Available at: <https://www.washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html> [Accessed 27 May 2022].

Zetter, K. 2014. *Countdown to Zero Day: Stuxnet and the launch of the world's first digital weapon*. New York, NY: Crown.

Zukowski, D. 2022. Rail transit vulnerable to cyberattacks, experts say. *Cybersecurity Dive*, 23 February. Available at: <https://www.cybersecuritydive.com/news/rail-transit-cyberattacks/619123/> [Accessed 2 June 2022].

Scientia Militaria
2023, VOL. 51, NO. 3, 187-190
DOI: 10.5787/51-3-1431

Book Review

Fighting the Fleet: Operational Art and Modern Fleet Combat

Jeffery R Cares & Anthony Cowden

Annapolis: Naval Institute Press
2021, 189 pages
ISBN: 978-1-682477274

The foreword to *Fighting the fleet* by Adm. Scott Swift (USN retd) dwells very appropriately on the great power and peer-related competitiveness of China and Russia. Very aptly, considering the current Russo–Ukraine war, Adm. Swift describes Russia as less of a competitor and more of a spoiler. This fact is now cast in stone by the actions of Russia in the 2022 war with Ukraine. However, Adm. Swift categorises Russia as being innovative and agile (based on evidence from the Russo–Georgian war, the 2014 conflict with Ukraine, and the Russian adventures in Syria). This characterisation is eroded each day the Russo–Ukraine (2022) war is progressing. Russia currently does not display any ability to execute joint warfare doctrine (e.g. concentration of fire and manoeuvre warfare). Russia also does not seem to understand the criticality of logistics and supply-chain management. Adm. Swift points out that Russia does not have the diplomatic, informational, military and economic power to assert itself internationally. This statement is currently showcased on a grand scale in Ukraine.

Accurately and with great brevity, Adm. Swift describes the contribution of the book as critical to the understanding of operational art that is calibrated by "the science of applying kinetic effects"[1] – the art of warfare. This is combined with more "subjective elements of the art of war, such as variabilities of weather, logistics, system functionality, readiness, training quality and quantity, and human decision making".[2] Reading (even studying) this book contributes to an understanding of the art of naval warfare, and will therefore assist in understanding the current demise of Russia in the Ukraine as well as the significance of the Chinese naval expansion and pre-positioning in the Asian Pacific.

In a final comment on context by Adm. Swift, he states that this book is about operational art in the maritime domain, which provides the bridging mechanism between tactical actions and strategic effects in recognising that the "the sum of tactical successes would never result in an equation of strategic success"[3] without artful operations and scientific understanding.

1 JR Cares & A Cowden. *Fighting the fleet*. Annapolis, MD: Naval Institute Press, 2021, p. xii.
2 *Ibid*, p. xii.
3 JR Cares & A Cowden. *Fighting the fleet*, p. xv.

Fighting the fleet is a precise narrative about the art of naval warfare and the science that supports such combat through a US naval warfare dominance lens. The book informs and challenges current perspectives of operational art with the intent to change the strategic outcomes and provide critical links between tactics and operational and strategic effects. More importantly, the authors make a distinction between operational art and naval operational art defining it as "what admirals do"[4] as opposed to what generals do. With this said, the book positions itself as a thought-provoking narrative about the requirement for joint warfare from two perspectives – the traditional land warfare perspective, and the nuances of such perspectives that makes naval warfare joint and combined by its very nature.

This book might have arrived on our bookshelves just in time. The authors state, "[t]hankfully, it has been many decades since this knowledge [technical and mathematical equations about naval salvos] has been needed"[5] – referring to the absence of grand-scale kinetic naval engagements at sea for decades. The current international security dynamics driven by the imperialism of Russia and China could very soon break this trend, rendering this book a must-read for naval combat officers.

A fundamental wisdom shared by Adm. Fiske during the early 1900s – which might remain unread by those reading this book, as it is part of the introduction – is that he foresaw that naval warfare was spiralling towards untold levels of complexity, which would insist on "deep intellectual commitment in peacetime because failure to do so would leave us wishing we were smarter when war came again".[6] Many nations, including the South African Navy (SAN), should reflect very critically on the implications of these wise words whilst the international maritime security in the Indian Ocean has the potential to be contested kinetically very soon based on current challenges to world order.

Jeffery Cares and Anthony Cowden achieve with relatively simplistic comparative analysis informative perspectives on the immense advantages of having both maritime and naval power. They point out and discuss the advantages of (albeit) developed world naval power as a joint and combined force (carrier battle group configurations) enabling expeditionary force projection over vast distances in a day with the ability to engage kinetically any foe in its way. Neither the army nor the air force contributes this level of force projection, thus informing the concept of 'admiralship'.

Combining interesting snippets of the historical development of naval power, the authors expertly build the puzzle with pieces that describe the importance and place of buoyancy, throw weight, pulsepower interaction, and how these inform salvo theory. The book is not short on mathematical equations that ground these constructs and theories, making

4 *Ibid*., p. 4.

5 *Ibid*.

6 *Ibid*., p. 6.

S Fellman. "Ukraine's sinking of the Russian flagship Moskva is a 'wake-up call' for the world's top navies". *Business Insider.* 24 April 2022. < https://www.businessinsider.com/?ir=t/russia-moskva-sinking-wake-up-call-for-navies-experts-say-2022-4> [Accessed on 17 May 2022].

this an excellent book to include as compulsory reading for any naval officer. It should also be included in general warfare programmes to ensure that all future generals and admirals have the same understanding of the attributes of naval power and how it could be employed to multiply the delivery of land and air power within a specific theatre or multitude of theatres. The recent sinking of the Russian Black Sea fleet flagship *Moskva* is an excellent (almost real-time) example of how pulse fire impacted the Russian Naval Power in the Black Sea during the 2022 Russo–Ukraine war.[7]

The book is a must-read for naval officers even if his or her specific navy is not even close to the league of those kept buoyant by the Great Powers because the theory can be scaled down to fit size and complexity levels. It also provides an important guide to General Staff that would inform their analysis of the situation before providing decision-making knowledge to those responsible for international relations and at tables of diplomacy. Asymmetric warfare and hybrid applications of available warfare materiel are therefore important spoilers to conventional theories. *Fighting the fleet* is divided into five chapters that address complexities and practical suggestions on naval power, search and surveillance, logistics and manoeuvre, control, with an end perspective of robotics and fighting fleets.

Commander Jeffrey R Cares[8] and Captain (retd.) Anthony Cowden[9] drew on rich experiences from extensive careers within the US Navy as Reserve Officers. Jeffrey R Cares specialises in "Information Age Warfare, distribute control in military operation, and Network Centric Warfare, […] Antiair Warfare Technical and Operational Expert as well as [being] an Antisubmarine Warfare Operational Expert".[10] Other areas of excellence and leadership include being the co-founder of Newport Center for Information Age Warfare Studies and being recognised by "Cap Gemini Ernst & Young as one of the top 'Innovators and Thought Leaders' of the Information Age".[11]

Anthony Cowden is a history graduate (University of Michigan) with master's degrees in science (University of New Haven) and in national security (Naval War College). He is a US Naval Reserve Captain and co-author of the US Navy *Naval Institute Almanac*.[12] He retired from active naval service during 2021 with 37 years of service.

Dries Putter
Stellenbosch University

7 *Ibid*.

8 New England Complex Systems Institute. "Jeffrey R. Cares". < https://necsi.edu/jeffrey-r-cares> [Accessed on 19 May 2022].

9 US Naval Institute. "Anthony Cowden". <https://www.usni.org/people/anthony-cowden> [Accessed on 19 May 2022].

10 New England Complex Systems Institute *op cit*.

11 *Ibid*.

12 US Naval Institute *op cit*.

Scientia Militaria
2023, VOL. 51, NO. 3, 191-194
DOI: 10.5787/51-3-1432

Book Review

The Naval War in South African Waters, 1939–1945

Evert Kleynhans

Stellenbosch: African Sun Media
2022, viii + 315 pages
ISBN 089-1-991201-74-4 (paperback); 978-1-991201-75-1 (e-book)

On 6 September 1939, the then Union of South Africa, under its new Prime Minister, General Jan Smuts, declared war against Nazi Germany. Similar declarations of war would later follow against Italy (11 June 1940) and Japan (8 December 1941). The Union Defence Force (UDF) was soon transformed into a formidable fighting force, with the Army deployed to fight in East Africa, in Madagascar, in North Africa, and eventually also in Italy, supported by aircraft of the South African Air Force (SAAF). SAAF squadrons also saw action in other war zones. The country's naval forces, established in 1922 as the South African Naval Service (SANS), had to be built up from scratch, because the three small SANS ships were withdrawn from service in 1933–1934, and when the Second World War broke out, the SANS only had a handful of staff – and, obviously, no ships.

Far removed from the main European, North African and Pacific war zones, South Africa was spared direct land and air attacks, as well as the concomitant destruction and civilian casualties, but in light of the strategic value of the Cape sea route, the war soon came nearer to South African shores. The SANS officially became the Seaward Defence Force (SDF) on 1 September 1939, albeit that in practice it only started to operate as such from 15 January 1940. On 1 August 1942, the SDF and the Royal Naval Volunteer Reserve (South Africa Division) amalgamated to form the South African Naval Forces (SANF). Several years later, on 1 January 1951, the SANF was renamed the South African Navy. In the course of the Second World War, the SDF, and later the SANF, operated in four operational areas, namely the South African coastal waters, the Mediterranean, the Atlantic Ocean and the North Sea, and (in the last months of the war) in the Far East. Most of the 88 South African World War II warships were small trawlers or whalers that were converted into minesweepers or anti-submarine vessels.

With the publication of Evert Kleynhans's *The naval war in South African waters 1939–1945*, extensive coverage is now at least given to the African local operational area. Previously, operations in South African waters were dealt with by LCF Turner *et al*. in *War in the southern oceans 1939–1945* (1961), by CJ Harris in *War at sea: South African maritime operations during World War II* (1991), and by HR Gordon-Cumming in the *Official history of the South African naval forces during the Second Word War (1939–1945*) (2008). For chapters on the role of South African naval forces in the war, and for the history of the South African naval forces in general, there are, for example, the books by JC Goosen (compiler), *South Africa's navy: The first fifty years* (1973),

Chris Bennett and Arnè Söderlund, *South Africa's navy: A navy of the people and for the people* (2008), and two books by André Wessels, *Suid-Afrika se vlootmagte 1922–2012* (2017) and *A century of South African naval history: The South African Navy and its predecessors 1922–2022* (2022).

Based on comprehensive and solid archival research (see the source list, pp. 292–315, and the 675 endnotes), Kleynhans's excellent latest book provides a critical and an in-depth analysis of the naval war off the South African coast and in the adjacent oceans during the Second World War. After discussing the strategic context of the naval war in South African waters, providing a literature review, and discussing his methodology in the elaborate introduction to his book, Kleynhans indicates the strategic importance of South African waters in Chapter one. Chapter two deals with the South African coastal defence system in the years 1933–1945. This includes the establishment of radar stations, air patrols, anti-submarine operations, and minesweeping. Opportunistic Axis naval attacks are scrutinised in Chapter three, including the role played by German pocket battleships and other surface raiders, and mine-laying operations, as well as the limited Japanese submarine offensive in the Mozambique Channel in 1942. "The German U-boat operations, 1942-1945" is the title of Chapter four. In this period, a total of 105 merchant ships were sunk by the German submarines, as well as five by an Italian submarine, the *Leonardo da Vinci*.

Kleynhans devotes two chapters to the naval intelligence war. In Chapter five, early wartime contacts are discussed, including the role of Will and Marietjie Radley as wartime couriers, and Hans Rooseboom as secret agent for the Germans. In the next chapter, the Felix Organisation is discussed in detail, with particular reference to the role played by Lothar Sittig. Throughout Chapters five and six, the role of the Ossewabrandwag is referred to. "The naval counterintelligence war" is the title of Chapter seven. This includes wireless interception, security, and naval censorship. These chapters on intelligence and counterintelligence matters are of particular importance, and the author succeeded admirably in integrating these issues with the broader topic of naval warfare in South African waters. The anti-submarine war, 1942–1945, is discussed in Chapter eight, including the sinking of three Axis submarines in South African waters.

In his conclusion, Kleynhans correctly points out that his book "provides a critical, comprehensive analysis of the all-encompassing naval war waged in South African waters between 1939 and 1945. In doing so, it introduces a fresh, in-depth discussion of the topic" (p. 286), and indeed, "[t]he book is novel in that it provides a unique analysis of the Axis and Allied naval operations in South African waters during the war" (p. 290).

The naval war in South African waters 1939–1945 is based on Kleynhans's doctoral dissertation, "The Axis and Allied maritime operations around Southern Africa, 1939–1945", which he completed in 2018 at Stellenbosch University. The published version is Volume four in the *African Military Studies* series. The book reflects a solid academic study, and the target audience is in the first place specialists and peers, as well as serious students in the field of military (and in particular naval) history. However, the book

is written in such a way that anyone interested in the topic will find it of value. The publication contains 22 informative tables, 15 maps, four figures and six graphs, as well as 20 apt photographs. Unfortunately, there is no index.

South Africa is supposed to be a maritime nation. Regrettably, too many South Africans, from all cultural groups, suffer from what could be termed 'a land rat mentality', and from sea blindness. The strategic Cape sea route has always been one of the world's most important maritime choke points. The importance of the Cape sea route was, once again, emphasised in the course of the Second World War. The safeguarding of this sea route was indeed of crucial importance for the Allied strategy and war effort. This is one of the many important matters that come to the fore in *The naval war in South African waters 1939–1945*, in which Evert Kleynhans makes an invaluable contribution towards the South African military – and in particular naval – historiography. This excellent scholarly publication is highly recommended. Hopefully, it will stimulate debate and generate more interest in the South African naval history.

André Wessels
University of the Free State

Scientia Militaria
2023, VOL. 51, NO. 3, 195-198
DOI: 10.5787/51-3-1433

Book Review

President Mandela's Admiral: The South African Navy's Story of the 1990s: Challenging Politics, Radical Transformation, Ambitious Voyages and the Quest for New Ships and Submarines

Robert C Simpson-Anderson

Muizenberg: Naval Heritage Trust
2021, 196 pages
ISBN 978-0-620-94594-3 (softcover)

The 1st of April 2022 marked the centenary of the South African Navy. Compared to other dominion navies, the early history of the Navy remains complex and often contested in terms of its lineage and date(s) of establishment. The 'hundred years of the Navy' include the establishment of the SA Naval Service in 1922, the formation of the Seaward Defence Force in 1939, its amalgamation with the South African division of the Royal Naval Volunteer Reserve in 1942 to establish the SA Naval Forces (SANF), the constitution of the SANF after the war in 1946 as a permanent component of the Union Defence Force, its ultimate renaming in 1951 to the South African Navy, and finally, its rebirth in 1994 as part of the democratic South African National Defence Force (SANDF), as we know it today.[1]

With the above in mind, South African naval historiography shows a varied range of coverage, themes and focus, but autobiographies and biographies do not feature prominently, even though this form of writing has long been a respected source for historical inquiry.[2] The absence of biographical works that feature the careers of our naval flag officers is most notable. South African military leaders have written about themselves. Rudolph Hiemstra,[3] Magnus Malan,[4] Constand Viljoen,[5] Jannie Geldenhuys[6] and George Meiring[7] have all added their voices after retirement, but the most prominent

1 See A du Toit. "A navy for the nation". *Naval Digest* 33 (2022), pp. 1-165; A Wessels. *A century of South African naval history: The South African Navy and its predecessors 1922–2022*. Gansbaai: Naledi, 2022.

2 See B Caine. *Biography and history*. London: Bloomsbury, 2018.

3 R Hiemstra. *Die wilde haf*. Cape Town: Human & Rousseau, 2001.

4 M Malan. *My life with the SA Defence Force*: Pretoria: Pretoria Boekhuis, 2006.

5 D Cruywagen. *Brothers in war and peace: Constand and Abraham Viljoen and the rebirth of the new South Africa.* Cape Town: Penguin Random House, 2014.

6 J Geldenhuys. *Ons was daar: Wenners van die oorlog om Suider-Afrika.* Pretoria: Kraal, 2011.

7 G Meiring. *Soldaat en mens.* Pretoria: STN Printers, 2020.

South African naval figure, Hugo Biermann,[8] is conspicuously absent from the list. The important work done by the Naval Heritage Trust (NHT) offered some retort in 2003 when a Naval Digest of (only) 35 pages on Biermann's career appeared.[9] Louise Jooste,[10] Roger Boulter[11] and Rodney Warwick[12] offered valuable insight, but a dedicated biography about the life and times of Admiral HH Biermann (1913–2003) would indeed make a welcome addition to South African naval historiography.

In the light of the Biermann anomaly, the publication of *President Mandela's Admiral* therefore comes as a welcome surprise and is a gem in our naval historiography. The author was no Biermann, but nevertheless widely regarded to be the 'right man at the right time'. Vice-Admiral Robert Simpson-Anderson served as chief of the Navy between 1992 and 2000 – a time that can be regarded as one of the most significant in South African history. The book is however more than just an autobiography about Simpson-Anderson's naval career; it is a history of the South African Navy of the 1990s. In fact, only half a page in the preface is dedicated to his own curriculum vitae and thereafter the work is devoid of any focus on the 30-year naval career that led up to his appointment as chief of the Navy on 1 September 1992.

In Chapter one, Simpson-Anderson acknowledges that his appointment – less than two years after his promotion to rear admiral – came as a complete surprise. His predecessor, the popular Vice-Admiral Lambert 'Woody' Woodburne had retired early, after only two years as chief of the Navy.[13] Simpson-Anderson inherited a navy that had transitioned from its traditional blue-water design of the 1960s to one that had to adapt to the broader national (total) strategy, mostly in support of South African Defence Force operations during the 1980s. The Navy had been hard hit by the long-term effects of arms embargoes and was still reeling following the retrenchment of 22% of its personnel in 1990 at the conclusion of the Border War.

---

8 Biermann served as chief of the Navy for an unprecedented 19 years and remains the only naval flag officer to serve as CSADF. The Naval Heritage Trust has similarly published short biographies of SAN flag officers in their series of Naval Digests (ND). See, for example, ND no. 32 – R Adm CH Bennett; ND no. 29 – Cmdre EW Jupp; ND no. 20 – Cmdre AC McMurray; ND no. 17 – Cmdre B Hogg; ND no. 13 – Cmdre J Dalgleish; ND no. 10 – R Adm MR Terry-Lloyd; ND no. 7 – Cmdre RP Dryden Dymond. (For a complete list of Naval Digests, see < https://navalheritagetrust.co.za/digests/>.)

9 R Williams. "Admiral H.H. Biermann". *Naval Digest* 9 (2003), pp. 1-35.

10 L Jooste. "FC Erasmus as Minister van Verdediging, 1948–1959". MA thesis. University of South Africa, 1995.

11 RS Boulter. "FC Erasmus and the politics of South African Defence 1948–1959". PhD dissertation. Rhodes University, 1997.

12 R Warwick. "White South Africa and defence, 1960–1968: Militarization, threat perceptions, and counter strategies". PhD dissertation. University of Cape Town, 2009.

13 The preceding 15 years (1977–1992) saw the appointment of no less than six different chiefs of the Navy. They were JC Walters (1977–1980), RA Edwards (1980–1982), AP Putter (1982–1985), G Syndercombe (1985–1989), AP Putter (1989–1990) and L Woodburne (1990–1992). This stood in stark contrast to the continuity that was offered by the appointments of HH Biermann (1952–1972) and J Johnson (1972–1977).

Simpson-Anderson's appointment as chief of the Navy came eighteen months after FW de Klerk's landmark speech at a time when negotiations for a new political order were gaining momentum. Chapter two offers insightful reading into the first 'behind the scenes' talks with senior members of Umkhonto we Sizwe. The Navy took the initiative to meet with Joe Modise and Ronnie Kasrils before their respective appointments as Minister of Defence and Deputy Minister of Defence. This early initiative was aimed to introduce the future political leaders to the Navy and to ensure "a mutual agreement that South Africa needed a capable navy and that political support would be needed to ensure [its] survival as an important arm of the Defence Force".[14] Forging good relationships with the new Ministry of Defence paid off handsomely in the long run, and Kasrils developed a liking and a "passion for the Navy's case".[15]

After 1990 and in stark contrast to many years of isolation, the world literally opened up to South Africa. The Navy took on an important role to fly the new South African flag in foreign ports, in operational, diplomatic, humanitarian roles, and often in support of other state departments. During the course of his eight years at the helm, Simpson-Anderson paid official visits to nineteen countries to re-establish naval partnerships. In Chapter three, he proudly shares the numerous accolades and compliments bestowed on the Navy after such visits abroad.

One of the greatest public events ever put together by the Navy is recounted in Chapter seven. Simpson-Anderson had assembled a talented team of flag officers and Navy personnel that organised a memorable Navy 75 anniversary in April 1997. The Navy hosted an International Fleet Review on 5 April 1997 in which no fewer than 22 foreign warships from 13 countries participated. President Nelson Mandela, the commander-in-chief, was present on 5 April 1997 to take the salute at the fleet review, alongside Simpson-Anderson on board the review vessel SAS *Protea*. The president clearly enjoyed the event, and the amicable relationship that developed between himself and the chief of the Navy was of great future importance to the Navy. President Mandela provided vital support to the Navy in the long and drawn-out process to re-equip its fleet. Simpson-Anderson later admitted that "had we not had his backing it is quite possible that the eventual renewal of the Navy's combat fleet would not have materialised".[16]

The most appealing aspect of this book is the view the reader gets 'from behind the scenes' or should one say 'from behind C Navy's desk'. The author admits:

The book is a record of my experiences, good and bad, happy and unhappy, during my term of office, and I dare not skip unpleasant incidents lest the impression I left that my story deals with the sunny days of my term of office only.[17]

---

14 R Simpson-Anderson. *President Mandela's admiral: The South African Navy's story of the 1990s*. Muizenberg: Naval Heritage Trust, 2020, 9.

15 R Kasrils. *Armed and dangerous: From undercover struggle to freedom*. Auckland Park: Jacana Media, 2013, 295.

16 Simpson-Anderson *op. cit.*, p. 160.

17 *Ibid.*, p. 95.

Simpson-Anderson dedicates Chapter nine to a number of more 'amusing incidents' reflecting on the lighter side of his term of office, but in Chapter ten also sombrely reflects on the tragic events that had to be dealt with.

The catchy title of the book and Simpson-Anderson's claim that he was "President Mandela's Admiral" is revealed in Chapter eight (p. 166). Here he describes, in the most humble terms, how it happened in 1995 that he was accorded the honorary title by President Mandela himself "through circumstances well beyond my control".[18]

Simpson-Anderson blames (or thanks) his wife Geesje for being the main impetus to write his story. She had devotedly compiled no fewer than twenty-five scrapbooks filled with newspaper cuttings, reports and photographs of her husband from 1992 to 2000. He makes it clear that the book was written to be readable and enjoyable. It is therefore devoid of statistics, dates, fine detail or even references. The glossy book is adequately complemented by good quality colour photos, illustrations, extracts from speeches, letters, signals as well as a list of acronyms and abbreviations. *President Mandela's Admiral* is an insightful and revealing read from start to finish, and is highly recommended. The book is a welcome addition and reference to an important era in our naval history.

Leon Steyn
South African Naval Museum

[18] *Ibid.*, p. 159.

Scientia Militaria
2023, VOL. 51, NO. 3, 199-202
DOI: 10.5787/51-3-1434

Book Review

A Century of South African Naval History: The South African Navy and its Predecessors, 1922–2022

André Wessels

South Kensington: Naledi
2022, 496 pages
ISBN 9781928530978 (Paperback)

This year marks the centenary of the establishment of a small, nascent, permanent naval service in South Africa, to which the modern South African Navy, which serves all the people of a vibrant, democratic South Africa, owes its direct ancestry.

To commemorate this significant milestone, Professor André Wessels has produced his latest book, *A century of South African naval history*, which was launched at the South African Naval Museum in Simon's Town on 31 March 2022. Professor Wessels is a senior professor emeritus and a research fellow in the department of history at the University of the Free State in Bloemfontein. The history of the South African Navy and its predecessors is one of his main research focus areas, and he has published extensively on the subject over many years.

While the SA Navy is neither one of the oldest nor one of the major navies in the world, it does, however, have a fascinating and proud, albeit chequered history serving the nation and its people. And while there are several books on the history of the SA Navy and its fighting ships, including those of this reviewer, this impressive new book provides a timeous, comprehensive and up-to-date history of the SA Navy and its predecessors over the 100 years of its existence.

This new work by André Wessels builds on the author's 2017 Afrikaans book, *Suid-Afrika se vlootmagte 1922–2012* and, understandably, there is overlap between the two publications. His latest book is, however, not merely an English translation of his previous work. In this new book, based on more than four decades of research and writing, Wessels adopts a fresh approach to both content and presentation, with much additional material and historical and political context to provide a more comprehensive review of the rich history of the SA Navy. He also updates the history of the SA Navy since 2012, which was the cut-off date for the author's 2017 publication. Importantly, in addition to recognising its many operational achievements, this book provides considerable insights into the all-important diplomatic role fulfilled by the SA Navy throughout its existence. The book concludes with some perspectives on 100 years of naval developments in South Africa.

The history of SA Navy ships has also been incorporated into a single chronological narrative, rather than being dealt with by ship type in separate chapters. This has prevented repetition and greatly improved the flow of this new publication. Moreover, while the 2017 book only provided a broad history of the South African naval forces from 1922 to the establishment of a permanent post-war navy in 1946, two new chapters are now dedicated to this important formative period.

Wessels contends that, in the first century of its existence, the South African naval forces have, on several occasions, undergone a process of transformation, and have grown and contracted depending on the whims of government, the vagaries of the economy, and the perceptions of the largely 'sea blind' nation.

With the global predominance of British maritime power and the long-standing presence of a squadron at the Cape, which safeguarded South African shores and protected trade and sea communications, no South African government after unification of the four South African colonies in 1910 showed much interest in South Africa as a maritime nation. Moreover, with South African maritime defence largely in the hands of the Royal Navy – which could be counted on to maintain a substantial presence in South African waters – there was, despite the establishment of a small, short-lived permanent naval service in 1922, a distinct lack of interest by politicians and the predominantly army hierarchy in having a navy at all. This situation would repeat itself during the late 1970s and throughout the 1980s.

Almost thirty years after the Union, and just five years after the disposal of the last vessels of the fledgling South African Naval Service (SANS) during the Great Depression (1929–1939), the outbreak of war in 1939 provided the necessary impetus for South Africa to finally embark on the voyage of establishing a permanent, credible and enduring navy for the nation.

The SANS became the Seaward Defence Force (SDF) in January 1940, which in turn, was transformed in 1942 when it amalgamated with the South African Division of the Royal Navy Volunteer Reserve to become the South African Naval Forces (SANF). Under the leadership of the South African wartime Prime Minister, General Jan Smuts, the Union Defence Force was expanded considerably, including its naval forces.

While the end of the Second World War saw the Navy established as a full-time, albeit much reduced service, it remained the 'Cinderella' service until the mid-1950s, by which time it had been renamed the South African Navy in 1951. The transfer of the Simon's Town Naval Base to the South African government in 1957 and the commissioning of many new ships under the terms of the 1955 Anglo–South African Simon's Town Agreement for the Cold War defence of the sea routes round the Cape, led to the unprecedented expansion of the fleet and the professionalisation of the service, culminating in the successful establishment of a submarine squadron in the late 1960s.

The impact the growing international isolation of South Africa due to its apartheid policies had on the Navy is analysed together with the years of almost total isolation from 1977 to 1979, during which time the SA Navy entered the missile age but largely lost its blue

water capabilities and increasingly became involved in supporting regional clandestine special forces operations. Wessels then discusses the opportunities that the new political dispensation had on the SA Navy after 1990. He contends that, while en route to a new South Africa, the SA Navy took full advantage of the opportunities presented to it to build a new, transformed navy, for a new South Africa.

Looking to the future, Wessels argues that, in accordance with the core business of the modern SA Navy, 'to fight at sea', its mission 'to win at sea', and its vision 'to be unchallenged at sea', it is of the utmost importance for South Africa to have a well-equipped, well-balanced, well-trained and disciplined navy. He argues that what has been achieved since 1994 has been built on the solid work done over many decades, and that the centenary of the Navy is an opportunity for all South Africans to reflect on the proud history of the SA Navy, to take stock of the present state of the Navy, and to look to the future, clearly understanding that South Africa is a maritime nation.

Professor Wessels should be congratulated on producing a very comprehensive, readable and up-to-date history of the SA Navy and its predecessors over the 100 years of its existence.

Allan du Toit
University of New South Wales

Scientia Militaria
2023, VOL. 51, NO. 3, 203-206
DOI: 10.5787/51-3-1435

Book Review

Die Affäre Patzig: Ein Kriegsverbrechen für das Kaiserreich?

Ulrich van der Heyden

Kiel: Solivagus Praeteritum
2021, 239 pages
ISBN 978-3-947064-06-9

Van der Heyden's *The Patzig affair. A war crime for the empire?* is a richly illustrated study of the case of U-boat commandant Helmut Patzig, whose U-86 torpedoed the British hospital ship, *Llandovery Castle,* on 27 June 1918.

U-boats were stealth weapons, and therefore of a dubious reputation. They could launch surprise attacks without being spotted, only to disappear quickly again after a successful kill. Submarine warfare therefore occurred in an ethically grey area that many contemporaries viewed with disdain, akin to another terrifying invention used in the Great War, namely poison gas. When the British naval blockade began to upset the German economy, the Germans declared in February 1915 that they would retaliate by conducting unrestricted submarine warfare around the British Isles. This resulted not only in serious losses of tonnage, which threatened to disrupt Britain's own economic lifeline, but also in German attacks on neutral vessels on the mere suspicion that they might transport military supplies. The torpedoing of the ocean liner *Lusitania* by a German U-boat on 7 May 1915 killed nearly 1 200 passengers, which confirmed the image of Germany as a ruthless belligerent that ignored the rules of 'civilised' warfare. The further escalation of submarine warfare in 1916 saw attacks on foreign vessels in British waters without any warning. These assaults were brought to a halt temporarily because American citizens were among the victims. At that stage, the German military leadership was concerned not to provoke the United States into entering the war. These endeavours of scaling tactics back to less jarring practices were short-lived, however, and in February 1917, Germany officially returned to unrestricted submarine warfare. The United States entered the war in April 1917 against the background of an increasingly pugnacious mood amongst the American public that was incited partly by the indiscriminate U-boat attacks. The decision to return to a more rules-based form of submarine warfare in October 1918 came too late to change Allied perceptions of entrenched German malice. More importantly, German U-boats proved to be powerless to prevent the arrival of American 'dough boys' on the Western battlefields, which precipitated the final defeat of the *Kaiserreich*.

Patzig's ruthless actions against the British hospital ship, which was placed in the service of the Canadian forces, may be viewed in the context of an increasingly desperate mood in the German navy. The rules of 'civilised' combat – as much as all governments promised to respect them in peacetime – had been eroded quickly after the shooting

started. The merciless German strategy failed to release the stranglehold of the blockade, but accelerated the spiral of violence, also leading to incidents of coldblooded killing of survivors of destroyed German submarines. The last year of the war saw an unprecedented loss of 90 German submarines due to combat, mines, accidents and scuttling by their own crews.[1]

Oberleutnant zur See Helmut Patzig was a decorated officer with a record of many missions in the North Atlantic when he sank the *Llandovery Castle* off the southern Irish coast. The ship was on its return voyage from Halifax to where it had transported wounded soldiers. On board were crew members and medical personnel of which 234 died, including 14 Canadian nursing sisters. The officers of the U-boat later claimed that they had reason to believe that the *Llandovery Castle* transported soldiers and military supplies. After the initial interrogation of the surviving captain of the hospital ship, Patzig must have realised that the sinking could not be justified in military terms (pp. 64–65). What made Patzig's actions even more conspicuous among war-time atrocities, however, was that he later returned to the scene to finish off the surviving witnesses of his actions. He had his crew fire on the victims and, in addition, he tried to ram the only lifeboat that managed to escape with 24 survivors on board. Patzig then falsified his logbook to erase any evidence that his U-boat had been present in the area of the attack.

After the war, the German authorities at first responded quite disinterestedly to questions from the British by claiming their ignorance about the event (pp. 84–85). In the face of the political and economic turmoil in post-war Germany, the Allied powers hesitated to fan the flames of nationalist discontent by handing over war crime cases to British courts. The 'stab in the back' legend was adopted enthusiastically by large parts of the political elites and the public, and the Allies wanted to avoid the impression of meting out unilateral victor's justice. When the British government did not desist from their investigation, however, a case was opened at the Leipzig Supreme Court in 1921. Patzig went underground without ever having to face up to his crime. Only two of his officers, who turned out to be uncooperative witnesses, were found guilty, which unleashed a wave of nationalist resentment in Germany. They received short prison sentences, but were sprung from jail a little later with the help of members of right-wing militias. The arrest warrant for Patzig was cancelled in 1926 in the course of a wider amnesty for soldiers accused of war crimes, which was supported by parties across the political spectrum of the Weimar Republic (pp. 143–146).

Patzig apparently managed to return to civilian life once the danger of extradition to the British had passed, at first under the name of his wife. He joined the Nazi Party in November 1933. In 1937, he was appointed lieutenant commander (*Kapitänleutnant*) of the reserve, to be promoted to corvette captain in 1939, and to frigate captain in 1944. He died in West Germany in 1984 (pp. 178–183).

---

[1] See uboat.net. "U-boat fates: U-boat losses 1914–1918". 2022. <https://www.uboat.net/wwi/fates/losses.html> [Accessed on 20 March 2022].

The author, whose forte is a prolific output on South African colonial history and missionary studies, has succeeded in contributing a detailed account of the sinking of the *Llandovery Castle* and its political repercussions in Germany to the existing literature on this event. As he explains, this study was motivated by his discovery of a link between the event and his own family history. The *Gefechtsrudergänger*, a term that could be translated as combat steersman, on Patzig's U-boat was an ancestor of the author. This crew member was a witness to the atrocity, but never dared to step into the limelight as a witness. As the author convincingly points out, the fierce nationalism and right-wing culture prevalent during the Weimar period and then again in Nazi Germany hardly encouraged the presentation of a truthful account of Patzig's attack on the hospital ship and the subsequent murder of the survivors. The story of the torpedoing of the *Llandovery Castle* became a tale that was passed down in hushed tones over several generations in the author's family. It is not clear, however, why Van der Heyden decided merely to hint at the identity of this crew member who died in 1970. Whether the combat steersman was the author's grandfather or granduncle remains the reader's guess, but the last part of the book somewhat meanders through a complex narrative of the repercussions of this event for his family history during the Second World War and its aftermath. The author has chosen to tell this story in the voice of the objective historian, but some readers may regret that the author has thrown a semi-transparent veil of secrecy over the after-effects of the traumatic events on his own family. Despite these quibbles, however, this accessible publication will be welcomed, not only by historians, but also by a wider readership. The dramatisation of the fate of the *Llandovery Castle* in the form of an opera, which has recently been staged in Canada, is a reminder that the memory of this horrible event is still alive.[2]

Tilman Dedering
University of South Africa

[2] The Llandovery Castle. N.d. <https://www.llandoverycastle.ca/> [Accessed on 20 March 2022].

SCIENTIA MILITARIA
South African Journal of Military Studies

NOTES TO CONTRIBUTORS

Scientia Militaria is published bi-annually by the Faculty of Military Science (Military Academy), Stellenbosch University. It is an accredited, scholarly journal, which investigates a broad spectrum of matters and issues relating to military affairs, and publishes both discipline-based and inter-disciplinary research. In order to ensure that articles are of a high quality, all submissions are refereed (peer-reviewed) by at least two experts in the field. Refereeing is done with complete anonymity and confidentiality. Articles published in *Scientia Militaria* qualify for a subsidy from the South African Department of Education.

- To speed up the review process, it is recommended that authors submit an electronic copy to the editors. It is also possible to submit manuscripts in printed form.
- The length of papers should be between 7 000–10 000 words, including footnotes, schedules and reference lists.
- A written guarantee that the manuscript has not been submitted to other publications is required.
- All papers must be language-edited by a language practitioner.
- Please see the *General Guidelines for Contributors* for the preferred reference technique. Research containing no references will not be considered.
- Where maps, figures and graphs are presented, they must be professionally produced and ready for photographic reproduction.
- The final decision concerning the publication of papers lies with a subcommittee of the editorial committee. No correspondence will be carried on in this respect.
- Copyright on all published material in *Scientia Militaria* rests with the Faculty of Military Science of Stellenbosch University.
- Authors submitting papers, which originally formed part of dissertations or theses, should consult with their study leaders/promoters prior to submission.
- Opinions expressed in the Journal, or conclusions made, are those of the author(s) alone and do not imply endorsement on the part of the editors.
- The assessment of submissions takes time, and authors are requested not to make enquiries before a period of at least four months has elapsed.

Editorial addresses

Scientia Militaria
Private Bag X2
Saldanha 7395
South Africa

Prof. E.P. Kleynhans
kleynhans@sun.ac.za
Tel: +27-22-702-3102
Fax: +27-22-702-3060

SCIENTIA MILITARIA

South African Journal of Military Studies