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.

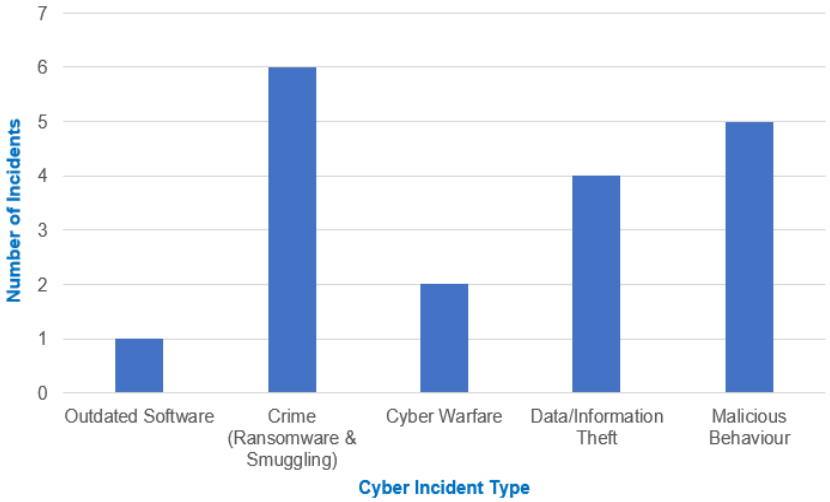

Figure 1: Maritime cyber incidents reviewed for period 2011–2020

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.