UNIVERSITY OF CAPE TOWN - FACULTY OF LAW

NAME : SAMKELISIWE CECELIA NTULI

STUDENT NO: NTLSAM006

SUPERVISOR: PROFESSOR GRAHAM BRADFIELD

QUALIFICATION: LLM SHIPPING LAW

SUBMISSION DATE: 28 JULY 2023

STEAMING TOWARDS A CYBER SECURE SHIPBOARD NAVIGATION SYSTEMS: A REVIEW OF INDUSTRY READINESS

Acknowledgements

I am grateful to my family and friends for their support during this time. They have been there for me through thick and thin, and I could not have done this without their support.

I would like to express my deepest gratitude to Professor G. Bradfield, for his guidance and support throughout this project, providing me with feedback, advice, and encouragement. I am truly grateful for his dedication and expertise.

Above it all, I thank God for seeing me through it all.

TABLE OF CONTENTS

CHAPTER 1 INTRODUCTION

I Aim of the dissertation

The overall aim of this dissertation is to review the industry's state of readiness in the fight against cybersecurity breaches onboard ships. Concurrently, the goal of this dissertation is to identify the key challenges and gaps in cyber security preparedness and propose recommendations for improving cyber security in shipboard navigation systems.

II Thesis

It will be argued that the maritime industry's state of readiness in the fight against shipboard cybersecurity threats is not yet adequate and to reach the state of readiness, the industry cybersecurity rules must be reformed to improve their efficacy, which will necessitate additional engagement from all industry stakeholders.

III Background to the research subject

(a) Maritime security

There are many ways in which one can define the idea of maritime security, Bueger defines maritime security as the safeguarding of a state's land as well as its maritime territories[1]. The author goes on to point out a wide variety of illegal activities that affects maritime security, such as dealing in arms and drugs, trafficking people, engaging in fishing that is illegal, unreported, and unregulated (IUU), polluting the ocean, and, more recently, failing to maintain adequate levels of cyber security. Protecting these vital pieces of infrastructure is, without a shadow of a doubt, of the utmost significance[2]. Due to the fact that we are now living in a new era and must constantly confront new difficulties, it is imperative that we emphasise the significance of this matter.

(b) Importance of safeguarding maritime supply chains against interruption

Transportation trade, in general, is a vital organ for world economic development[3]. Kosowska-Stamirowska considers the maritime industry to be the most critical sector, as it feeds into other supply chains[4]. The author goes on to assert that over 90% of the world trade is shipped by sea,

---

[1] Bueger, Christian 'What is maritime security?' (2015) 53 *Marine Policy* 159 at 160-1, available at *http://www.elsevier.com/locate/marpol*, accessed on 1 February 2022.

[2] Lehto, Martti 'Cyber Security in Aviation, Maritime and Automotive' in Diez, Pedro et al (eds) *Computational Methods in Applied Sciences Computation and Big Data for Transport Digital Innovations in Surface and Air Transport Systems* (2020) Springer Nature 23. available at *http://www.springer.com/series/6899*, accessed on 3 February 2022

[3] Ibid.

[4] Kosowska-Stamirowska, Zuzanna et al. 'Evolving structure of the maritime trade network: evidence from the Lloyd's Shipping Index (1890–2000)' (2016) 1 *Journal of Shipping and Trade* 1, available at *https://jshippingandtrade.springeropen.com/articles/10.1186/s41072-016-0013-3*, accessed on 1 Feb 2022.

because of this, the maritime industry is the pillar of the global economy. The movement of goods is the single, overarching goal of maritime transportation and finding people who need their goods moved and having the capacity to transport those peoples' goods in a secure and effective manner are essential to the company's success[5]. For this goal to be achieved, all systems in the supply chain must operate efficiently with minimum downtime[6].

It is without a doubt that the existence of trade has made a considerable contribution towards the world's economy and sustainability[7].Furthermore, a country or nation can only exist by exchanging resources with other nations to sustain what it lacks. The shipping industry made this possible for decades, connecting countries and forging new nations by navigating beyond charted waters.

(c) Digital reliance

The world has evolved into a digital era, which opens endless possibilities and simplifies processes that used to be tedious, keeping different processes and sectors interconnected[8]. That does have an upside to it. Take, for example, the move from celestial navigation, which had the navigator looking up to the stars to fix the ship's position. Nowadays, that tedious and time-consuming task has been replaced by the GPS (Global Positioning System), RADAR (Radio Detection and Ranging) and ECDIS (Electronic Chart Display Information and System), thereby freeing the navigator for other pressing matters on the ship and simplifying navigation. However, that simplicity does come at a cost, as it exposes the ship to hacking. In less than a decade, there has been an indication of a significant increase in cyber-attacks in the shipping industry[9].

Before the digital era, trade was isolated and secure from any remote access, whether malicious or not[10]. Nowadays, the ship can be led to the wrong port or led to follow the wrong route through its navigation system without the navigator's knowledge or suspicion[11]. The

---

[5] Bielawski, Antoni & Lazarowska, Agnieszka 'Discussing cybersecurity in maritime transportation' (2022) 4 *Maritime Technology and Research* 1, available at *https://doi.org/10.33175/mtr.2022.252151*, accessed on 7 February 2022.

[6] Ibid.

[7] Ibid.

[8] Meland, P H et al. 'A retrospective analysis of maritime cyber security incidents' (2021) 15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 519, available at *http://www.transnav.eu*, accessed on 7 February 2022.

[9] Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 7-8.

[10] Ibid at 1-3.

[11] King, Justin 'The Story You Aren't Being Told About Iran Capturing Two American Vessels' *MPM News* 2016/1// 2016, available at *https://www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two-american-vessels/212937/*, accessed on 07 February 2022.

impact of this malicious act can be far-reaching in just one attack. Considering the type of ships available in the market these days, each has far more advanced navigation equipment than the last model, with a high level of integration which primarily works independently of the navigator, is continuously connected to the satellites/network, and carries a various cargo of different value and hazard[12]. One needs to imagine what could prevent pirates from re-routing a ship to a pre-determined location to serve their ends and what could prevent a terrorist or activists from gaining access to navigation of a naval vessel, a vessel carrying dangerous cargo or any significant vessel, from disrupting the trade to serve their cause.

(d) Security threats

The industry has battled numerous illegal activities for years; among the predominant ones is piracy. Piracy raged on for years, and it cannot be said that it is vanquished from the seas[13]. Cybersecurity breaches can enhance piracy, terrorism and a mix of criminal activities that need to be curbed before it reaches the same and a possibly higher level of destruction as their predecessors.

(e) Consequences of cybersecurity breaches

It can be safely assumed that allowing more time for this kind of security threat can prove very disruptive and far more costly to the industry and the world economy[14]. The incentive for this crime for entities that profit illegally from the trade cannot be ignored. All it takes for the execution of a cybersecurity attack is a good hacker, a device, and an uninterrupted connection to the network. Even more appealing is that the perpetrator need not be physically on a ship. The breach can be initiated anywhere in the world, protected by anonymity. With this kind of incentive, the illegal activities that the industry is facing could shift to a new platform exerting more pressure on the legal system[15].

For these reasons, it is deemed necessary to raise further awareness of the looming cybersecurity threat onboard ships by outlining cybersecurity risks posed by navigation systems on a modern-day ship's bridge as a typical example and a point of departure. Thereafter, review the industry's readiness status in the fight against cyber security breaches

---

[12] Bolbot, Victor et al. 'A novel cyber-risk assessment method for ship systems' (2020) 131 *Safety Science* 1-2, available at *www.elsevier.com/locate/safety*, accessed on 1 February 2022.

[13] ICC International Maritime Bureau 'Maritime piracy rises again in 2020' 2020 available at *https://www.hdi.global/infocenter/insights/2021/piracy/*, accessed on 6 August 2021.

[14] Kao, M. B 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' (2021) 45 *Tulane Maritime Law Journal* 467 at 472.

[15] Ibid.

by analysing the measures, guidelines, strategies, etc., currently in place against the risk, identifying shortfalls and areas needing reform.

In every field, there is a response to any threats and challenges to the trade to make sure the industry continues to flourish, and the maritime industry is no exception. The IMO (International Maritime Organisations) has passed down guidelines to combat this threat[16], state authorities have raised awareness, such as SAMSA (South African Maritime Safety Authority)[17], industry partners such as BIMCO (Baltic and International Maritime Council) and many more have intervened, raised awareness, trained the crew, and proposed solutions[18]. However, guidelines and recommendations are only worthwhile with implementation and follow-through. Therefore, the need for research and development in cybersecurity cannot be overly emphasised; only a better understanding of the threat can yield effective preventative measures. Notably, cybersecurity differs from any past safety and security issues the industry has encountered. Furthermore, it is continuously advancing with technology and should be expected to counteract all preventative measures put in place; therefore, there is a need for continual research and development on preventative measures to stay ahead of the threat.

---

[16] International Maritime Organisation *Guidelines on maritime cyber security risk management* (2017), available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents*, accessed on 6 December 2021.
[17] SAMSA *Cyber Security* (Marine Notice No 18 of 2017), available at https://*www.samsa.org.za*, accessed on 1 February 2022.
[18] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021), available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

IV Structure

(a) Outline

In broad outline the dissertation, will take as its point of departure a brief overview of the cyber security risks posed by shipboard electronic navigation systems to give context to what is to follow. Thereafter, the response from the industry regulatory bodies, for a broad overview, in the form of industry guidelines and publications currently in place as means of averting or minimising cyber security breaches onboard ships, will be reviewed to ascertain the industry status of readiness by measuring such guidelines or measures against the possible risks and demonstrate possible shortfalls and need for reform.

(b) Chapter 2: Shipboard electronic navigation systems

This chapter consist of 3 parts, dealing with the electronic navigation systems typically found onboard ships.

(i) Operation of shipboard electronic navigation systems

This part gives a brief description of what electronic navigation systems are and how they operate. This is to provide a better understanding of the context and serve as the basis for the vulnerability assessment.

(ii) Cybersecurity risk assessment of shipboard electronic navigation systems

This part focuses on the cybersecurity vulnerabilities posed by electronic navigation systems onboard and illustrate the severity of these risks by briefly touching on the reported shipboard cyber breaches where these systems were used as the gateway to illegal interception. This is to justify the need for conducting a review of industry readiness.

(iii) Cybersecurity risk measures for shipboard electronic navigation systems

This part discusses possible countermeasures for cybersecurity risk management. This serves as the basis for the industry cyber risk management review to provide the reader with an understanding of what is needed to reach the point of readiness against cybersecurity attacks.

(c) Chapter 3: Maritime Industry cybersecurity risk management review

This section deals with the maritime industry’s measures and guidelines currently in place to respond to cyber security threats and evaluate these measures by comparing them with the proposed measures. This is to provide a clear picture of what is currently implemented and what is lacking.

(d) Chapter 4: Review results

This chapter discusses the review's outcome, highlighting shortfalls, if any, and identifying areas needing reform. Thereafter, providing the answer to the research question.

(e) Chapter 5: Electronic banking systems

This chapter consist of 3 parts providing a brief overview of electronic banking systems in use.

(i) Comparisons with electronic banking systems operation

This part gives a brief description of what electronic banking systems are and how they operate. This is to illustrate similarities between the two systems and establish grounds for benchmarking the two sectors.

(ii) Cyber security vulnerability and management of electronic banking system

This part of the dissertation focuses on the cybersecurity vulnerabilities of electronic banking systems and illustrate how attackers gain access to these systems. This is to show similarities in the vulnerabilities, and the attack strategies on both systems, thereby justifying benchmarking.

(iii) Cyber security management strategies of electronic banking systems

This part deals with measures used by the finance sector in safeguarding against cybersecurity breaches in electronic banking systems. Concurrently, evaluating if such measures could be suited for use onboard ships or improved upon for adoption onboard ships.

(f) Chapter 6: Maritime industry state of readiness in relation to Banking sector state of readiness

This chapter compares the state of readiness of the maritime industry to deal with cyber security breaches to that of the banking sector. Following that, offer suggestions on what the maritime industry might use to improve its cybersecurity measures for shipboard electronic navigation systems by drawing measures deployed by the banking sector.

(g) Chapter 7: Conclusion

This chapter sums up the arguments raised by this study and address the aim of the study introduced in the first chapter. Thereby concluding the findings concerning the industry's readiness status in the fight against shipboard navigation systems cyber security risks.

CHAPTER 2 SHIPBOARD ELECTRONIC NAVIGATION SYSTEMS

I Introduction

On board, a modern vessel, various pieces of equipment are designed to assist a navigator in navigating the vessel safely. This equipment together forms a system that assists the navigator in determining the ship's position, course, speed, and depth under the keel, developing dangerous situations with other vessels and objects, etc.

Electronic navigation systems have revolutionised navigation principles by simplifying complicated and tedious tasks while reducing human error in navigation. Gone are the days when restricted visibility used to be the enemy of the trade, forcing vessels to anchor or remain adrift until it was clear to navigate.

The following equipment will be assessed: Automatic Identification System (AIS), Global Positioning System (GPS), Radio Detection and Ranging (RADAR), Electronic Chart Display and Information Systems (ECDIS), as a sample to show satellite, radio waves, network connectivity and integration cybersecurity vulnerabilities.

II Operation of shipboard electronic navigation systems

(a) AIS

(i) What is it?

AIS is an automated system that transmits a ship's identification, position, course, speed, and other information used to avoid collisions and improve maritime safety to other ships or coast stations in the vicinity[19]. This is a broadcast transponder system that transmits signals in the VHF mobile maritime band[20]. It uses two VHF channels, 161.975 MHz - channel 87B (Simplex, for the ship to ship) and 162.025 MHz - channel 88B (Duplex for the ship to shore)[21], which are monitored autonomously and continuously using the (S)TDMA (Self-Organising Time Division Multiple Access) technologies[22]. This technology allows AIS to transmit a minimum of 2,000 messages per minute, which is necessary to meet the high broadcast rate

---

[19] Bhattacharjee, Shilavandra 'What is Automatic Identification System (AIS)- Types and Working (FAQs)' *Marine insight* available at *https://www.marineinsight.com/marine-navigation/automatic-identification-system-ais-integrating-and-identifying-marine-communication-channels/*, accessed on 2 Feb 2023.2023.

[20] Karahalios, Hristos 'Appraisal of a Ship's Cybersecurity efficiency: the case of piracy' (2020) 13 *Transportation Security* 179 at 182, available at *https://doi.org/10.1007/s12198-020-00223-1*, accessed on 19 July 2022.

[21] Revised Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS) 2015 International *Maritime Organisation* 1 at 17, available at *https://edocs.imo.org/Final Documents/English/A 29-J-62 - RES.1106 (E).doc*, accessed on 2 February 2023.

[22] Ibid.

required for maritime safety[23]. Each AIS station is able to customise its own transmission schedule according to the volume of data link traffic history as well as their knowledge of the upcoming actions of other stations[24].

AIS stations coordinate with each other to avoid transmitting their messages at the same time[25]. They do this by randomly selecting a time slot within a set interval[26]. If a station's schedule changes, it will broadcast the new location and timeout information[27]. This ensures that all stations are able to receive each other's messages, even if they are new or if they suddenly come within range[28].

(ii) How it works?

An Automatic Identification System (AIS) consists of a VHF transmitter, two VHF TDMA receivers, one VHF Digital Selective Calling (DSC) receiver, and a standard marine electronic communications link to shipboard display and sensor systems[29]. The AIS also comes with a built-in GPS receiver, which is used to provide timing information for the SOTDMA protocol. If the external GPS fails, the built-in GPS is used to derive both position and timing information[30].

Other information broadcast by the AIS, such as heading, course and speed over ground, rate of turn, angle of heel, pitch, and roll, is electronically obtained from shipboard equipment through a standard marine integration system[31].

The AIS has three modes of operation which are automatically defined without the user interface[32]. These are: Autonomous and continuous mode: Autonomous and continuous mode: When operating in this mode, the AIS will automatically determine its reporting rate based on

---

[23] Furuno *ClassA AIS Operator's manual* (2015) Japan, Furono Electric Co., LTD. iii, available at *https://www.furunousa.com//media/sites/furuno/document_library/documents/manuals/public_manuals/fa170_operators_manual.pdf*, accessed on 2 February 2023.

[24] Revised Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS) 2015 *International Maritime Organisation* 1 at 17, available at *https://edocs.imo.org/Final Documents/English/A 29-J-62 - RES.1106 (E).doc*, accessed on 2 February 2023.

[25] Gaugel, Tristan et al 'In-depth Analysis and Evaluation of Self-Organizing TDMA' (2013), *IEEE Vehicular Networking Conference* 79 at 80-5, available at *https://ieeexplore.ieee.org/abstract/document/6737593*, accessed on 2 February 2023.

[26] Ibid.

[27] Ibid.

[28] Ibid.

[29] Revised Guidelines for the onboard operational use of shipborne Automatic Identification Systems (AIS) 2015 *International Maritime Organisation* 1 at 15, available at *https://edocs.imo.org/Final Documents/English/A 29-J-62 - RES.1106 (E).doc*, accessed on 2 February 2023.

[30] Ibid.

[31] Ibid.

[32] Furuno *ClassA AIS Operator's manual* (2015) Japan, Furono Electric Co., LTD. iii, available at *https://www.furunousa.com//media/sites/furuno/document_library/documents/manuals/public_manuals/fa170_operators_manual.pdf*, accessed on 2 February 2023.

the navigational mode, speed, and course it is currently following[33]. Polled/Controlled mode: When operating in this mode, the AIS will immediately respond to any interrogation posed by an authorised party through a base station located on land[34]. Assigned/ Controlled Mode: In the Assigned/Controlled Mode, a competent authority in charge of traffic monitoring has the ability to remotely set transmission intervals and time slots for the vessel's mobile stations[35].

(b) GPS

(i) What is it?

GPS, or Global Positioning System, is a satellite-based navigation system that helps ships navigate safely and efficiently; it is one of the most relied-upon aids to navigation, as it saves navigators time in position fixing and integrates with almost all navigation systems onboard a ship to generate other outputs. The official name of GPS is Navigational Satellite Timing and Ranging Global Positioning System (NAVSTAR GPS)[36]. It is a form of Global Navigation Satellite System (GNSS) that the United States Department of Defense (DoD) developed primarily for military use[37]. This system consists of three segments: the space segment (satellite constellation), the control segment (ground monitor and control stations), and the user segment[38].

(ii) How it works?

There are 24 satellites making up the GPS, orbiting Earth at about 20,200 km away; These satellites complete two orbits around the planet every day and send radio waves at low frequencies to Earth stations[39]. GPS receivers take this information and calculate the user's precise location by using a technique called triangulation[40]. The signals contain information about the location of the satellite; the GPS receiver then determines the position of at least three

---

[33] Omholt-Jensen, Kristin & Engnæs, Pål-Robert 'AIS and the main categories of AIS challenges' *Maritime Optima*, available at *https://www.maritimeoptima.com/blogdata/ais-and-the-main-categories-of-ais-challenges*, accessed on 6 February 2023.

[34] Ibid.

[35] Ibid.

[36] Sturdevant, R W 'The navstar global positioning system: From military tool to global utility' (2012) *Down to Earth: Satellite Technologies, Industries, and Cultures* 331, available at *https://www.researchgate.net/publication/283483513_The_navstar_global_positioning_system_From_military_tool_to_global_utility*, accessed on 6 February 2023.

[37] Ibid at 332.

[38] Federal Aviation Administration, USA. *Global Positioning System Wide Area Augmentation System (WAAS) performance standard* (2008) Department of Transportation, USA.1 at 2, available at *http://www.nstb.tc.faa.gov/*, accessed on 6 February 2023.

[39] Revised performance standards for shipborne Global Positioning System (GPS) receiver equipment (2000) *International Maritime Organisation* 1 at 2, available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.112(73).pdf*, accessed on 6 February 2023.

[40] Ibid.

satellites, as well as their distance from it, and then computes the position using triangulation[41]. Therefore, the accuracy of the position received is dependent on a number of factors, including the positions of the satellites in the space segment, the effects of the atmosphere, errors in the satellite clock and ephemeris, etc[42].

(c) RADAR

(i) What is it?

RADAR is officially known as Radio Detection and Ranging, and it is one of the key features in the marine bridge[43]. RADAR assists in safe navigation and collision avoidance by detecting other ships, obstructions and dangers to navigation, navigation objects, and shorelines using radio waves[44].This allows the navigator to assess the situation around the ship and make an informed decision suitable for the prevailing circumstances[45].

(ii) How it works?

The RADAR detects surrounding objects by transmitting short, powerful pulses of electromagnetic energy through the scanner unit several times per second[46]. These pulses travel at the speed of light, and when they strike any object in their path, they are reflected in the scanner as echoes[47].The reflected pulses pass through the receiver, which processes each echo and causes it to show up visually as a bright spot on the display unit screen[48].

From this process, the bearing and the range of the echo can be acquired on demand by the operator. The RADAR is designed to operate in any form of visibility, whether restricted or not, day or night[49].

---

[41] Federal Aviation Administration, USA. *Global Positioning System Wide Area Augmentation System (WAAS) performance standard* (2008) Department of Transportation, USA 1 at. 3-5, available at *http://www.nstb.tc.faa.gov/*, accessed on 6 February 2023.

[42] Ibid at 2-5.

[43] Revised performance standards for RADAR equipment (2004) *International Maritime Organisation,* available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.192(79).pdf*, accessed on 8 February 2023.

[44] Bole, A G et al *Radar and ARPA Manual: Radar and Target Tracking for Professional Mariners, Yachtsmen and Users of Marine Radar* (2005) 1, available at *http://ebookcentral.proquest.com/lib/cput/detail.action?docID=234979*, accessed on 8 February 2023.

[45] International Maritime Organisation 'Convention on the International Regulations for Preventing Collisions at Sea 1972 Rule 7b' *International Maritime Organisation* (2003). available at *https://www.imo.org/en/About/Conventions/Pages/COLREG.aspx*, accessed on 8 February 2023.

[46] Bole, A G et al *Radar and ARPA Manual: Radar and Target Tracking for Professional Mariners, Yachtsmen and Users of Marine Radar* (2005) 27, available at *http://ebookcentral.proquest.com/lib/cput/detail.action?docID=234979*, accessed on 8 February 2023.

[47] Ibid at 29-30.

[48] Ibid.

[49] Revised performance standards for RADAR equipment (2004) *International Maritime Organisation* 1 at 5-7, available at

(d) ECDIS

(i) What is it?

An ECDIS, formally known as an Electronic Chart Display and Information System, is a computer-based navigation system that uses electronic charts to replace paper charts[50]. It is compliant with the standards of the International Maritime Organization (IMO)[51] and displays selected information from a System Electronic Navigational Chart (SENC)[52].

In addition to making navigation safer, ECDIS also reduces the workload of navigators by automating tasks such as route planning, route monitoring, ETA calculation, and ENC updating[53]. This makes the ECDIS one of the most relied-upon navigation aid onboard ships.

(ii) How it works?

The ECDIS combines information from a variety of sources, including GPS, radar, and the echosounder, AIS, etc, to provide navigators with the information they need to safely navigate[54]. ECDIS systems can display two types of charts: raster navigational charts (RNCs) and electronic navigational charts (ENCs)[55].

Raster Navigational Charts are electronic versions of paper charts, they are created by scanning paper charts and do not include any additional data features[56]. This means that ECDIS systems that use RNCs are more limited than those that use electronic navigational charts (ENCs)[57].

---

https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.192(79).pdf, accessed on 8 February 2023.

[50] Revised performance standards for Electronic Chart Display and Information Systems (ECDIS) (2006) *International Maritime Organisation 1 at* 2-3, available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232(82).pdf*, accessed on 6 March 2023.

[51] Revised performance standards for Electronic Chart Display and Information Systems (ECDIS) (2006) *International Maritime Organisation 1 at* 2-3, available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232(82).pdf*, accessed on 6 March 2023.

[52] SOLAS Consolidated Edition Reg. 19 Chapter v (2018) 412,428.

[53] Revised performance standards for Electronic Chart Display and Information Systems (ECDIS) (2006) *International Maritime Organisation* 1 at 2, available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232(82).pdf*, accessed on 6 March 2023.

[54] Ibid at 6.

[55] Ibid at 2-3.

[56] Ibid at 21-5.

[57] Ibid.

An Electronic Navigational Chart are more informative than a Raster Chart [58]. These charts are computer-generated, and each object on the chart can be probed for additional details[59]. As sophisticated as they may be, these charts have limitations. Due to the cost of producing these charts, some regions still need to be covered by vector charts[60].

III Cybersecurity risk assessment of shipboard electronic navigation systems

(a) Introduction

Over the past decade, the world has seen an increased use of electronic gadgets and the Internet in every aspect of life. Experts refer to this as the 4th industrial revolution or digital era. This era comes with innovative technologies which enable big data sharing, 'connecting the physical world to the information world, at a fast pace'[61]. The same innovation has been seen on ships, and the industry has advanced itself in research and development, building ships far more advanced in autonomy, smart functionalities, and connectivity.

Navigation systems used onboard are now dependent on the 'Internet of things', and most systems are interconnected to others. For example, the AIS (Automatic Identification System) feeds into systems like the Radar and ECDIS, making them interdependent. Furthermore, most of the processes done by a navigator onboard are now replaced by automation, removing the human interface. Increasing automation onboard, though beneficial to the trade, however, it also makes ships a target for security breaches[62]. This chapter will outline these vulnerabilities, highlighting instances in which navigation systems listed below have been used as a gateway for cyber security breaches.

The following navigation systems will be outlined as they show both satellite and radio frequency vulnerabilities which is mainly what other navigation systems not mentioned below use as the network connection: Automatic Identification System (AIS), Global Positioning

---

[58] Bhattacharjie, Shilavandra 'What is Electronic Chart Display and Information System (ECDIS)?' *Marine Insight* (2021), available at *https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/*, accessed on 6 March 2023.

[59] Ibid.

[60] Bhattacharjie, Shilavandra 'What is Electronic Chart Display and Information System (ECDIS)?' *Marine Insight* (2021) available at *https://www.marineinsight.com/marine-navigation/what-is-electronic-chart-display-and-information-system-ecdis/*, accessed on 6 March 2023.

[61] Zarzuelo, Ignacio de la Peña 'Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue' (2021) 100 *Transport Policy* 1, available at *http://www.elsevier.com/locate/tranpol*, accessed on 1 February 2022.

[62] Muronga, K et al 'Towards secure maritime transport in South Africa: An investigation of cybersecurity readiness of organisations' (2019) Research space 1, available at https://researchspace.csir.co.za/dspace/bitstream/handle/10204/11176/Muronga_2019.pdf?sequence=1&isAllowed=y, accessed on 6 December 2021.

System (GPS), Radio Detection and Ranging (RADAR) and Electronic Chart Display and Information Systems (ECDIS).

(b) Shipboard navigation systems' cyber vulnerabilities

(i) AIS

a) Background

Having an AIS onboard merchant vessels is a mandatory requirement by the IMO's revised SOLAS chapter 5 in 2004[63]. The AIS proved to be a very useful tool in the industry, not only for ship-to-ship interaction but also for simplifying ship-to-shore interaction by continually transmitting vessel information and allowing continuous tracking of vessels by coast radio stations. However, research has shown that this system's cyber security is outdated and weak, therefore easily susceptible to cybersecurity attacks such as 'disabling AIS communications, tampering with existing AIS data, triggering search and rescue alerts to lure a victim ship into navigating to a hostile and attacker-controlled sea space, or spoofing a collision to possibly bring a ship off course'[64].

(ii) AIS vulnerabilities overview

a) Spoofing

Experts have defined spoofing as the attacker's ability to create a non-existent vessel and furnish it with complete AIS data to mislead the target[65]. This kind of attack has been used in various cases, mainly to 'conceal illegal fishing and other illegal activities' at sea[66]. From case studies, it can be said that AIS spoofing provides the attacker with endless scenarios, some of which may still be unknown, for conducting malicious acts, from crafting a fake vessel that can appear charging into another state's sovereign water to possibly start a war, to misleading an officer on board ship to avoid a collision with a fake vessel which may lead to a targeted collision with another vessel, or even creating a fake distressed vessel to lure vessels to an attack[67].

---

[63] SOLAS Consolidated Edition Reg. 19 Chapter v (2018) 409-10.

[64] Balduzzi, Marco et al 'A security evaluation of AIS automated identification system' (2014) *ACSAC* 436, available at *http://dx.doi.org/10.1145/2664243.2664257*, accessed on 28 July 2022.

[65] Iphar, Clément et al. 'An expert-based method for the risk assessment of anomalous maritime transportation data' (2020) 104 *Applied Ocean Research* 1 at 4, available at *https://doi.org/10.1016/j.apor.2020.102337*, accessed on 6 July 2022.

[66] Androjna, Andrej et al 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied Science* 1 at 9, available at *https://doi.org/10.3390/app11115015*, accessed on 11 July 2022.

[67] Ibid.

b) AIS hijacking

In this scenario, the attacker alters the AIS information of an existing vessel to mislead the receiving station. This is achieved by intercepting the AIS communication midway and overriding it with a high-powered fake signal[68]. Therefore, what the receiving station gets on its end, is a modified version of the vessel's original message. This kind of malicious attack can ignite conflict, depending on the attacker's intentions. If used to conceal illegal activities, the perpetrators can steal another vessel's identity to shift blame.

c) AIS availability disruption

This is a vulnerability in AIS radio frequency, through which an attacker can shutdown AIS across a wide area by posing as maritime authorities and 'reserve the entire AIS transmission "address space"'[69].This action will prevent all AIS transmitters and receivers within that area from communicating with each other[70].Coastal stations use AIS to track and monitor traffic along the coast; should all AIS in a particular region suddenly shut down, coastal stations will lose effective control of the movement of vessels along their coastlines. Additionally, vessels relying on AIS information for navigation will be in a blind spot which may lead to collisions, depending on the amount of traffic and environmental factors. Furthermore, the attacker can command AIS transponders to change their frequency, thereby rendering the AIS useless, or delay the transmission, which will, in turn, prevent the vessel from transmitting its position; as a result, the targeted vessels or region will disappear from AIS tracking systems[71].This kind of attack can be conducted on a large scale depending on the attacker's intentions.

In all three vulnerabilities mentioned above, the attacker need not be on board the vessel to launch an attack. Instead, the attacks happen remotely by intercepting the AIS signal of the targeted station or in the targeted region and creating enough chaos necessary to achieve the desired intent[72].

(iii) GPS

a) Background

GPS is one of the overly relied-upon equipment on board ships today. It continuously provides the navigator with satellite-based position, speed, course, and time, informing most of the ship's

---

[68] Balduzzi, Marco et al A security evaluation of AIS automated identification system (2014) *ACSAC* 436 at 437, available at *http://dx.doi.org/10.1145/2664243.2664257*, accessed on 28 July 2022.
[69] Ibid at 438.
[70] Ibid.
[71] Ibid at 439.
[72] Androjna, Andrej et al 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied Science* 1 at 9, available at *https://doi.org/10.3390/app11115015*, accessed on 11 July 2022.

navigation decisions. However, researchers have warned against confidence in this system as it is one of the cyber-attack gateways to ship navigation systems[73]. Amongst others, the GPS is vulnerable to spoofing and signal jamming, conducted remotely without visual indication to the navigator[74].

b) Vulnerabilities

(a) GPS spoofing

GPS spoofing is when the attacker intercepts the GPS signal and manipulates it into mistaking their remote hacking tool as the satellite[75]. In June 2017, it was reported that hackers were able to interfere with the entire traffic in the Black Sea. According to the report, the GPS of a ship was altered to the extent that the position seen by the navigator on screen was out by 17 nautical miles from the actual position. During such time, no alarms were raised by the system to alert the navigator of foul play[76]. This incident did not affect only one vessel but the entire traffic within the spoofed region[77]. Though this attack did not cause any loss to the industry, it is a cause for concern as it has a potential for significant loss if the attackers decide to weaponise it to serve their cause.

(b) GPS jamming

GPS jamming is when an attacker uses radio frequency signals to overpower the GPS signals so that the receiver can no longer operate[78]. GPS jamming differs from spoofing since it does not require the attacker to create an accurate GPS signal[79]. Because the GPS signals must travel such a great distance to reach the receivers from the satellites, the strength of the signals that sent is significantly reduced[80]. As a result, they are susceptible to interference, whether that interference is accidental or intentional.[81]. The practise of jamming refers to the use of a

---

[73] Mohamed, Amine Ben Farah et al 'Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends' (2022) 13 *Information* 1 at 12, available at *https://doi.org/10.3390/info13010022*, accessed on 11 July 2022.

[74] Tam, Kimberly & Jones, Kevin D. 'MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment' (2019) *Maritime Affairs* 1 at 11, available at *https://doi.org/10.1007/s13437-019-00162-2.*, accessed on 4 August 2022.

[75] Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 8-9.

[76] Goward, Dana 'Mass GPS Spoofing Attack in Black Sea?', *Maritime Executive* available at *https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea*, accessed on 8 July 2022.

[77] Ibid.

[78] Ibid.

[79] International Association of Independent Tanker Owners (INTERTANKO) *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)* (2019) 1 at 4-5, available at *https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf*, accessed on 6 March 2023.

[80] Ibid.

[81] Ibid.

transmitter to produce radio frequency signals at a higher or the same frequency as GPS signals for the purpose of intentionally causing interference[82]. This interference makes it difficult for GPS receivers to receive any signal, which renders the receivers useless[83]. The problem of jamming is made even worse by the fact that GPS jammers have become relatively more accessible in recent years[84].

(iv) RADAR

a) Background

For decades RADAR has played a significant role in onboard navigation, simplifying the navigator's duties, and reducing human error in collision avoidance situations. Furthermore, RADAR has played a significant role in search and rescue, making detecting those in distress possible in all types of visibility. As a result, RADAR is one of the mandatory equipment onboard seagoing vessels[85]. However, technological advancement and over-reliance on automation have opened a gateway for hackers to attack ships through these navigation aids.

b) RADAR vulnerability

Research has shown that hacking into radio waves is not readily achievable like satellite hacking; however, it is not impossible[86]. It has been identified that two or more RADARs operating on the same frequency band can cause interference onboard ships resulting in RADARs spiralling and [?] causing difficulty in detection[87]. The same vulnerability can be used by hackers to spoof or jam onboard RADAR signals? to achieve their objective; however, since modern navigation bridge has various navigation aids that support the RADAR, hacking a RADAR might yield minimal result, thereby making it less appealing to the attacker[88].

(v) ECDIS

a) Background

ECDIS is one of the electronic navigation aids that has been made mandatory by the IMO on seagoing vessels, except for the few vessels which are exempted[89]. ECDIS is one of the over-

---

[82] International Association of Independent Tanker Owners (INTERTANKO) *Jamming and Spoofing of Global Navigation Satellite Systems (GNSS)* (2019) 1 at 4-5, available at *https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf*, accessed on 6 March 2023.
[83] Ibid.
[84] Ibid.
[85] SOLAS Consolidated Edition Reg. 19 Chapter v (2018) 409.
[86] Tam, Kimberly & Jones, Kevin D. 'MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment' (2019) *Maritime Affairs* 1 at 11, available at *https://doi.org/10.1007/s13437-019-00162-2.*, accessed on 4 August 2022.
[87] Ibid.
[88] Ibid.
[89] SOLAS Consolidated Edition Reg. 19 Chapter v (2018) 407.

relied-on navigation aids onboard a modern vessel, as it simplifies, amongst other things, passage planning, position fixing and chart updates, and is interconnected to other navigation aids giving the navigator an all-rounded picture of the situation around him/her[90]. As valuable as the ECDIS features may be, they make it vulnerable to cyber security breaches.

b) ECDIS vulnerability

One of the exposures to cyber security breaches is presented by the weekly updates of electronic charts, which is done by use of the Internet, USBs, or CD/DVDs and present 'network, hardware, and social engineering vulnerabilities with potential low Ease of Exploit (EoE) levels and high rewards for multiple attackers'[91].

Though ECDIS does not have a satellite connection, it is connected to servers that an attacker can remotely access. Additionally, research has shown that ECDIS presents cyber vulnerabilities that can impact other systems internetworking onboard[92]. This is due to the lack of end-to-end encryption and outdated security software[93]; the table in Appendix A is an abstract of the cyber vulnerability test results conducted on IMO-type approved ECDIS onboard Kobe University's training ship *Fukae-maru*[94].Similar tactic was also used to test ECDIS cyber vulnerability on a 'paperless SOLAS-certified tanker engaged in international trade'[95], and on the 'training and research ship *Kraljica mora* of the Croatian Ministry of the Sea, Transport and Infrastructure'[96], both of which yielded similar concerns.

It is clear, from the research, that for the attacker to gain access to the ship's navigation system, they need not hack all the available systems, but one weakest link which connects to all. The impact of which is dependent on the type of attacker and the desired end goal[97].

---

[90] Ibid.

[91] Tam, Kimberly & Jones, Kevin D. 'MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment' (2019) *Maritime Affairs* 1 at 11, available at *https://doi.org/10.1007/s13437-019-00162-2.*, accessed on 4 August 2022.

[92] Svilicic, Boris et al 'Assessing ship cyber risks: a framework and case study of ECDIS security' (2019) 18 *Maritime Affairs* 509 at 514-17, available at *https://doi.org/10.1007/s13437-019-00183-x*, accessed on 5 July 2022.

[93] Ibid.

[94] Svilicic, Boris et al 'Maritime Cyber Risk Management: An Experimental Ship Assessment' (2019) 72 *The Royal Institute of Navigation* 1108 at 1114, available at *https://doi.org/10.1017/S0373463318001157*, accessed on 19 July 2022.

[95] Svilicic, Boris et al 'Paperless ship navigation: cyber security weaknesses' (2020) 13 *Journal of Transportation Security* 203 at 206-8, available at *https://doi.org/10.1007/s12198-020-00222-2*, accessed on 5 July 2022.

[96] Svilicic, Boris et al 'Shipboard ECDIS Cyber Security: Third-Party Component Threats' (2019) 33 *Scientific Journal of Maritime Research* 176 at 178, available at *https://doi.org/10.31217/p.33.2.7*, accessed on 11 August 2022.

[97] Ibid.

(vi) Recent Cybersecurity reports

The table in Appendix B has been collated to understand better the likelihood and severity of a cybersecurity breach occurrence onboard, listing instances in which hackers intercepted these navigation systems in recent years. The list is not exhaustive and only shows a few reported incidents. More cases go unreported, and it is assumed that the industry might have so far experienced what one may refer to as a testing phase for hackers.

IV Cybersecurity risk measures for shipboard electronic navigation systems

(a) Introduction

Experts in cyber security, shipping companies, industry key role players, etc., have researched onboard cyber security breaches to find ways to neutralise or, at the very least, minimise the growing risk in cyber security onboard ships. The analysis and recommendations from this research inform the following measures.

(b) Shipboard navigation system cyber security measures

(i) Limiting/starving the attacker on availability of resources

The most significant incentive when it comes to cybersecurity breaching has been the feasibility[98]. The cost to the attacker on a single attack is meagre but yields excellent results, making it very appealing to the attackers. The devices used in cybersecurity breaches, such as spoofing and jamming, are easily acquired and affordable[99].It does not cost much for the attacker to spoof or jam a signal of any onboard navigational device; experts have identified that even the cheapest of jammers can cause significant damage[100].

Various case studies have been conducted on ships' navigation systems by intentionally hacking the systems to assess their weaknesses[101].What the research has shown is that, while autonomy onboard ships have advanced through the years, the systems' defences are meagre and outdated, which makes these systems an easy target for attackers[102]. Therefore, fortifying the cybersecurity in these navigation systems onboard to detect and evade an imminent cybersecurity breach, or at the very least, alert interested parties in due time, may provide some

---

[98] Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1-2.
[99] Androjna, Andrej et al. 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied Science* 1 at 20, available at *https://doi.org/10.3390/app11115015*, accessed on 11 July 2022.
[100] Ibid.
[101] Karahalios, Hristos 'Appraisal of a Ship's Cybersecurity efficiency: the case of piracy' (2020) 13 *Transportation Security* 179 at 181, available at *https://doi.org/10.1007/s12198-020-00223-1*, accessed on 19 July 2022.
[102] Svilicic, Boris et al. 'Paperless ship navigation: cyber security weaknesses' (2020) 13 *Journal of Transportation Security* 203 at 208, available at *https://doi.org/10.1007/s12198-020-00222-2*, accessed on 5 July 2022.

relief from these attacks[103]. Cybersecurity upgrades on the navigation systems may provide a degree of difficulty for the attacker, thereby reducing the success rate and rendering some hacking tools useless, limiting the scope of availability and incentives. However, achieving such a measure will require collaboration from all parties, including manufacturing, standardisation, and installation of ships' navigation systems.

(ii) Continuous risk assessment

Technology is progressive, and the threats that come with it are progressive. As a result, measures that may be effective today may not stay effective. Attackers will always look for countermeasures so long as the incentive remains. Therefore, the industry must stay current and ahead in its fight against cybersecurity breaches.

Various research studies have echoed risk assessments as the first step in response to this growing threat[104]. One can begin to draw up countermeasures by knowing the risk. It is this rationale that makes risk assessment an integral part of cybersecurity[105]. However, cybersecurity risk assessment may only be practical if it is done continuously to measure up against the innovative nature of technology, thereby avoiding ending up with obsolete security frameworks that no longer serve their purpose[106]. It is in the industry's interest to avoid settling into a 'false sense of security' and be complacent in its processes[107]. Various risk assessment tools involving test models, risk management programs, etc., have been made available by different experts in the field[108]. However, one must acknowledge that, though effective, the feasibility challenge may make such tools unattainable to interested parties.

(iii) Cybersecurity awareness culture onboard

Though autonomy has taken over most of the tasks that were manually done by the navigator onboard, however, it has not eliminated the user interface. Navigators are over-reliant on

---

[103] Androjna, Andrej et al 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied Science* 1 at 21, available at *https://doi.org/10.3390/app11115015*, accessed on 11 July 2022.

[104] Hemminghaus, C et al 'BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems' (2021) 15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 35 at 35,36,42, available at *http://www.transnav.eu*, accessed on 1 February 2022.

[105] Kavallieratos, Georgios et al. 'Shipping 4.0: Security Requirements for the Cyber-Enabled Ship' (2020) 16 *IEEE Transactions on Industrial Informatics* 6617 at 6618-21, available at *https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9016093&isnumber=9128058*, accessed on 7 February 2022.

[106]Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 5-6.

[107] Meland, P H et al 'A retrospective analysis of maritime cyber security incidents' (2021) 15 *the International Journal on Marine Navigation and Safety of Sea Transportation* 519 at 526, available at *http://www.transnav.eu*, accessed on 7 February 2022.

[108] Ibid.

autonomy which leads to poor awareness culture onboard[109]. Furthermore, systems updates, as in the case of ECDIS onboard, are carried out by the navigator. Depending on the company processes, this is done using drives to download the updates from the Internet, thereafter, insert them into the system[110]. Often, these drives are not scanned for viruses before being inserted into the navigation system due to the lack of awareness. Some companies send these updates to ships via a third party and complacently insert them into the system without question[111].

By raising the cybersecurity awareness culture onboard, navigators will be able to notice the signs of a compromised system, thereby allowing for the engagement of cybersecurity protocols in due time. To achieve this, the industry must continuously remind seafarers of the importance of cybersecurity awareness onboard. However, even with the promotion of cybersecurity awareness onboard, success depends on the seafarer's honesty in following protocol.

(iv) Cybersecurity training

Awareness is not possible without proper training. Before any seafarer embarks onboard a vessel, they must undergo vigorous training as stipulated by the STCW (Standard of Training, Certification and Watchkeeping for Seafarers) convention for their rank[112]. This is not a once-off training; it requires revalidation at different intervals whilst the seafarer is in service[113]. Furthermore, the SOLAS convention and the ISM code require onboard emergency drills to be conducted regularly[114]. Training, when carried out properly, raises awareness onboard. Therefore, conducting cybersecurity training for seafarers may assist in reducing cybersecurity breaches[115]. As the training will concurrently increase the level of cybersecurity awareness, thereby eliminating human error-aided attacks[116]. However, it is noteworthy that training is only practical if conducted honestly and as close as practicable to real-life scenarios. This will

---

[109] Svilicic, Boris et al 'Paperless ship navigation: cyber security weaknesses' (2020) 13 *Journal of Transportation Security* 203 at 204-5, available at *https://doi.org/10.1007/s12198-020-00222-2*, accessed on 5 July 2022.

[110] Svilicic, Boris et al 'Assessing ship cyber risks: a framework and case study of ECDIS security' (2019) 18 *Maritime Affairs* 509 at 515, available at *https://doi.org/10.1007/s13437-019-00183-x*, accessed on 5 July 2022.

[111] Caprolu, Maurantonio et al 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead' (2020) *Division of Information and Computing Technology* 1 at 4, available at *https://www.researchgate.net/publication/342965489*, accessed on 2 February 2022.

[112] EduMaritime 'STCW VI/1 - Safety Familiarization and Basic Training' *EduMaritime* available at *https://www.edumaritime.net/stcw-code/stcw-vi-1-safety-familiarization-and-basic-training*, accessed on 7 March 2023.

[113] Ibid.

[114] SOLAS Consolidated Edition 2018 Reg. 19 Chapter III (2018) 334-38.

[115] Androjna, Andrej et al 'Assessing Cyber Challenges of Maritime Navigation' (2020) *Journal of Marine Science and Engineering* 1 at 11, available at *https://www.mdpi.com/journal/jmse*, accessed on 9 July 2022.

[116] Ibid.

require personnel knowledgeable in cybersecurity to draw up these drills, which will be an additional expense to the shipowners.

(v) Designated cybersecurity personnel ashore and onboard

As an experienced seafarer, the author has knowledge of the different departments onboard and the designated personnel ashore. Training onboard is not conducted by a specified department that deals with staff development, as is the case ashore. Instead, training onboard is conducted by the officers as per the hierarchy, with the assumption that the officers have the proper knowledge. However, after analysing the research that has been conducted in this field of cybersecurity, one must appreciate the level of technicality that is required[117]. This is not an issue that can be responded to with conventional means. As far as it falls under security, it is not a conventional security matter that can be combated by physical means only. It will take more than just a short course or a poster of the procedures on the bulkheads to fully understand what is required. For ship personnel who are already overstretched with their designated operational duties, it might be farfetched to expect them to adequately take the role of training, monitoring, and improving cybersecurity awareness onboard. Furthermore, being a nautical science or marine engineering officer does not automatically make one an expert in all trades.

It is through this rationale that an appointment of cybersecurity personnel is imperative. Ships' processes have become similar to shore processes, making the vulnerability similar in most ways. Therefore, having an expert on information technology onboard liaising with the designated cybersecurity officer ashore may improve cybersecurity awareness onboard, the level at which cybersecurity drills are conducted and achieving continuous cyber risk assessment.

(vi) Designated cybersecurity reporting system and information-sharing platforms

The industry is dealing with a new enemy which has the potential to do significant damage with just one attack[118]. They do not need to target a specific ship, and the attack can be targeted on a specific region, affecting the entire fleet in that region[119].Furthermore, the attackers do not rely on physical means to do damage but rely on technology and all its innovations[120]. To neutralise such an enemy, the industry must stay ahead in every way, e.g., research and

---

[117] Androjna, Andrej et al 'Assessing Cyber Challenges of Maritime Navigation' (2020) *Journal of Marine Science and Engineering* 1 at 11, available at *https://www.mdpi.com/journal/jmse*, accessed on 9 July 2022.

[118] Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 2.

[119] Kapalidis, Polychronis 'Cybersecurity at sea' in Otto, Lisa (ed) *Global Challenges in Maritime Security* (2020) 142, available at *https://doi.org/10.1007/978-3-030-34630-0*, accessed on 1 February 2022.

[120] Androjna, Andrej et al 'Assessing Cyber Challenges of Maritime Navigation' (2020) *Journal of Marine Science and Engineering* 1 at 3, available at *https://www.mdpi.com/journal/jmse*, accessed on 9 July 2022.

development of its systems. This means the industry will need not only to deal with the known means of attack but also to forecast the enemy's possible attacks and fortify its systems against them[121].

To achieve this, the industry will require every bit of information on cybersecurity breaches to fully understand what the strengths, weaknesses, and drive for these attacks are[122]. For this to be possible, information must be shared among stakeholders[123]. Research has shown that thus far, some incidents go unreported, and only those that are too great to conceal make it to the news[124]. The old saying "sharing is caring" must be at the industry's heart. As it was established for piracy, reporting procedures need to be established for cybersecurity to empower the industry with rich knowledge which can be weaponised against the enemy. Furthermore, platforms for sharing good practices must be established to learn from each other and spread cybersecurity awareness. However, this can only be possible with stakeholders' full cooperation[125].

(vii) Implementation

Procedures without implementation are futile exercises. Implementation is critical, and the industry needs to establish a system, framework, or convention to deal with cybersecurity issues and ensure that procedures developed to combat cybersecurity breaches are implemented onboard[126]. This is a great task to achieve and will take more than talk but consensus among stakeholders and resources that might not be readily available to all interested parties. However, notwithstanding the challenges of ensuring the implementation of cybersecurity onboard, the industry needs to open a dialogue on implementation strategies in its pursuit of secure cyber seas[127]. This will require significant cooperation from stakeholders to find common ground.

(viii) Solidarity

The saying "stronger together" has proven true for the industry during the peak of Somalian piracy disrupting the trade. The industry came together, developed procedures and laws, and

---

[121] Ibid.
[122] Ibid.
[123] Greiman, V A 'Defending the cyber sea' (2020) 19 *Journal of Information Warfare,* 68 at 76-7, available at *https://www.jstor.org/stable/10.2307/27033633*, accessed on 7 July 2022.
[124] Meland, P H et al 'A retrospective analysis of maritime cyber security incidents' (2021) 15 *the International Journal on Marine Navigation and Safety of Sea Transportation* 519 at 526, available at *http://www.transnav.eu*, accessed on 7 February 2022.
[125] Greiman, V A 'Defending the cyber sea' (2020) 19 *Journal of Information Warfare,* 68 at 76-7, available at *https://www.jstor.org/stable/10.2307/27033633*, accessed on 7 July 2022.
[126] Ibid at 76.
[127] Ibid.

formed alliances with navy forces and private security companies[128]. A great deal of resources from various member states were deployed to protect the ships from piracy. This kind of cooperation will make all other measures possible, working together to protect the cyber sea by sharing resources and finding common ground[129].

(c) Conclusion

The above list of measures is not exhaustive; combined, they may be the first step towards cyber secure navigation systems and beyond. Furthermore, it is noteworthy that these cannot be achieved overnight; it will take more effort from all interested parties to reach a consensus on cybersecurity issues. After all, it needs to be appreciated that the industry only recently just realised cybersecurity threats[130].

[128] Ibid at 76-7

[129] Greiman, V A 'Defending the cyber sea' (2020) 19 *Journal of Information Warfare,* 68 at 76-77, available at *https://www.jstor.org/stable/10.2307/27033633*, accessed on 7 July 2022.

[130] Ibid at 72.

CHAPTER 3 MARITIME INDUSTRY CYBER RISK MANAGEMENT REVIEW

I Introduction

Ships' navigation systems will be at risk of cyber security breaches as long as they stay connected to the internet, directly or indirectly, through another system in the same network[131]. This realisation is apparent in the industry stakeholders, moving to generate and adopt cyber security guidelines to remedy the situation.

The IMO, BIMCO and various industry role players' cyber security guidelines will be reviewed below. These guidelines feature other industry stakeholders not reviewed individually and incorporates what has been formulated by other industry role players such as classification societies, flag states and insurers, thereby giving a holistic view of the industry standpoint on cyber security. The review will then clarify the industry's readiness in the fight against cybersecurity breaches by comparing what is already in place with what is needed to be done.

II BIMCO Guidelines on cybersecurity onboard ships

In July 2017, BIMCO published cyber security guidelines for ships[132]. These guidelines aim to help the maritime industry prevent major safety, environmental, and commercial issues that could result from a cyber security breach onboard a ship[133]. Industry stakeholders, including the International Maritime Organization (IMO), have widely recommended these extensive and comprehensive guidelines[134]. The guidelines are continuously reviewed to keep them current and effective[135]. This ensures that they are always cutting-edge in the fight against cyber security breaches[136].

The guidelines cover, in detail: 'Establishment of awareness of the safety, security and commercial risks that present themselves due to lack of cyber security measures, protection of shipboard IT infrastructure and connected equipment, system for authentication and authorisation of users to ensure appropriate access to necessary information, protection of data

---

[131] Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 4-6.

[132] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021), available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

[133] Ibid.

[134] International Maritime Organisation *Guidelines on maritime cyber security risk management* (2017) 1 at 4, Available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

[135] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021) available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

[136] Ibid.

that is used in the ship environment, ensuring it has adequate protection based on the sensitivity of the information, management of IT users to make sure they only have access and rights to the information for which they are authorised, management of communication between the ship and the shore side, and develop and implement a cyber incident response plan based on risk assessment'[137].

BIMCO's approach makes it clear that it will take more than the ship's crew to strengthen the cybersecurity firewall onboard. It will require all interested parties, from shipowners to shipbuilders, hardware and software developers, service providers and onboard personnel[138]. They have shown that cybersecurity threats continually innovate. Day by day, they are improving and reaching new heights, and they will continue to innovate with every measure put in place. Therefore, the industry needs to continually innovate to stay ahead[139]. There is no once-off approach to this problem, but continuous risk assessment and development and implementation of new prevention measures to meet new threats.

For the industry to stand a chance against cyber security breaches, awareness must start at the top management and flow down[140]. The guidelines further demonstrate the need to continuously identify and update the vulnerabilities and measures to prevent breaches onboard. This is required from all key role players in their respective capacities, including manufacturers[141].

On the face of it, these guidelines cover all bases, from identifying risks to prevention measures and the need for training[142]. However, even in its elaborative form, there remain the feasibility questions. There is still an element of choice even for companies that can afford to build this cyber security fortress. These guidelines are only given as recommendations and are not legally binding[143].

III IMO, Cybersecurity resolution

The IMO, as the industry regulatory body, in its response to cyber security threats, published Guidelines on maritime cyber risk management in 2017[144]. These guidelines states, on a broad

---

[137] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021), available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.
[138] Ibid at 3.
[139] Ibid at 5-6.
[140] Ibid at 6.
[141] Ibid at 10.
[142] Ibid.
[143] Ibid.
[144] International Maritime Organisation *Guidelines on maritime cyber security risk management* (2017) 1, available at

overview, that 'effective cyber risk management should start at the senior management level'[145]. However, the guidelines are only recommendatory, meaning the choice rests with the interested parties on whether and, if so, how to apply them in their respective organisations[146]. However, the guidelines include an amendment to the general safety management code to explicitly include cybersecurity. The International Safety Management Code (ISM) mandates every shipping company to ensure that cybersecurity risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021[147].

The IMO's approach, at first glance, appears to be voluntary [compliance?], therefore, not legally binding. However, the inclusion of cybersecurity in the ISM code suggests a degree of compulsory element. This makes cybersecurity an audit item. Though the resolution does not explicitly state the implications of non-compliance, one can safely assume that there will be legal implications for non-complying parties, which can be an incentive for ensuring a cyber-secure future for the maritime industry[148]. Nevertheless, there is much contradiction pertaining to the voluntary nature of the guidelines, which poses a potential for varying interpretations to different stakeholders[149].

The IMO Guidelines on Maritime Cyber Risk Management goes on to call for developing guidelines that included national and international standards, best practices, and the implementation of risk-control processes and measures, as well as contingency planning[150].

---

https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

[145] International Maritime Organisation *Guidelines on maritime cyber security risk management* (2017) 1 at 4, available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

[146] Ibid.

[147] International Maritime Organisation *Maritime Cyber Risk Management in Safety Management Systems* (2017) 1, available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

[148] The International Maritime Organisation (IMO) has a long history of adopting resolutions that are legally binding. For example, the IMO's ISM code is a legally binding treaty that sets international standards for the safety management of ships and impose penalties for non-compliance, see IMO Knowledge centre at *https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx.*

[149] Voluntary guidelines are not legally binding. This means that organisations are not required to comply with them, and they can choose to interpret them in any way they see fit. However, the ISM code is a legally binding treaty. This can lead to different organisations having different understandings of what the guidelines mean, which can make it difficult to ensure that everyone is on the same page.

[150] International Maritime Organisation *Maritime Cyber Risk Management in Safety Management Systems* (2017) 1, available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

This is believed to be a promising start of a more holistic approach to maritime cybersecurity regulation and achieving uniformity in the cyber risk control and application of measures to neutralise cyber security threats in maritime. However, an accelerated pace will be needed for the maritime industry to get ahead in the fight against cybersecurity breaches. This opinion is based on the time lapse between adopting the guidelines in 2017 and the application date for such guidelines, which was 2021.

IV Other industry key role players' initiative

(a) Background

The guidelines above show that the industry is taking a stand against cybersecurity breaches. The scope of these guidelines includes vulnerabilities posed by electronic navigation systems onboard and, if implemented correctly, have the potential to make an impact in neutralising the threat or, at the very least, to minimise the impact of the threat[151].

(b) Standardisation organisations

More guidelines have been published by different entities in the industry, all echoing a similar message which is, when loosely interpreted, to wake up and stand together in the fight against cybersecurity breaches[152]. Amongst others, there are industry standards organisations such as the International Electrotechnical Commission (IEC)[153], the International Organisation for Standardisation (ISO)[154] and the US National Institute of Standards and Technology (NIST)[155]. These standards share a common objective, which is to ensure cyber resilience in the maritime sector, thereby protecting critical infrastructure from cybersecurity breaches by employing effective cyber security framework[156]. Furthermore, the standards set the requirements for both

---

[151] See BIMCO Guidelines on cyber security onboard ships and IMO Guidelines on maritime cyber security risk management referenced above.

[152] There is a growing sense of urgency among the shipping industry to address the issue of cyber security. This has led to the publication of several guidelines by different entities in the industry, all which spreads awareness on cybersecurity. See BIMCO Guidelines on cyber security onboard ships and IMO Guidelines on maritime cyber security risk management reviewed above.

[153] International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27001 *Information technology — Security techniques — Information security management systems — Requirements* (2013) Switzerland International Organization for Standardization, available at *http://www.itref.ir/uploads/editor/42890b.pdf*, accessed on 6 December 2021.

[154] Ibid.

[155] National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 ed (2018) available at *https://doi.org/10.6028/NIST.CSWP.04162018*, accessed on 6 December 2021.

[156] Ibid.

technical and operational cyber security for general industrial and maritime assets[157], and cover vulnerabilities to systems that are in operation within the maritime domain[158].

(c) Classification societies

Several maritime classification societies have recently published guidelines on cybersecurity. Amongst others, there is the American Bureau of Shipping (ABS)[159], the Lloyd's Register (LR)[160], the International Association of Classification Societies (IACS)[161], and the Det Norske Veritas-Germanischer Lloyd (DNV GL)[162]. Like the standardisation organisations, the classification societies guidelines on cybersecurity seem to share the same objective which is ensuring cyber resilience in maritime critical infrastructure. ABS guidelines on cybersecurity which is developed for vessel operators, owners, construction, and integration companies, cover operational and technical cybersecurity measures, as well as data integrity and risk reduction strategies for IT and OT systems[163]. Lloyd's Register has also published three guidelines on cybersecurity, which cover the implementation of IT and OT systems in maritime infrastructure and autonomous ships[164]. Furthermore, the IACS also issued a recommendation on cyber resilience, which outlines the technical requirements for building cyber-resilient infrastructure for vessels[165]. Lastly, the DNV GL has released a set of recommended practices that implement the IEC cybersecurity assessment standard for IT and OT systems and

---

[157] Ibid.

[158] International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27001 *Information technology — Security techniques — Information security management systems — Requirements* (2013) Switzerland International Organization for Standardization, available at *http://www.itref.ir/uploads/editor/42890b.pdf*, accessed on 6 December 2021.

[159] American Bureau of Shipping (ABS) *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety* (2016) available at https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf, accessed on 6 December 2021.

[160] Lloyd's Register *Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping—Lloyd's Register's Approach to Assurance* (2016) available at https://www.lr.org/en/latest-news/early-adopters-and-innovators-in-connected-assets-on-ships/, accessed on 6 December 2021.

[161] International Association for Classification Societies (IACS) *Recommendation on Cyber Resilience Recommendation No. 166* (2020) available at *https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1*, accessed on 6 December 2021.

[162] Det Norske Veritas-Germanischer Lloyd *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation* (2016), available at https://www.dnv.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585, accessed on 6 December 2021.

[163] American Bureau of Shipping (ABS) *Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS CyberSafety* (2016) available at https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf, accessed on 6 December 2021.

[164] Lloyd's Register *Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping—Lloyd's Register's Approach to Assurance* (2016) available at https://www.lr.org/en/latest-news/early-adopters-and-innovators-in-connected-assets-on-ships/, accessed on 6 December 2021.

[165] International Association for Classification Societies (IACS) *Recommendation on Cyber Resilience Recommendation No. 166* (2020) available at *https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1*, accessed on 6 December 2021

infrastructure, as well as industrial automation and control systems used onboard ships[166]. These practices are intended to protect against cyberattacks and are all consistent with cyber resilience model.

This list is by no means exhaustive, and it constitutes acknowledgement of the cyber security threats in the industry and the consensus reached by stakeholders for the need to address the issue. The movement is evident, and the message echoes globally; however, the question remains, does this assure industry readiness in the fight against cyber security threats? Has the industry done everything to stay ahead of the cyber security threat wave?

[166] Det Norske Veritas-Germanischer Lloyd *Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation* (2016), available at https://www.dnv.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585, accessed on 6 December 2021.

CHAPTER 4 REVIEW RESULTS

I Introduction

It seems clear from the review that the industry has recognised the threats posed by cybersecurity breaches and is moving to safeguard against further breaches. This indicates that the industry acknowledges the importance of assessing cyber security risks with the intention of putting effective preventative measures in place. This chapter will outline the review outcome by comparing what the industry has in place and what is needed to ensure readiness.

(a) Meaning of 'readiness'

The Oxford Dictionary defines 'readiness' as 'the state of being fully prepared for something'[167]. From this definition, one can safely assume that for the industry to be at the state of readiness for cybersecurity, it will need to be fully prepared to be able to identify and manage cybersecurity risks, which will allow for early detection of cybersecurity threats and effective response to prevent loss or damage due to breach.

From the review and research on this field, it has become apparent that readiness starts with proper planning from all interested parties. Feeding into the plan is data from various relevant and competent departments regarding the risk one wants to safeguard against. For these departments to comply, top management needs to play its role. Furthermore, after a thorough assessment of the data has been conducted and measures drawn up, there remains action.

II Industry's state of readiness

(a) What is in place

As the industry stands now, based on the above review, there is a plan in motion and awareness has been spread through guidelines and various academics and experts' writing, some of which have been cited in this study. The need for continuous awareness and means to achieve it have been shared. Furthermore, the need for seafarer training, strengthening cybersecurity on navigation systems, and assigning designated cybersecurity personnel are amongst the measures proposed by the guidelines.

(b) What is lacking

(i) Lack of compulsion

The lack of compulsion in maritime cybersecurity measures is a major challenge to the safety and security of ships. While there are several guidelines and best practices available, there is

---

[167] Oxford online dictionary 'Readiness' available at *https://www.oxfordlearnersdictionaries.com*, accessed on 12 July 2022.

no single, mandatory set of standards that all ships must comply with. This leaves ship operators with a great deal of flexibility in how they approach cybersecurity, and it can be difficult to ensure that all ships are adequately protected.

There are several reasons why there is no compulsion in maritime cybersecurity measures. One reason is that the shipping industry is highly decentralised, with many different stakeholders involved. This makes it difficult to reach consensus on a single set of standards. Another reason is that the cost of implementing cybersecurity measures can be high, and some ship operators may not be able to afford them.

(ii) Why is lack of compulsion a problem?

The lack of compulsion in maritime cybersecurity measures has a number of negative consequences. Ships that are not adequately protected are more vulnerable to cyber-attacks, which can have a range of serious consequences, including: loss of control of the ship, damage to the ship's systems, loss of data, financial losses, environmental damage, etc. As the say goes, 'strong as the weakest link', a handful of ships not adequately protected will negatively affect the supply chain.

In addition, the lack of compulsion in maritime cybersecurity measures can also undermine public confidence in the shipping industry. If investors, shippers, passengers, charterers, etc, believe that ships are not adequately protected, they may be less likely to use them, which could have a negative impact to the industry and the economy.

Addressing the lack of compulsion in maritime cybersecurity measures is essential to ensuring the safety and security of ships. By taking steps to improve the cyber security of ships, the shipping industry can protect itself from the serious consequences of cyber-attacks and maintain public confidence.

(iii) Reporting procedures

Furthermore, at this point, there have not been any reporting procedures established for cyber security breach incidents, or near misses, as evident in safety-related matters[168]. These have played a significant role in improving safety at sea as they identify gaps and make it possible to put proper measures in place to prevent re-occurrence, not only for the vessels involved but for the benefit of the industry[169]. Information sharing is vital for any trade; as the say goes, 'sharing is caring', but, so far, most companies rather conceal these incidents in fear of losing

[168] Section 9 of the International Safety Management Code (ISM) mandates accidents and near-miss reporting on hazardous situations.
[169] Ibid.

business, and so long as that continues to be the case[170], the industry will remain in hindsight of the full impact of this threat.

(iv) Cybersecurity training

There is also a need for training for those on board and the entire supply chain connected to shipping; as BIMCO guidelines have highlighted, one of the cases of cyber security breach did not originate onboard the vessel but was planted during the installation of an ECDIS[171]. It will take all hands on deck for all parties connected, physically or remotely, to shipping to close all vulnerability gaps. Just as IMO has reduced safety-related accidents at sea through continuous development in seafarer training, the same is necessary for cyber security training. Maritime-specific training must be developed targeting various positions and roles in shipping. There is no use in building cyber-secure shipping if the users lack knowledge of the operation. This has already been proven by safety equipment at sea; before proper training on lifeboat handling and maintenance was given in the use of lifeboats, there were more incidents reported due to lifeboat launching failures[172].

(c) Issues affecting industry readiness

(i) Element of unknown

The industry needs to appreciate that there is much to learn about cybersecurity threats. The perpetrators' intentions are yet to be discovered; it is believed that they are still in the research and development phase, testing ways to breach the industry's cyberspace to gauge its response. This is purely speculative, based on analysis of recent cases[173], however, it can be appreciated that cybersecurity breaches have far more incentives to perpetrators due to their remoteness, minimal risk, expense, and exposure. This form of security threat has the potential to feed into various crime syndicates like piracy, terrorism, geopolitical warfare, activism, etc. If this menace continues to gain access to the industry, there is no telling on the magnitude of disruption it will go, what level it will innovate to and what predators it will attract.

---

[170] Capt. Saito, Naoki *Cyber Security Onboard* (2022) Tokyo, Japan, Nippon Kaiji Kyokai (ClassNK) 1 at 5, available at *https://www.classnk.com*, accessed on 14 September 2022.

[171] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021) 1 at 11, available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

[172] Yatsenko, Nick 'Why are lifeboats killing seafarers' *GCaptain*, available at *https://gcaptain.com/why-are-lifeboats-killing-seafarers/*, accessed on 12 September 2022.

[173] See the table of cases in Appendix B.

The industry has yet to give legal meaning to cybersecurity threats in shipping[174], and the marine insurance domain faces challenges in allocating cover for cybersecurity-related risk, leaving shipping companies exposed to significant risk[175]. Giving cybersecurity threats legal meaning is a necessary step towards achieving industry readiness, as that will allow for more concerted efforts to be put in place, e.g., law enforcement, insurance companies and possible private entities. Relying on national laws is not prudent as many national jurisdictions do not have cybersecurity laws, and many usually adopt international laws into national laws. It took a great deal of collaboration from the industry role players, private entities, navy, and legal system to minimise piracy in the Horn of Africa; it will take even greater efforts and louder voices to alert the industry on cybersecurity awareness.

(ii) Onboard cybersecurity challenges

It is also noteworthy that though IMO may mandate cybersecurity measures onboard ships, a shipowner has limited control once the ship leaves the quayside. Ships operate remotely; as a result, the shipowner and the industry depend on the seafarer's good faith for safety and security during such times. The shipowner and the industry cannot guarantee complete compliance for the seafarer.

Seafarers often face long hours of work, strict deadlines, fast-paced cargo operations, extensive periods away from loved ones and unfavourable environmental conditions. Over time, this adversely affects seafarers' well-being, thereby affecting the commitment level to conduct required tasks faithfully and being complacent and resistant to change. Various research has identified that the human element is a significant contributor to cybersecurity breaches, which led to the realisation of the need for awareness through training and continual cybersecurity alertness. However, ensuring this training is carried out as required heavily relies on good faith. Ships have been known to look good on paper but not in practice.

Furthermore, there are also language barriers due to different nationalities on board that have varying proficiency in the ship's official language, which then end up not understanding what is required of them. Training drills end up being conducted for the sake of ticking boxes rather than effective learning, therefore, not serving the purpose for which they were designed.

Another issue with onboard cybersecurity is the absence of a cybersecurity expert to oversee all cybersecurity-related matters and be able to correct cybersecurity loopholes before

---

[174] Greiman, V A 'Defending the cyber sea' (2020) 19 *Journal of Information Warfare* 68 at 72, available at *https://www.jstor.org/stable/10.2307/27033633*, accessed on 07 July 2022.
[175] Ibid at 71.

they materialise. Expecting ship personnel to train each other on matters they lack understanding is ignorant and relying on training videos leads back to limited control.

On the other hand, there is an issue with common network points used for private crew communications and browsing and the ship's operational communications. If this remains, the hacker only needs one crew member to click on the wrong link and follow that connection to the shared network point.

III Conclusion

It is noteworthy that there is a degree of difficulty and complexity in dealing with security matters. Unlike safety-related matters, where a problem is identified and known and therefore can be simulated and preventative measures put in place will continue to be efficient so long as the source remains. With security, there is an element of unknowns, the mystery of how the perpetrator will counteract the preventative measure and how destructive that action would be to the current measures. In safety matters, for example, it took a collision bulkhead to minimise the impact after a ship collided[176]. But looking at piracy, an extensive effort had to be applied[177], and even then, piracy continues. Therefore, expecting industry readiness to be achieved by the efforts of IMO and the like would be ambitious.

Therefore, due to these findings, the industry is not yet fully ready to fight against cybersecurity breaches. While there has been some progress in recent years, there are still several challenges that need to be addressed. This rationale is informed by the research conducted by the experts cited in this study, the gaps between the proposed measures and the measures put in place by the industry.

---

[176] SOLAS Consolidated Edition 2018 regulation II 1/12

[177] Concerted efforts from various States and international bodies devising plans on combating piracy in the form of armed guards onboard, vessel security hardening, seafarer security training, navy convoys, information sharing, International legal framework to bring perpetrators to justice etc. see Gard ' Piracy and armed robbery at sea' available at *https://www.gard.no/web/content/piracy-and-armed-robbery-at-sea*, accessed on 12 July 2022

CHAPTER 5 ELECTRONIC BANKING SYSTEMS

I Introduction

It has been established that the maritime industry is increasingly reliant on electronic systems for a wide range of tasks, from navigation to cargo management. This reliance on electronic systems has made the maritime industry a target for cyber-attacks. In recent years, there have been several cyber-attacks on maritime targets[178]. To protect itself from cyber-attacks and bridge the gaps in cybersecurity onboard ships, the maritime industry can learn from the experience of the banking industry, and, if possible, adopt or improve on some of their strategies that may prove effective.

Benchmarking organisation's strategies, processes and performance with the best competitors or common sectors is standard practice in any industry. This practice is usually fruitful and promotes organisational growth because it frequently reveals areas for improvement. However, cybersecurity is undoubtedly a new threat in the maritime sector due to the industry's previous remoteness and solitude. As a result, it should come as no surprise that there is still room for more research and study into ways to combat this threat. However, while the industry's class is in session, the threat grows exponentially, leaving the industry in retrospect.

The banking sector's electronic banking systems cybersecurity vulnerabilities and measures to combat cybersecurity breaches will be studied briefly, for benchmarking purposes, in this chapter.

II Background

It is undeniable that banks are frequent targets of cybersecurity breaches and have been dealing with this threat since the dawn of technological evolution[179]. This gives the banking sector a better understanding of cyber security risk than other sectors[180]. In a heavily regulated industry, businesses must stay on top of the most recent technical and regulatory advancements[181]. The maritime industry and the banking sector have in common in-demand assets that appeal to the eye[182]. They both have assets that operate remotely and out of reach at times, prone to various

---

[178] See table of cases in Appendix B.

[179] International Monetary Fund 'The Global cyber threat' available at *https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm,* accessed on 7 February 2023

[180] Ibid.

[181] Ibid.

[182] Banking sector moves large sums of money in a daily basis, and the maritime industry moves highly valuable cargo, making both these sectors very appealing to the perpetrators.

threats without the company's alertness[183]. Furthermore, both sectors' technology relies on network connectivity and integrating different systems for the desired outputs[184].

This research will examine the cyber security vulnerabilities and countermeasures the banking industry uses to protect its electronic banking systems from cyber security breaches.

III Comparisons with electronic banking systems operation

(a) Electronic banking

(i) What is electronic banking?

A style of banking known as "electronic banking" is one in which the transfer of funds is done digitally as opposed to physically exchanging cash or relying on other paper-based documents[185]. Transfers occur between financial institutions or business establishments like banks, credit unions, shops, and financial organisations[186]. Electronic banking is a system that allows people to access their bank accounts and conduct financial transactions electronically[187]. This can be done through ATMs, debit cards, or online banking[188].

Electronic banking is supported by complex computer networks that connect over telephone lines[189]. These computerised systems keep track of money transfers and ownership of funds and regulate how customers and commercial institutions access money[190]. Access codes, such as a personal identification number (PIN) used to withdraw money from an ATM, are a typical way to get access to a computer system[191].

Electronic banking systems come in various types and sizes, depending on the system's functions and capabilities[192]. Users of large systems can manage significant, urgent payments like those needed to close real estate deals without the use of paper-based documents[193].

---

[183] Ships operates remote from its operators and ATM's and self-service electronic banking systems operates remote from the banks, offering very little control for the operators.

[184] See chapter 2 above for shipboard electronic navigation systems connectivity, and electronic banking systems connectivity is discussed in this chapter below.

[185] Schaechter, Andrea 'Issues in electronic banking: An overview' (2002) *Monetary and exchange affairs department* 1 at 3-4, available at *https://www.imf.org/external/pubs/ft/pdp/2002/pdp06.pdf*, accessed on 6 April 2023.

[186] Chaimaa, Belbergui et al. 'E-banking Overview: Concepts, Challenges and Solutions' (2021) 117 *Wireless Personal Communications* 1059 at 1060-1, available at *https://doi.org/10.1007/s11277-020-07911-0*, accessed on 6 April 2023.

[187] Ibid.

[188] Ibid.

[189] Cengage 'Electronic Banking' (2019) *Encyclopedia.com*, available at *https://www.encyclopedia.com/finance/encyclopedias-almanacs-transcripts-and-maps/electronic-banking*, accessed on 7 February 2023.

[190] Ibid.

[191] Ibid.

[192] Ibid.

[193] Ibid.

(ii) How does it work?

Typically, three parties are involved in an electronic banking transaction: the bank, the customer, and the merchant[194]. Some transactions require the involvement of the bank and the customer[195]. The transaction is initiated by the customer, whether by making the request online, going to a store, or going to an ATM[196]. Based on the accuracy of the information provided in the request, the bank receives the request and, in the case of withdrawals, decides whether to allow or refuse the electronic transfer of cash[197]. The money is sent electronically to or from the consumer's account and then to the designated recipient after processing is finished[198].

To remain within the confines of this research, two types of electronic banking will be briefly discussed, namely: ATM and Internet banking, to illustrate the similarities in the operation of electronic banking systems and electronic navigation systems. Thereby justifying the reason for this benchmarking.

(b) ATM

(i) What is it?

An ATM, formally known as an automated teller machine, is a computerised telecommunications device that allows users access to financial transactions remotely without a bank personnel interface[199]. This provides the user with convenience, privacy, simplicity, and freedom to perform financial transactions without the limitations of the bank[200].

Additionally, banks usually install on-premises ATMs to simplify processes, freeing bank operators from other duties requiring their attention and enhancing customer service[201]. On-premises ATMs are technically more advanced and support multiple services to

---

[194] Hajera, Fatima 'E-Banking System Benefits and Issues' in Dr. Kaustubha Nand Bhatt (ed) *Insights into Economics and Management* Vol 11 (2021) 40-1, available at *https://www.researchgate.net/publication/351959769_E-Banking_System_Benefits_and_Issues*, accessed on 6 March 2023.

[195] Ibid.

[196] Cengage 'Electronic Banking' (2019) *Encyclopedia.com*, available at *https://www.encyclopedia.com/finance/encyclopedias-almanacs-transcripts-and-maps/electronic-banking*, accessed on 7 February 2023.

[197] Ibid.

[198] Ibid.

[199] Mahmood, Tariq & Mujtaba, Shaikh Ghulam 'Adaptive Automated Teller Machines (2013) 40 *Expert Systems with Applications* 1152 at 1152-3, available at *http://www.elsevier.com/locate/eswa*, accessed on 30 March 2023.

[200] Ibid.

[201] Khalifa, Salem S. M. & Saadan, Kamarudin 'The Formal Design Model of an Automatic Teller Machine (ATM)' (2013) 1 *Lecture Notes on Information Theory* 56, available at *https://www.academia.edu/26612106/The_Formal_Design_Model_of_an_Automatic_Teller_Machine_ATM*, accessed on 1 April 2023.

complement a bank branch's capabilities. In contrast, remote ATMs are primarily designed for a single function based on the need for that location[202].

(ii) How it works?

An ATM is a computerised terminal with 'two inputs (card reader and the keypad) and four output devices (speaker, display screen, receipt printer and cash dispenser)'[203]. The ATM, though remotely situated, forms part of an integrated system which consists of the ATM, the host processor/computer, and the bank server/computer[204]. The ATM operation is dependent upon connection to the network and communication between the ATM and the bank server through the host processor[205]. The host processor is similar to an internet service provider (ISP) in that it is gateway through which users can access different ATM networks[206]. Just as an ISP connects users to the internet, the host processor connects users to ATM networks[207]. This allows users to withdraw cash, check their balance, and perform other banking transactions from any ATM in the world [208].

ATMs can be categorized into two types based on their mode of communication: leased-line ATMs and dial-up ATMs[209]. Leased-line ATMs connect to the host processor through a dedicated four-wire telephone line, while dial-up ATMs connect to the host processor through a normal phone line using a modem[210].

The communication between an ATM and a bank server begins when the user enters the necessary details to perform the desired transaction[211]. The ATM forwards this information to the host processor, which directs the transaction request to the user's bank server[212].The bank server verifies the user's details and, if they are valid, transfers electronic funds from the user's account to the host processor's account[213]. Once the communication between the host and the bank is finalised, the host processor will then send an approval code to the ATM authorising cash dispensation[214]. Like electronic navigation systems onboard ships, this entire

---

[202] Ibid.
[203] Ibid at 57.
[204] Ibid at 56-7.
[205] Ibid at 58.
[206] Ibid.
[207] Ibid,
[208] Ibid.
[209] Bowen, Jim 'How ATMs Work' available at *https://money.howstuffworks.com/personal-finance/banking/atm.htm*, accessed on 30 March 2023.
[210] Ibid.
[211] Ibid.
[212] Ibid.
[213] Ibid.
[214] Ibid.

communication process is conducted independently without the bank personnel interface through integration[215].The communication beyond the user's input data point is automated, and the output data is dependent upon the integrity of the input data and the verification points[216]. Therefore, compromise in one or more links in the communication chain will result in erroneous transactions.

(c) Internet banking

(i) What is it?

The past decade has seen a rise in the popularity of online banking, commonly referred to as Internet banking[217]. It is a convenient method of banking and a great approach to taking charge of one's finances[218]. Internet banking is using a smartphone, tablet, or computer to access a bank account and conduct financial transactions via the internet[219]. It is quick, generally free of charge, and allows the user to complete transactions like bill payments and money transfers without having to visit or phone your bank[220]. Users can also send money locally, nationally, and internationally by using Internet banking services[221]. These services also allow users to access and print their bank statements without having to visit the bank[222].

(ii) How it works

Internet banking can be accessed from any place of choosing, at home, office, café, etc., so long as the user's device remains connected to the internet[223]. Internet banking system connects a user's personal computer directly to the host computer system of a bank through the use of a network service provider[224]. This allows for the automatic processing of user service requests, which eliminates the need for customer service representatives to be involved in the process[225].

---

[215] Wang, Yingxu et al. 'The Formal Design Model of an Automatic Teller Machine (ATM)' (2010) 2 *IJSSCI* 102 at 103, Available at *https://www.researchgate.net/publication/220636950_The_Formal_Design_Model_of_an_Automatic_Teller_Machine_ATM*, accessed on 30 March 2023.

[216] Ibid.

[217] Dr Bansal, Kamal Mohan 'Cyber Security Issues Affecting Online Banking Transaction: A Thematic Analysis' (2020) 19 *Elementary Education Online,* 7724 at 7728, available at *https://www.ilkogretim-online.org/fulltext/218-1659017731.pdf*, accessed on 6 April 2023.

[218] Ibid

[219] Ibid.

[220] American Express 'Advantages and Disadvantages of Online Banking' available at *https://www.americanexpress.com/en-ca/business/trends-and-insights/articles/advantages-and-disadvantages-of-online-banking/*, accessed on 6 March 2023..

[221] Ibid.

[222] Ibid.

[223] Chaimaa, Belbergui et al. 'E-banking Overview: Concepts, Challenges and Solutions' (2021) 117 *Wireless Personal Communications* 1059 at 1061, available at *https://doi.org/10.1007/s11277-020-07911-0*, accessed on 6 April 2023.

[224] Ibid at 1062-3.

[225] Ibid.

The software is able to differentiate between customer service requests that can be handled automatically and those that require the assistance of a human customer service representative[226]. The host computer system of the bank is interconnected with the system, allowing remote banking customers to access additional automated services provided by the bank[227].

The route of the integration includes entering a customer banking request at a remote personnel computer from a menu of banking requests[228]. The request is then sent over a network to a host computer[229].The host computer determines the type of customer banking request and automatically logs the service request[230].The request is then compared to a table of stored request types. Each request type has a characteristic that indicates whether a customer service agent or an automated system can handle it[231]. Depending on the characteristic, the request is then routed either to a queue for handling by an agent or to a queue for processing by an automated system[232].

Online banking can also be conducted on a pre-defined home banking system. A typical home banking system comprises a program/ application on the client's device and one on the bank's computer[233]. The program acts as a communication server between the bank and the user[234]. It takes calls from the user, confirms identity, collects data, verifies digital signatures, creates digital receipts, and provides data to the user[235].

(d) Conclusion

Though electronic banking systems and electronic navigation systems serve different purposes, however, when focusing on the hardware, software, and operation of these systems, they share similarities. Both systems are computerised and integrated and depend on the connection to the network for their functions. Furthermore, from the research, both systems communicate

---

[226] Nedbank 'online banking' available at *https://personal.nedbank.co.za/bank/digital-banking/channels/online-banking.html*, accessed on 6 April 2023

[227] Islam, Salekul & Mahfuz, A S M 'Adoption of e-banking in Bangladesh: Evolution, status and prospects' (2014) *Int'l Conf. Computer and Information Technology, ICCIT 2013* 255 at 257, available at *https://www.researchgate.net/figure/The-Internet-banking-architecture_fig5_289334661*, accessed on 6 April 2023.

[228] Ibid.

[229] Ibid.

[230] Ibid.

[231] Nedbank 'online banking' available at *https://personal.nedbank.co.za/bank/digital-banking/channels/online-banking.html*, accessed on 6 April 2023.

[232] Ibid.

[233] Chovanová, Ing. Adriana 'Forms of electronic banking' (2006) 15 *BIATEC* 22 at 24, available at *https://www.nbs.sk/_img/documents/biatec/bia06_06/22_25.pdf*, accessed on 8 April 2023.

[234] Ibid.

[235] Ibid.

through a pre-defined path that connects one computer to the other, exchanging data between processors and generating outputs based on input data and analysis of such data. This communication path is mapped down and can be tracked, intercepted, and exploited if not properly secured. Therefore, both systems share similarities in operation principles.

IV Cyber security vulnerability and management of electronic banking system

(a) Background

Cybersecurity is becoming a significant concern as the world transitions to a digital revolution. The banking sector is no exception to this concern, as most of the sector's processes have long moved from traditional to digital banking, exposing the sector to cybersecurity breaches. This chapter will outline the cybersecurity vulnerabilities associated with electronic banking, focusing on ATMs and Internet banking systems.

(b) ATM cyber security vulnerabilities

ATMs are a part of our daily lives; they offer the user a convenient banking experience outside the bank at any preferred time. However, this convenience is also accessible to malicious users, making it vulnerable to physical and remote hacking.

(i) PIN card transactions vulnerability

ATMs work on two-step user verification, inserting the card and typing the Personal Identification Number (PIN). When the user inserts the card and PIN into the ATM, the ATM runs the verification process in the background, which consists of communication between the PIN Entry Device (PED) and the card[236]. This information exchange is often unencrypted and unsecured, making it a gateway for hackers to access users' information to duplicate and withdraw funds from the ATM[237].

(ii) Hardware tampering vulnerability

The ATM's designs are not fully robust; therefore, due to some weak points in design, hackers can open and alter hardware features without leaving noticeable evidence of foul play[238]. This is usually the case in ATMs not installed with anti-tempering protection, where the Chip and PIN terminals have been opened and replaced with fraudulent internal hardware that gives

---

[236] Navneet, Sharma & Dr Singh, Rathore Vijay Singh Rathore 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* 38, available at *www.jgrcs.info*, accessed on 6 October 2022.

[237] Ibid.

[238] IBM Corporation 'ATM security: Identify and fix critical flaws in machines and the connected infrastructure - Remediate exploitable vulnerabilities by understanding how attackers can compromise machines' available at *https://www.ibm.com/case-studies/large-commercial-bank?cm_sp=CTO-_-en_US-_-OYDG2REZ*, accessed on 6 October 2022.

control of the ATM transactions to the hacker, who then can steal user's information to make fake cards and gain access to their funds[239].

(iii) Skimming

ATM card skimming is amongst the popular card scams, where the hacker replaces the ATM card insertion terminal with a fraudulent one[240]. When an unsuspecting user inserts the card, the card information is digitally stolen to make fake cards and gain access to the user's funds.

(iv) Stand in time

This vulnerability is possibly caused by database maintenance, which changes ATM behaviour during 'stand in time where the bank cash dispensing network is unable to access the database containing account information'[241]. For customer convenience during this downtime, the ATM will prompt the user to allow cash withdrawal up to a certain amount, but since there is no access to the database, the ATM will not be able to get the user's account balance, potentially allowing the user to withdraw more than the available funds on the account[242].

(v) Network vulnerability attack

ATMs are continually connected to banking systems through the network connection[243]. Hackers can intercept this connection by using computer programmes (malware) to breach flawed computer software and gain control of the ATM without leaving any noticeable evidence of foul play on the ATM[244].Once the hackers gain control of the ATM, they can install their malicious software, which will allow them to have access to user's information and any other confidential information on the banking system, to use as they please[245].

(vi) Cash-out vulnerability

In an ATM cash-out attack, hackers gain access to a bank or payment card processor's systems and modify the fraud detection mechanisms[246]. This allows them to change user accounts so

---

[239] Ibid.

[240] Navneet, Sharma & Dr Singh, Rathore Vijay 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* 38, available at *www.jgrcs.info*, accessed on 6 October 2022.

[241] Ibid.

[242] Ibid.

[243] IBM Corporation 'ATM security: Identify and fix critical flaws in machines and the connected infrastructure - Remediate exploitable vulnerabilities by understanding how attackers can compromise machines' available at *https://www.ibm.com/case-studies/large-commercial-bank?cm_sp=CTO-_-en_US-_-OYDG2REZ*, accessed on 6 October 2022.

[244] Ibid.

[245] Ibid.

[246] Navneet, Sharma & Dr Singh, Rathore Vijay 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* 38. available at *www.jgrcs.info*, accessed on 6 October 2022.

that there are no restrictions on how much money can be withdrawn from ATMs in a short amount of time[247]. The hackers also frequently modify balances and withdrawal caps to allow withdrawals from ATMs until the ATMs run out of money[248].

An ATM cash-out attack is usually carefully planned and carried out. The hackers frequently acquire remote access to a card management system to change the withdrawal limits or PINs of compromised user accounts, which are fraud protection mechanisms. This is frequently accomplished by injecting malware into the systems of a financial institution or payment processor via phishing or social engineering techniques[249]. The hackers can then open new accounts, use already-existing accounts that have been compromised, and give compromised debit/credit cards to a group of persons who make coordinated withdrawals at ATMs. With influence over the card management system, hackers can modify withdrawal limits and balances to let ATM withdrawals until the cash in the machines runs out. Typically, these breaches do not take advantage of flaws in the ATM itself. The ATM is used to withdraw cash after vulnerabilities in the bank authorisation system have been exploited.

(c) Internet banking cyber security vulnerabilities

Internet/online banking is one of the most preferred banking methods due to the convenience it affords the user. Internet banking gives the user 24-hour banking services at any place of choosing. Nevertheless, it is attractive to hackers just like any other technological advancement.

(i) Denial-of-service (DoS)

This attack prevents the targeted users from using a computer resource[250].This is achieved by "flooding" a network to block authorised network traffic, breaking up connections between two computers to block access to a service or a specific person, and interrupting service to a particular system or person[251]. This attack allows the hacker to access confidential information on the bank and its clients, thereby posing considerable risk to system security because financial information might be of strategic value to the legitimate users[252].

---

[247] Navneet, Sharma & Dr Singh, Rathore Vijay 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* 38. available at *www.jgrcs.info*, accessed on 6 October 2022.
[248] Ibid.
[249] Ibid.
[250] Ghelani, Diptiben et al. 'Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking' (2022) *American Journal of Computer Science and Technology* 1 at 6. available at *http://www.sciencepublishinggroup.com/j/ajcs*, accessed on 9 April 2023.
[251] Ibid.
[252] Ibid.

(ii) Repudiation

This kind of breach is possible on programs/applications or systems which does not have controls to accurately track and log users' activities, making them vulnerable to repudiation attacks that allow for malicious manipulation or the creation of false action records[253]. Through this breach, incorrect data can be logged to log files by altering the authorising information of operations carried out by a malicious user[254]. The use of this information can be expanded to include general data modification done on behalf of others, thereby rendering the information in log files invalid[255].

(iii) Man-In-The-Middle

Man-In-The-Middle is an attack in which hackers breach an existing connection to intercept transmitted data and introduce fake information[256]. It entails monitoring connections, breaking into connections, intercepting messages, and selectively altering data[257].

(iv) Pharming

This breach is achieved by redirecting a user's internet connection to a fake website so that even when the user input address is correct, but still gets directed to the fake website[258]. This is achieved by changing the host's file on the user's device or taking advantage of the Domain Name System (DNS) server software vulnerability[259].

(v) Spoofing

Spoofing is identity theft that occurs when a person or computer effectively assumes someone else's identity by fabricating data and profiting from the situation[260].This form of breach allows the hacker to access the user's banking credentials through various mediums, e.g., emails, fake websites, SMS, etc[261].

---

[253] Vrîncianu, Marinela & Anica-Popa, Liana-Elena 'Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests' (2010) 12 *The Amfiteatru Economic Journal* 288 at 391, available at *https://core.ac.uk/download/pdf/6492899.pdf*, accessed on 9 April 2023.
[254] Ibid.
[255] Ibid.
[256] Ghelani, Diptiben et al. 'Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking' (2022) *American Journal of Computer Science and Technology* 1 at 6, available at *http://www.sciencepublishinggroup.com/j/ajcs*, accessed on 9 April 2023.
[257] Ibid.
[258] Belbergui, Chaimaa et al. 'E-banking Overview: Concepts, Challenges and Solutions' (2021) 117 *Wireless Personal Communications* 1059 at 1067, available at *https://doi.org/10.1007/s11277-020-07911-0*, accessed on 6 April 2023.
[259] Ibid.
[260] Vrîncianu, Marinela & Anica-Popa, Liana-Elena 'Considerations Regarding the Security and Protection of E-Banking Services Consumers' Interests' (2010) 12 *The Amfiteatru Economic Journal* 388 at 393, available at *https://core.ac.uk/download/pdf/6492899.pdf*, accessed on 9 April 2023.
[261] Ibid.

Conclusion

Although not comprehensive, the list mentioned above of vulnerabilities can be understood, given how similar they are to cybersecurity incidents involving marine electronic navigation systems. From the above assessment, the techniques hackers use to infiltrate electronic banking and navigation systems bear a striking resemblance. Unaware users, technicians, insecure network connections, and out-of-date hardware and software are all ways offenders obtain access. In both these systems, the infiltration is to gain an unfair advantage by manipulating the system's data, identity theft, gaining access to sensitive information, fabricating fake data, and misleading the users. Through this similarity, the author has sought to pursue benchmarking with the banking sector.

V Cybersecurity management strategies of electronic banking systems

(a) Introduction

The banking sector is a considerably bigger industry with many different national rules to follow, yet they all share a low tolerance for illicit behaviour. A summary of the cybersecurity measures of South Africa, the United Kingdom, and the United States will be given below as a sample to banking sector cybersecurity management strategies of electronic banking.

(b) Cybersecurity measures in the banking sector

(i) Common cybersecurity strategies

a) Encryption technology

Data security and privacy are paramount for financial institutions and their clients. To safeguard user information from cybersecurity risks, encryption technology has become the weapon of choice within the finance sector[262]. In addition to protecting data kept on computers and mobile devices, it secures data transported via networks, including ATM networks[263] Encryption renders personal data unreadable without the appropriate authorisation or access keys, ensuring a secure transacting line[264].

Using encryption technology in the banking sector helps protect, among other things, internet banking transactions, stop credit card fraud, and validate digital signatures when

[262] Kar, Arpan K & Dey, Supriya 'Cryptography in the Banking Industry' (2012) 1 *Business Frontiers* 1 at 2, available at *https://www.researchgate.net/publication/269405090_Cryptography_in_the_Banking_Industry*, accessed on 15 April 2023.
[263] Ibid.
[264] Ibid.

transferring money between accounts[265]. This makes encryption a crucial tool for protecting sensitive financial data from hackers who might use it to gain unfair advantage or hurt customers. Additionally, encrypting data can assist businesses in adhering to data protection laws[266].

b) Third-party cybersecurity risk management

Any risk imposed on any company or institution by external partners in its supply chain is called third-party risk[267]. These parties could be vendors, suppliers, partners, contractors, or service providers with access to confidential data, systems, or procedures belonging to the company or its customers[268].Similar to other sectors, the banking sector often relies on third-party vendors for their processes due to its advantages, e.g., cost-effective, risk reduction, regulation compliance etc[269].However, companies usually lack complete control over or full transparency into third parties' security measures[270]. Though some third-party vendors have strict security guidelines and effective risk management procedures, others fall short[271].This leaves a gap to be exploited in the supply chain and exposes the company to cybersecurity risks by giving hackers a more straightforward route to target even the most advanced security systems[272].

The usage of third parties affects the company's cybersecurity in both direct and indirect ways, making third-party risk management crucial.[273].Third-Party Risk Management (TPRM) is the procedure for evaluating and reducing risks related to outsourcing to third-party suppliers or service providers[274]. Having TPRM policies in place helps reduce cybersecurity risk in the banking sector and complies with the data protection laws[275].

---

[265] Uma, Dixit 'Cryptography – Security in E-Banking' (2017) *IOR Journals* 33 at 34-6, available at *https://www.iosrjournals.org/iosr-jbm/papers/Conf.17037-2017/Volume-2/6.%2033-37.pdf*, accessed on 15 April 2023.
[266] Ibid.
[267] *G7 Fundamental Elements for third-party cyber risk management in the financial sector* (2023). 1, available at *https://www.gov.uk/government/publications/g7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector*, accessed on 15 April 2023.
[268] Ibid.
[269] Ekran 'The importance of third-party vendor risk management for the banking industry' (2023) , available at *https://www.ekransystem.com/sites/default/files/file_resources/third-party-vendor-risk-management-for-the-banking-industry.pdf*, accessed on 15 April 2023.
[270] Ibid.
[271] Ibid.
[272] Ibid.
[273] *G7 Fundamental Elements for third-party cyber risk management in the financial sector* (2023). 1-6, available at *https://www.gov.uk/government/publications/g7-fundamental-elements-for-third-party-cyber-risk-management-in-the-financial-sector*, accessed on 15 April 2023.
[274] Ibid.
[275] Ibid.

(ii) South African approach

In South Africa, there is not a specific law governing cybersecurity yet. Instead, various pieces of law contain a jumbled collection of cybersecurity-related provisions. However, cybercrime is expressly addressed by several Electronic Communications and Transactions Act 25 of 2002 (ECTA) laws. ECTA covers every electronic transaction and data message. It makes unlawful acts involving computers like extortion, fraud, and forgery, as well as unauthorised access to, interception of, or interference with data, among other things, punishable by law[276]. The Regulation of Interception of Communications and Provision of Communication-related Information, Act 70 of 2002 (RICA), is a piece of legislation that, among other things, aims to control the interception of particular communications. Interception of direct and indirect communications is generally forbidden under RICA[277]. The Criminal Procedure Act (CPA) of 1977, which is South Africa's primary law governing criminal investigations and prosecutions, includes provisions for investigating and prosecuting cybercrimes[278]. The Protection of Personal Information Act of 2013 (POPIA) promotes the protection of personal data processed by public and private entities. It introduces several restrictions to set minimum standards for such processing[279].

The South African banking sector also follows the Financial Intelligence Centre Act (FICA) and the Know Your Client policy (KYC)[280]. Although the primary goals of FICA at the time it was implemented were to combat terrorism, money laundering, and tax evasion offences, FICA, on the other hand, is a legal framework established to assist in identifying the proceeds of illegal operations[281]. Then, any further criminal activity targeted at the financial industry is implicitly included. Banks must adhere to the absolute minimum-security standards set forth by FICA to operate legally. To consistently research new methods to ensure users may conduct safe banking, this includes all assets tied to the bank[282]. For instance, banks have

---

[276] Electronic Communications and Transactions Act 25 of 2002, available at *https://www.gov.za/sites/default/files/gcis_document/201409/a25-02.pdf*, accessed on 8 October 2022.
[277] Regulation of Interception of Communications and Provision of communication-related Information Act 70 of 2002, available at *https://www.gov.za/sites/default/files/gcis_document/201409/a70-02.pdf*, accessed on 8 October 2022.
[278] Criminal Procedure Act 51 of 1977, available at https://www.gov.za/sites/default/files/gcis_document/201503/act-51-1977s.pdf, accessed on 8 October 2022.
[279] Protection of Personal Information Act 4 of 2013, available at https://www.gov.za/sites/default/files/gcis_document/201409/3706726-11act4of2013popi.pdf, accessed on 8 October 2022.
[280] Financial Intelligence Centre Act 28 of 2001 (as amended), available at *https://www.gov.za/sites/default/files/gcis_document/201409/a38-010.pdf*, accessed on 8 October 2022.
[281] Ibid.
[282] Ibid.

developed innovative ATM transactions to enable cardless transactions, preventing the offenders from accessing user information and addressing the vulnerability of PIN card transaction skimming and other similar crimes[283].

The verification process has also become more stringent, requiring not just the PIN or ID numbers but also phone confirmations, fingerprints, and eye and voice recognition. This enables the user to be informed in the event of a breach of the account and to be able to mitigate or neutralise the loss that would follow the breach[284].

Additionally, the banking industry ensures that all workers receive regular training, ensuring they are all knowledgeable on risk management and relevant laws. They also endeavour to train users to ensure risk management and reduce vulnerabilities[285].Furthermore, they collaborate with others in the industry to stay informed about the most recent security flaws criminals are trying to exploit. By doing this, they may develop new risk-management techniques and offer their customers secure banking services[286].

Annual audits of FICA compliance are conducted to verify compliance and those who fail to comply risk losing their certification and being unable to continue operating until the problem is resolved. [287].

In addition, a Cybercrime Act 19 of 2020 has been enacted to target any threats that are related to the internet. The Cybercrimes Act is a significant statute that governs cybercrime in South Africa. It makes, among other things, the following types of online offences punishable by law and include a number of comprehensive provisions addressing cybercrime: 'Unlawful access to data, a computer program, a computer data storage medium or a computer system; unlawful interception of data; the unlawful and intentional use or possession of software and hardware tools in committing cybercrimes; cyber fraud; cyber extortion; cyber forgery and uttering; and malicious communications'[288].

The Cybercrimes Act also includes provisions dealing with, among other things, cybercrime investigation, state-to-state mutual assistance, and reporting obligations for

---

[283] Nedbank 'How to withdraw at an ATM' available at *https://personal.nedbank.co.za/bank/digital-banking/needs/payments/cardless-withdrawls/withdraw-money-at-an-atm.html*, accessed on 8 October 2022.
[284] Ibid
[285] Nedbank 'Fraud awareness and prevention: Your guide to beating fraud' (2023) *Nedgroup Investments*, 1 at 3-25, available at *https://www.nedgroupinvestments.co.za/content/dam/NGISingleSiteContent/pdfs/FRAUD%20AWARENESS%20BOOKLET%202022%20RISK%20VERSION.pdf*, accessed on 16 April 2023.
[286] Financial Intelligence Centre Act 38 of 2001 (as amended), available at *https://www.gov.za/sites/default/files/gcis_document/201409/a38-010.pdf*, accessed on 8 October 2022.
[287] Ibid.
[288] Republic of South Africa Cybercrimes Act 19 of 2020, available at *www.gpwonline.co.za*, accessed on 8 October 2022.

electronic communications service providers and financial institutions[289]. Electronic communications service providers and financial institutions must report to the South African Police Service (SAPS) any cybercrime offences that they become aware of, as soon as possible and, if possible, within 72 hours. This includes offences that are committed using their computer systems[290]. This will undoubtedly be a game changer in the fight against cyber security breaches, not just in the banking sector but in all cyber-related activities.

(iii) United States (US) approach

The banking industry in the United States has made significant progress in addressing cybersecurity breaches, both nationally and among state financial regulators. One example of this progress is the New York Department of Financial Services (NY DFS) cybersecurity requirements, which went into effect on March 1, 2017[291]. These requirements mandate that banks, insurance companies, and other financial services institutions under the NY DFS's jurisdiction establish and maintain a cybersecurity program designed to protect customer information and IT systems[292]. Among the requirements proposed for regulated financial institutions are the following: 'Establishment of a cyber-security program; adoption of a written cyber-security policy; designation of a Chief Information Security Officer responsible for implementing, overseeing and enforcing the new program and its policy; annual penetration testing and bi-annual vulnerability assessments of an entity's information system; maintenance of audit trails to detect and respond to cybersecurity events, limitation and regular review of user access privileges, encryption of Non-public information; establishment of an incident response plan; establishment of security policy for the third-party service provider'[293].

Because of this regulation, every company is required to conduct an analysis of the risks that are unique to their business and devise a plan to effectively mitigate those risks[294]. This matter needs to be taken very seriously by senior management, which also needs to take responsibility for the cybersecurity programme of the organisation and submit an annual certification confirming that it complies with these regulations. The cybersecurity programme

---

[289] Ibid.
[290] Ibid.
[291] *23 NYCRR 500* (2017), available at *https://www.governor.ny.gov/sites/default/files/atoms/files/Cybersecurity_Requirements_Financial_Services_23 NYCRR500.pdf*, accessed on 8 October 2022.
[292] Ibid.
[293] Ibid.
[294] Ibid.

of a regulated entity is required to protect the institution's safety and soundness as well as the customers of the entity[295].

Furthermore, US financial institutions must follow the Bank Secrecy Act (BSA)[296]. The (BSA), similar to the South African FICA, was enacted in order to better identify instances in which money laundering is used to further a criminal enterprise, support terrorism, cover up tax evasion, or conceal other illegal activities[297].

An advisory was published by the Financial Crimes Enforcement Network (Fin-CEN) of the United States Treasury Department in order to assist financial institutions in better comprehending their responsibilities under the Bank Secrecy Act (BSA) in regards to cyber-crime and cyber-enabled events[298]. This advisory also discusses the ways in which reporting mandated by the BSA helps authorities in the United States combat cyber events and crime that is enabled by the internet[299].

FinCEN guides financial institutions through this advisory on: 'Reporting cyber-enabled crime and cyber-events through Suspicious Activity Reports (SARs); including relevant and available cyber-related information (e.g., Internet Protocol (IP) addresses with timestamps, virtual-wallet information, device identifiers) in SARs; collaborating between BSA/Anti-Money Laundering (AML) units and in-house cyber-security units to identify suspicious activity; and sharing information, including cyber-related information, among financial institutions to guard against and report money laundering, terrorism financing, and cyber-enabled crime'[300].

The Federal Banking Agencies (FBAs) took a similar approach to FinCEN when they issued an Advanced Notice of Proposed Rulemaking (ANPR) to establish enhanced cybersecurity standards[301].

The list continues according to different states, agencies, and jurisdictions, each with compelling regulations, strategies, and guidelines for the financial sector to combat cybersecurity-related crimes.

---

[295] Ibid

[296] Comptroller's Handbook: Bank Secrecy Act/Anti-Money Laundering (2000). available at https://www.hsdl.org/?view&did=439815, accessed on 8 October 2022.

[297] Ibid.

[298] Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime FIN-2016-A005 (2016). available at https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf, accessed on 8 October 2022.

[299] Ibid.

[300] Ibid.

[301] Enhanced Cyber Risk Management Standards: Joint advance notice of proposed rulemaking Docket No. R-1550 (2016). available at *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf*, accessed on 8 October 2022.

(iv) United Kingdom (UK) Approach

On 25 May 2018, the UK General Data Protection Regulation (GDPR) was enacted. The GDPR, among other things, significantly increases the accountability of all organisations that process personal data, significantly broadens the scope of individuals' data rights, and mandates that data controllers and processors put in place adequate and proportionate organisational and technical safeguards to protect personal data[302].

In addition, data subjects have the right to an efficient legal remedy against data controllers and processors in the event that they believe their rights have been infringed upon as a result of processing that does not adhere to the regulation[303]. This right is granted to them in the event that they believe their rights have been violated as a result of processing that[304].

Organisations must comply with the regulation's requirements for data processing and be able to prove it. Companies can show their clients that they are dependable and responsible by implementing an effective compliance strategy that helps them avoid costly fines and reputational harm.[305].

The Financial Conduct Authority (FCA) and the Bank and the Prudential Regulation Authority (PRA) jointly issued the final regulations and policies in March 2021[306]. The regulations are applicable to institutions that have been authorised and registered in accordance with the Payment Services Regulations of 2017 and the Electronic Money Regulations of 2011, including but not limited to 'banks, building societies, insurance companies, PRA-designated investment firms, recognised investment exchanges, enhanced scope senior managers, and certification regime firms'[307]. The regulations and guidelines that were intended to improve the operational resilience of the financial sector went into effect on March 31st, 2022. Companies now have until no later than March 31st, 2025 to begin operating within their impact tolerances[308].

FCA defines Operational resilience as 'the ability of firms, financial market infrastructures and the financial sector to prevent, adapt and respond to, recover and learn from operational disruption'[309].

---

[302] Data Protection Act 2018 available at *https://www.legislation.gov.uk/ukpga/2018/12/enacted/data.pdf*, accessed on 10 October 2022.
[303] Ibid.
[304] Ibid.
[305] Ibid.
[306] Building operational resilience: Feedback to CP19/32 and final rules 2021 available at *https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf*, accessed on 10 October 2022.
[307] Ibid.
[308] Ibid
[309] Ibid

VI Conclusion

The above list is only an abstract for illustration purposes within the scope of the dissertation; however, the increasing number of cyberattacks directed at the financial industry has resulted in the establishment of a number of mandatory cybersecurity regulations. One of the most efficient methods for holding financial services accountable for their level of security is to ensure that they are following applicable regulations. However, it is not only through compulsion that the banking sector thrives but also through technological advancements and voluntary cybersecurity awareness campaigns. Because this sector has been dealing with cybersecurity breaches since the dawn of technological evolution, it is only natural that it would be an ideal candidate for benchmarking for an industry new to cybersecurity threats, such as shipping.

This is not to say that the financial services sector has defeated this threat, but rather that it has survived and grown in the face of relentless cyber-attacks through collaborative efforts, information sharing, training, innovative cybersecurity management strategies and strict compliance regimes. Regarding cybersecurity threats in the maritime sector, these are areas of improvement. Therefore, the maritime industry can benefit from the finance sector's experience with cybersecurity threats and improve where they fall short.

CHAPTER 6 MARITIME INDUSTRY STATE OF READINESS IN RELATION TO BANKING SECTOR STATE OF READINESS

I Introduction

The maritime and banking sectors are two of the most important and critical industries in the world. They are also two of the most vulnerable to cybersecurity breaches as both sectors rely on complex and interconnected networks[310]. The maritime sector relies on a network of ships, ports, and other infrastructure to transport goods and people around the world. The banking sector relies on a network of banks, financial institutions, and other infrastructure such as payment systems and data centres, to process financial transactions and provide financial services to businesses and individuals around the world. Both networks are complex and interconnected, using network of computers, servers and other devices which makes them vulnerable to cyberattacks.

Furthermore, both sectors store sensitive data. The maritime sector stores data on ships, cargo, and passengers. The banking sector stores data on customers, accounts, and transactions[311]. This sensitive data is a valuable target for hackers. Additionally, both sectors are increasingly reliant on technology. The maritime sector is increasingly using technology to improve safety, efficiency, and productivity. The banking sector is also increasingly using technology to provide new services and products to customers[312]. This increased reliance on technology makes both sectors more vulnerable to cyberattacks[313].

The research has shown the similarities between the shipboard electronic navigation systems and the electronic banking systems. In the maritime sector, electronic navigation systems are used to control and monitor ships. These systems are often interconnected with other systems, such as the ship's propulsion system, cargo handling system, and communications system[314]. In the banking sector, electronic banking systems are used to process payments, manage accounts, and provide other financial services. These systems are also often interconnected with other systems, such as the bank's customer relationship management system, fraud detection system, and risk management system[315]. This interconnection of systems creates a larger attack surface for cyber attackers. This is because there are more potential entry points for attackers to exploit. For example, if one system is not

---

[310] See chapter 2 and 5 of this dissertation
[311] Ibid.
[312] Ibid.
[313] Ibid.
[314] Ibid.
[315] Ibid.

properly secured, attackers can use it to gain access to other systems[316]. However, though both sectors share similarities in their processes, their state of readiness against cybersecurity breaches differs due to several factors highlighted below.

II Banking and maritime sector relative state of readiness

(a) Background

What sets the banking sector apart from the maritime sector is that it has been a target for cyber-attacks for many years, and as shown in this study, they have developed some of the most robust cyber security measures in the world. Based on the comparison of cybersecurity risk management strategies for the two industries discussed in this study, it has been determined that the following are some of the reasons why the banking industry is further along in cyber security management strategies than the maritime sector:

(b) Attack history

Because the banking industry has more experience dealing with cybersecurity breaches, more sophisticated security measures to protect their customers' data have been developed. The maritime industry, on the other hand, has only recently begun to recognise the significance of cybersecurity breaches, and as a result, it has not had to invest as heavily in cyber security.

(c) Regulations

Due to many years in the fight against cybersecurity breaches, the banking sector has become heavily regulated, and these regulations often require banks to implement certain cybersecurity measures. The maritime sector, on the other hand, is still at the beginning phases in its fight against cybersecurity breaches, as a result, still lacks cybersecurity regulations.

(d) Resources

The banking sector has more resources at their disposal than the maritime sector, and these resources can be used to invest in cyber security. The maritime sector, on the other hand, has fewer resources, and as a result, they may not be able to invest as much in cyber security.

(e) Culture

The banking sector has a strong culture of cyber security, and this culture is often driven by the need to protect customer data. The maritime sector has, for decades, enjoyed the protection of isolation and have not been exposed to cybersecurity breaches.

---

[316] See cybersecurity vulnerabilities in chapter 2 and 5 of this dissertation.

It is through this rationale that it is believed that the maritime sector can learn a lot from the banking sector when it comes to cyber security management strategies and take advantage of what the banking sector have tried and perfected. This way, the maritime sector will use what limited resources it has on strategies that are guaranteed to work.

III Banking sector strategies that might be used by maritime sector

(a) Introduction

There are some strategies employed in banking sector that the maritime sector might consider implementing. It is believed that for an industry that is resource-constrained, it might be beneficial to adopt and improve upon what has already been tried and tested. Therefore, using the little resources available to finding suitable ways to implement these strategies in their respective organisations rather than re-inventing the wheel.

(b) Implement a zero-trust security model.

Through the Data protection regulations and cybersecurity/ fraud awareness campaigns, the banking sector has implemented a zero-trust security model which assumes that no one is trusted by default, not even the banks employees[317]. This means that all traffic, whether it is from an internal or external source, is subject to scrutiny. This helps to prevent attackers from gaining access to sensitive data or systems. Electronic navigation systems are often intercepted by hackers assuming identities of coastal stations, ships, or service providers[318]. With a zero-trust model, identity theft would be minimised.

(c) Use multi-factor authentication.

This tool adds an extra layer of security by requiring users to provide two or more forms of identification before they can gain access to a system. This makes it much more difficult for attackers to gain access to accounts, even if they have stolen a user's password[319].

(d) Keep software up to date/ Encryption technology:

Outdated software is one of the issues found on shipboard electronic navigation systems, making them susceptible to cybersecurity breaches[320]. Software updates often include security

---

[317] In South Africa, the Financial Sector Conduct Authority (FSCA)'s requires banks to have a comprehensive cybersecurity program in place which includes a number of principles that are consistent with a zero-trust approach, such as least privilege, micro segmentation, and continuous monitoring. Another example is the New York State Department of Financial Services (NYDFS) Cybersecurity Regulation which includes a number of requirements that are consistent with a zero-trust model, such as continuous monitoring, vulnerability remediation, and incident response. See chapter 5 of this dissertation.

[318] See electronic navigation systems cybersecurity vulnerabilities in chapter 2 of this dissertation.

[319] Nedbank 'Security is a top priority for Nedbank electronic banking channels' available at *https://businessbanking.nedsecure.co.za/download.aspx?tp=302&id=124,* accessed on 6 April 2023.

[320] See chapter 2 of this dissertation.

patches that can help to protect systems from known vulnerabilities that can be exploited by attackers. When software vendors release updates, they typically include fixes for security vulnerabilities that have been discovered. In addition to fixing known vulnerabilities, software updates can also include new features and functionality that can help to improve security. For example, new security features may be added to software that can help to prevent attacks or detect malicious activity.

(e) Educate employees about cyber security

Employees are often the weakest link in a company's cyber security defences. They may click on phishing links, open infected attachments, or use weak passwords. This is even a bigger threat at sea due to the use of common network point for private and ships operation use. It is important to educate employees about cyber security risks and how to protect themselves and the company from attack.

(f) Implementing a risk assessment

A risk assessment can help to identify the maritime sector's most critical assets and the threats that they face. This information can be used to develop and implement appropriate security measures. Risk assessments models have been developed within the sector, however, without implementation they are not useful.

(g) Having a plan in place for responding to a cyber-attack

A cyber-attack can have a significant impact on any company's operations. It is important to have a plan in place for responding to a cyber-attack so that the company can minimise the damage and recover as quickly as possible. From the reported incidents in the maritime sector, it has been evident that the companies did not expect these attacks and as a result had no response plan in place[321]. In a very fast paced industry there is no room for undue delays.

(h) Working with partners:

The maritime sector is a global industry, and cyber-attacks can come from anywhere. It is important to work with partners, such as shipping companies, ports, service providers and governments, to improve cyber security across the industry.

(i) Manage third-party risk:

The maritime sector relies on a wide range of third-party vendors for a variety of services, including IT services, technician, manufacturers, logistics, and transportation. These third-party vendors may have access to sensitive data such as shipping data, route etc. or critical

[321] See table of cases in Appendix B.

navigation equipment. If a third-party vendor is compromised, this sensitive data could be exposed. The maritime industry can reduce the risks associated with third-party vendors and safeguard its vital infrastructure from cyber security breaches by implementing third party risk management strategies.

IV Possible challenges in implementation of cybersecurity strategies in maritime sector

It must be conceded that not all banking sector strategies can be adopted by the maritime sector. Though the sectors share similarities in the electronic systems, there are differences between the maritime and banking sectors when it comes to cybersecurity. For example, the maritime sector is more geographically dispersed than the banking sector and consist of a wide range of actors, including ship owners, operators, and ports. This can make it difficult to coordinate cybersecurity efforts and to ensure that all actors are taking the necessary precautions. Therefore, creating a challenge in implementing and enforcing consistent cybersecurity measures. Additionally, the maritime sector is more reliant on third-party vendors than the banking sector. This makes it more difficult for the maritime sector to control its cybersecurity risks.

V Conclusion

Despite these differences the similarities between the two sectors are such that there are reasons to believe that the maritime sector could profitably consider using at least some of the banking sector strategies together with what has been proposed and developed by industry experts to improve its cybersecurity position to the degree that it can be said, with minor exceptions, that it is ready for the fight against cybersecurity breaches.

CHAPTER 7 CONCLUSION

Once considered conservative and conventional, the maritime industry has become connected and accessible[322]. Over the years ships has evolved, employing state-of-the-art equipment that operates independently and capable of running the ship with minimal human interface[323]. This evolution and overreliance on technology has brought with it newfound threats and exposure[324]. It is without a doubt that technology simplifies onboard navigation and reduces human error-aided incidents. However, the industry must ensure readiness in all aspects of this evolution.

This study was set to review the industry's readiness in the fight against cybersecurity breaches while covering possible cybersecurity vulnerabilities posed by modern-day shipboard electronic navigation systems and highlighting possible shortfalls. In addition, the study highlighted the need to venture outside the industry parameters to extract knowledge from those who have been in this fight longer than the industry, not only to learn from their victories but also their failures to avoid succumbing to the same fate.

It has been argued that cybersecurity risks have continued to evolve to the point that attacks that were once not considered to be possible are now occurring more frequently. From the cybersecurity vulnerability assessment conducted, the root causes were identified as increased exposure to the Internet of Things, lack of awareness, outdated systems, unsecured connections, high incentives for attackers, etc. There is a need for innovative asset protection strategies to mitigate these risks. The scope of these strategies will need to go beyond the borders of the ships and include all parties rendering any service to the ships.

It is evident from the research that technological innovations in the industry will continue to progress as the years pass; therefore, cybersecurity risks should be expected to follow the same trend. To prevent an upward curve in cyber security breaches, the industry must safeguard against present and future threats. The reason for this emphasis is that looking at the technology forecast, which involves autonomous vessels on cross-ocean voyages, soon the industry will not only have to concern itself with human error and complexity of the technology for the average seafarer but the systems connectivity reliability as well. Therefore, the industry must be ready when that time comes.

---

[322] See chapter 1 of this dissertation.
[323] See chapter 2 of this dissertation.
[324] Ibid.

Cyberspace is undoubtedly the most valuable tool as it provides cost-effective, far-reaching connectivity at a very fast pace. Its benefits to the industry cannot be overlooked; however, the challenges that come with it cannot be ignored.

During the industry cybersecurity risk management review, it was established that the IMO officially recognised '… the urgent need to raise awareness on cyber threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks'[325]. Thus, the IMO sees 'Maritime Cyber Resilience' as key to improving maritime cyber security[326]. The IMO further provided the Guidelines on Cyber Risk Management[327], that provided high-level recommendations for maritime cyber risk management and included functional elements to mitigate cyber risks. The IMO urged ship owners to implement a cybersecurity risk management approach, which is meant to be resilient against cybersecurity risks. However, it became apparent that more is still needed to reach the readiness status against cybersecurity breaches. Expecting the readiness to be achieved by the efforts of the IMO and the likes alone is unrealistic. Cybersecurity challenges go beyond the borders and jurisdictions of any single regulatory body or State, and it will therefore require collaboration from all industry stakeholders to get ahead of this fight.

The benchmarking exercise conducted in this study revealed a link between vulnerabilities and attack strategies for electronic systems used in the industry and banking. Therefore, the tools for fighting against cybersecurity breaches are already available, which means the industry does not need to reinvent the wheel. However, the challenge of feasibility and implementation cannot be ignored. If these gaps remain, the strategies and the tools available will not matter much. The research has shown that the banking industry primarily relies on strict regulations to incentivise compliance. However, it may take time for the maritime industry to build up to that point.

Meanwhile, the common ground needs to be reached on guaranteeing cybersecurity risk management strategies implementation. Incentives have proven to be the best policy for

---

[325] International Maritime Organisation *Maritime Cyber Risk Management in Safety Management systems* (2017) 1. available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents,* accessed on 6 December 2021.
[326] Ibid.
[327] International Maritime Organisation *Guidelines on maritime cyber security risk management* (2017) 1 at 4, available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents,* accessed on 6 December 2021.

ensuring implementation. It is assumed that using the same strategy for cybersecurity risk management would achieve the desired effect.

The vulnerabilities discussed in this study are only abstract and maybe, in retrospect, to recent cybersecurity breaches, as they only comprise the few cases that made it to public knowledge. However, more significant challenges could be hidden beneath the surface like an iceberg. Therefore, it is to the industry's benefit to ensure readiness against cybersecurity breaches by coming together.

APPENDIX A

Table 4. ECDIS cyber vulnerabilities computationally detected and assigned with the critical risk factor.

	Vulnerability	Description	Risk Factor	Possible Solution*
1.	MS Windows XP unsupported	Support for this operating system by the vendor (Microsoft) ended 8 April 2014. Lack of support implies that no new security patches for the product are released by the vendor. In addition, the vendor is unlikely to investigate or acknowledge reports of vulnerabilities.	Critical	Upgrade to a version of operating system that is currently supported
2.	Unsupported Windows operating system	The version of operating system is missing a service pack. As a result, it is likely to contain security vulnerabilities.	Critical	Upgrade to a supported service pack
3.	Vulnerability in SMB could allow remote code execution	The version of the operating system contains a flaw in the Server Message Block (SMB) service implementation that may allow an attacker to execute arbitrary code on the remote host. An attacker does not need to be authenticated to exploit this flaw.	Critical	Vendor has released a set of patches for the operating system.
4.	Vulnerability in Server service could allow remote code execution	The ECDIS is vulnerable to a buffer overrun in the Server service that may allow an attacker to execute arbitrary code on the ECDIS with ultimate privileges.	Critical	Vendor has released a set of patches for the operating system.
5.	Server service crafted Remote Procedure Call (RPC) request handling remote code execution	The ECDIS is affected by a remote code execution vulnerability in the Server service due to improper handling of RPC requests. An unauthenticated, remote attacker can exploit this, via a specially crafted RPC request, to execute arbitrary code with ultimate privileges.	Critical	Vendor has released a set of patches for the operating system.
6.	SMB vulnerabilities remote code execution	The ECDIS is affected by a memory corruption vulnerability in SMB that may allow an attacker to execute arbitrary code or perform a denial of service against the ECDIS.	Critical	Vendor has released a set of patches for the operating system.
7.	Security update for SMB service	The ECDIS is affected by multiple vulnerabilities: • Multiple remote code execution vulnerabilities exist in SMBv1 service. An unauthenticated, remote attacker can exploit these vulnerabilities to execute arbitrary code. • An information disclosure vulnerability exists in SMBv1 service. An unauthenticated, remote attacker can exploit this to disclose sensitive information.	Critical	Vendor has released a set of patches for the operating system.

*Implementation of the possible solution is to be conducted by the ECDIS equipment manufacturer.

APPENDIX B

Year	Incident	Details
2019	Navigation systems spoofing in the Strait of Hormuz	A British oil tanker, the Stena Impero, was seized by Iranian forces after the ship was spoofed into changing course into Iranian waters[328].
2019	Malware on a U.S vessel	In February 2019, a deep draft vessel on an international voyage bound for the Port of New York and New Jersey reported that they were experiencing a significant cyber incident impacting their shipboard network[329].
2018	ECDIS infected by virus	A vessel ECDIS was infected by a virus which resulted in undue delay on sailing schedule[330].
2017	Ships in Novorossiysk	At least 20 ships in the Black Sea were reporting false data was being transmitted, indicating the ships were 32 km inland of their actual position. It is

[328] Iphar, Clément et al 'An expert-based method for the risk assessment of anomalous maritime transportation data' (2020) 104 *Applied Ocean Research* 1 at 4, available at *https://doi.org/10.1016/j.apor.2020.102337*, accessed on 6 July 2022.

[329] U.S Coast Guards '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 on 6 July 2022.

[330] BIMCO *Guidelines on cyber security onboard ships* 4 ed (2021) 1 at 11. available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

		now believed to have been as a result of a GNSS spoofing attack[331].
2013	Experiment on a Yacht	GPS spoofing attack by a research team at the University of Texas on a Yacht[332].
2008-2018	Illegal fishing activities	M/v Andrej Longov/Sea Breez1/Ayda/STS-50 committed identity fraud by repeatedly falsifying her registry, producing multiple fake signals, and appearing in nearly 100 different locations simultaneously[333].

[331] Kapalidis, Polychronis 'Cybersecurity at sea' in Otto, Lisa (ed) *Global Challenges in Maritime Security* (2020), 142. available at *https://doi.org/10.1007/978-3-030-34630-0*, accessed on 1 February 2022.
[332] Brian Dodson 'University of Texas team takes control of a yacht by spoofing its GPS' available at *https://newatlas.com/gps-spoofing-yacht-control/28644/*, accessed on 7 February 2022.
[333] Iphar, Clément et al 'An expert-based method for the risk assessment of anomalous maritime transportation data' (2020) 104 *Applied Ocean Research* 1 at 4, available at *https://doi.org/10.1016/j.apor.2020.102337*, accessed on 6 July 2022.

BIBLIOGRAPHY

Legislation

South Africa

Cybercrimes Act 19 of 2020
Criminal Procedure Act 51 of 1977
Electronic Communications and Transactions Act 25 of 2002
Financial Intelligence Centre Act 38 of 2001
Protection of Personal Information Act 4 of 2013
Regulation of Interception of Communications and Provision of communication-related information Act 70 of 2002

United Kingdom

Data Protection Act 2018, c. 12.

United States

Acts

Bank Secrecy Act of 1970

Regulations

New York Cybersecurity Regulation (23 NYCRR part 500) 2017

International Conventions

International Convention on the Safety of Life at Sea, 1974.

Guidelines

Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime FIN-2016-A005 (2016), available at *https://www.fincen.gov/sites/default/files/advisory/2016-10-25/Cyber%20Threats%20Advisory%20-%20FINAL%20508_2.pdf*, accessed on 8 0ctober 2022.

American Bureau of Shipping (ABS) Guidance Notes on Data Integrity for Marine and Offshore Operations—ABS CyberSafety (2016) Houston, TX, USA, American Bureau of Shipping (ABS), available at *https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/252_cybersafetyV3/CyberSafety_V3_Data_Integrity_GN_e.pdf*, accessed on 6 December 2021.

American Bureau of Shipping (ABS) Guidance Notes on Software Provider Conformity Program—ABS Cyber Safety (2016) Houston, TX, USA, American Bureau of Shipping (ABS), available at *https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/254_cybersafetyV5/CyberSafety_V5_SPCP_GN_e.pdf*, accessed on 6 December 2021.

American Bureau of Shipping (ABS) Guide for Software Systems Verification—ABS CyberSafety (2016) Houston, TX, USA, American Bureau of Shipping (ABS), available at *https://ww2.eagle.org/content/dam/eagle/rules-and guides/current/other/253_cybersafetyV4/CyberSafety_V4_SSV_Guide_e.pdf*, accessed on 6 December 2021.

American Bureau of Shipping (ABS) Guidance Notes on the Application of Cybersecurity Principles to Marine and Offshore Operations—ABS Cyber Safety (2016) Houston, TX, USA, ABS, available at *https://ww2.eagle.org/content/dam/eagle/rules-and-guides/current/other/250_cybersafetyV1/CyberSafety_V1_Cybersecurity_GN_e.pdf*, accessed on 6 December 2021.

American Bureau of Shipping (ABS) Guide for Cybersecurity Implementation for the Marine and Offshore Industries—ABS CyberSafety (2016) Houston, TX, USA, American Bureau of Shipping (ABS), available at *https://ww2.eagle.org/content/dam/eagle/rules-and-guides/archives/other/251_cybersafetyV2/CyberSafety-V2-Cybersecurity-Guide-June18.pdf*, accessed on 6 December 2021.

BIMCO Guidelines on cyber security onboard ships 4 ed (2021), available at *https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships*, accessed on 6 December 2021.

Building operational resilience: Feedback to CP19/32 and final rules (2021), available at *https://www.fca.org.uk/publication/policy/ps21-3-operational-resilience.pdf*, accessed on 10 October 2022.

Det Norske Veritas-Germanischer Lloyd Cyber Security Resilience Management for Ships and Mobile Offshore Units in Operation (2016) Oslo, Norway, available at *https://www.dnv.com/news/dnv-gl-launches-recommended-practice-to-enhance-the-cyber-security-of-maritime-assets-74585*, accessed on 6 December 2021.

International Maritime Organisation Guidelines on maritime cyber security risk management (2017), available at *https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents*, accessed on 6 December 2021.

International Maritime Organisation Maritime Cyber Risk Management in Safety Management systems (2017), available at https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf, accessed on 6 December 2021.

Lloyd's Register Cyber-Enabled Ships—Deploying Information and Communications Technology in Shipping—Lloyd's Register's Approach to Assurance (2016) London, UK, Lloyd's Register, available at *https://www.lr.org/en/latest-news/early-adopters-and-innovators-in-connected-assets-on-ships/*, accessed on 6 December 2021.

International Association for Classification Societies (IACS) Recommendation on Cyber Resilience Recommendation No. 166 (2020), available at *https://www.iacs.org.uk/publications/recommendations/161-180/rec-166-new-corr1*, accessed on 6 December 2021.

International Association of Independent Tanker Owners (INTERTANKO) Jamming and Spoofing of Global Navigation Satellite Systems (GNSS) (2019), available at *https://www.maritimeglobalsecurity.org/media/1043/2019-jamming-spoofing-of-gnss.pdf*, accessed on 6 March 2023.

Revised Guidelines for the onboard operational use of shipborne Automatic Identification Sytems (AIS) (2015), available at *https://edocs.imo.org/Final Documents/English/A 29-J-62 - RES.1106 (E).doc*, accessed on 2 February 2023.

SAMSA Cyber Security (Marine Notice No 18 of 2017). available at www.samsa.org.za, accessed on 1 February 2022.

Standards

Enhanced Cyber Risk Management Standards: Joint advance notice of proposed rulemaking Docket No. R-1550 (2016), available at *https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20161019a1.pdf*, accessed on 8 October 2022.

Federal Aviation Administration, USA. *Global Positioning System Wide Area Augmentation System (WAAS) performance standard* (2008) Department of Transportation, USA, available at *http://www.nstb.tc.faa.gov/*, accessed on 6 February 2023.

International Organization for Standardization/ International Electrotechnical Commission standard ISO/IEC 27001 Information technology — Security techniques — Information security management systems — Requirements (2013) Switzerland International Organization for Standardization, available at *http://www.itref.ir/uploads/editor/42890b.pdf*, accessed on 6 December 2021.

National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (2018), available at *https://doi.org/10.6028/NIST.CSWP.04162018*, accessed on 6 December 2021.

Revised performance standards for Electronic Chart Display and Information Systems (ECDIS) (2022), available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.232(82).pdf*, accessed on 6 March 2023.

Revised performance standards for RADAR equipment (2004), available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.192(79).pdf*, accessed on 8 February 2023.

Revised performance standards for shipborne Global Positioning System(GPS) receiver equipment (2000), available at *https://wwwcdn.imo.org/localresources/en/KnowledgeCentre/IndexofIMOResolutions/MSCResolutions/MSC.112(73).pdf*, accessed on 6 February 2023.

Books

Bole A G et al *Radar, and ARPA Manual: Radar and Target Tracking for Professional Mariners, Yachtsmen and Users of Marine Radar* 2 ed (2005).

Furuno *Class A AIS Operator's manual* (2015).

Hajera, Fatima 'E-Banking System Benefits and Issues' in Dr. Kaustubha Nand Bhatt (ed) *Insights into Economics and Management* Vol 11 (2021).

Kapalidis, Polychronis 'Cybersecurity at sea' in Otto Lisa (ed) *Global Challenges in Maritime Security*. *Advanced Sciences and Technologies for Security Applications* (2020).

Kavallieratos, Georgios et al. 'Cyber-Attacks Against the Autonomous Ship' in Sokratis K. Katsikas, et al (eds) *Computer Security. SECPRE2018 CyberICPS2018. Lecture Notes in Computer Science* (2019).

Lehto, Martti 'Cyber Security in Aviation, Maritime and Automotive' in Diez Pedro et al (eds) *Computation and Big Data for Transport. Computational Methods in Applied Sciences* vol 54 (2020).

Journal articles

Androjna, Andrej et al 'AIS Data Vulnerability Indicated by a Spoofing Case-Study' (2021) 11 *Applied science* 1 at 9, available at *https://doi.org/10.3390/app11115015*, accessed on 11 July 2022.

Androjna, Andrej et al 'Assessing Cyber Challenges of Maritime Navigation' (2020) *Journal of Marine Science and Engineering* 1 at 3, available at *https://www.mdpi.com/journal/jmse*, accessed on 9 July 2022.

Bielawski, Antoni & Lazarowska, Agnieszka 'Discussing cybersecurity in maritime transportation' (2022) 4 *Maritime Technology and Research* 1, available at *https://doi.org/10.33175/mtr.2022.252151*, accessed on 7 February 2022.

Bolbot, Victor et al. 'A novel cyber-risk assessment method for ship systems' (2020) 131 *Safety Science* 1-2, available at *https://www.elsevier.com/locate/safety*, accessed on 1 February 2022.

Bueger, Christian 'What is maritime security?' (2015) 53 *Marine Policy* 159 at 160-1, available at *www.elsevier.com/locate/marpol*, accessed on 1 February 2022.

Caprolu, Roberto Di Pietro Maurantonio et al 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead' (2020) *Division of Information and Computing Technology* 1 at 4, available at *https://www.researchgate.net/publication/342965489*, accessed on 2 February 2022.

Chaimaa, Belbergui et al 'E-banking Overview: Concepts, Challenges and Solutions' (2021) 117 *Wireless Personal Communications* 1059 at 1060-1, available at *https://doi.org/10.1007/s11277-020-07911-0*, accessed on 6 April 2023.

Chovanová, Ing. Adriana 'Forms of electronic banking' (2006) 15 *BIATEC* 22 at 24, available at *https://www.nbs.sk/_img/documents/biatec/bia06_06/22_25.pdf*, accessed on 8 April 2023.

Daum, Oliver 'Cyber security in the maritime sector' (2019) 50 *Journal of Maritime Law and Commerce* 1 at 7-8.

Ghelani, Diptiben et al 'Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking' (2022) *American Journal of Computer Science and Technology* 1 at 6, available at *http://www.sciencepublishinggroup.com/j/ajcs*, accessed on 9 April 2023.

Hemminghaus C et al 'BRAT: A BRidge Attack Tool for Cyber Security Assessments of Maritime Systems' (2021) 15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 35 at 35,36,42, available at *http://www.transnav.eu*, accessed on 1 February 2022.

Iphar, Clément et al 'An expert-based method for the risk assessment of anomalous maritime transportation data' (2020) 104 *Applied Ocean Research* 1 at 4, available at *https://doi.org/10.1016/j.apor.2020.102337*, accessed on 6 July 2022.

Kao, M. Bob 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' (2021) 45 *Tulane Maritime Law Journal* 467 at 472, available at *https://heinonline.org/HOL/License*, accessed on 2 February 2022.

Kar, Arpan K & Dey, Supriya 'Cryptography in the Banking Industry' (2012) 1 *Business Frontiers* 1 at 2, available at *https://www.researchgate.net/publication/269405090_Cryptography_in_the_Banking_Industry*, accessed on 15 April 2023.

Karahalios, Hristos 'Appraisal of a Ship's Cybersecurity efficiency: the case of piracy' (2020) 13 *Transportation Security* 179 at 182, available at *https://doi.org/10.1007/s12198-020-00223-1*, accessed on 19 July 2022.

Kosowska-Stamirowska, Zuzanna et al 'Evolving structure of the maritime trade network: evidence from the Lloyd's Shipping Index (1890–2000)' (2016) 1 *Journal of Shipping and Trade* 1, available at https://jshippingandtrade.springeropen.com/articles/10.1186/s41072-016-0013-3, accessed on 1 February 2022.

Meland P. H et al 'A retrospective analysis of maritime cyber security incidents' (2021) 15 *The International Journal on Marine Navigation and Safety of Sea Transportation* 519, available at *http://www.transnav.eu*, accessed on 7 February 2022.

Mileski, Joan et al. 'Cyberattacks on ships: a wicked problem approach' (2018) 3 *Maritime Business Review* available at *www.emeraldinsight.com/2397-3757.htm*, accessed on 02 February 2022.

Mohamed, Amine Ben Farah et al 'Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends' (2022) 13 *Information* 1 at 12, available at *https://doi.org/10.3390/info13010022*, accessed on 11 July 2022.

Sharma, Navneet & Dr.Vijay Singh Rathore 'Analysis of different vulnerabilities in Auto Teller Machine transactions' (2012) 3 *Journal of Global Research in Computer Science* 38, available at *https://www.jgrcs.info*, accessed on 6 October 2022.

Schaechter, Andrea 'Issues in electronic banking: An overview' 2002 *Monetary and exchange affairs department* 1 at 3-4, available at *https://www.imf.org/external/pubs/ft/pdp/2002/pdp06.pdf*, accessed on 6 April 2023.

Svilicic, Boris et al 'Shipboard ECDIS Cyber Security: Third-Party Component Threats' (2019) 33 *Scientific Journal of Maritime Research* 176 at 178, available at *https://doi.org/10.31217/p.33.2.7*, accessed on 11 August 2022.

Svilicic, Boris et al 'Maritime Cyber Risk Management: An Experimental Ship Assessment' (2019) 72 *The Royal Institute of Navigation* 1108 at 1114, available at *https://doi.org/10.1017/S0373463318001157*, accessed on 19 July 2022.

Svilicic, Boris et al 'Assessing ship cyber risks: a framework and case study of ECDIS security' (2019) 18 *Maritime Affairs* 509 at 514-17, available at *https://doi.org/10.1007/s13437-019-00183-x*, accessed on 5 July 2022.

Svilicic, Boris et al 'Paperless ship navigation: cyber security weaknesses' (2020) 13 *Journal of Transportation Security* 203 at 206-8, available at *https://doi.org/10.1007/s12198-020-00222-2*, accessed on 5 July 2022.

Tam, Kimberly & Jones, Kevin D. 'MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment' (2019) *Maritime Affairs* 1 at 11, available at *https://doi.org/10.1007/s13437-019-00162-2.*, accessed on 4 August 2022.

Zarzuelo, Ignacio de la Peña 'Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue' (2021) 100 *Transport Policy* 1, available at *http://www.elsevier.com/locate/tranpol*, accessed on 1 February 2022.

Conference proceedings

Balduzzi, Marco et al ‘A security evaluation of AIS automated identification system’ (2014) *ACSAC* 436, available at *http://dx.doi.org/10.1145/2664243.2664257*, accessed on 28 July 2022.

Uma, Dixit 'Cryptography – Security in E-Banking' (2017) *IOR Journals* 33 at 34-6, available at *https://www.iosrjournals.org/iosr-jbm/papers/Conf.17037-2017/Volume-2/6.%2033-37.pdf*, accessed on 15 April 2023.

Muronga, K et al 'Towards secure maritime transport in South Africa: An investigation of cybersecurity readiness of organisations' (2019) Research space 1, available at https://researchspace.csir.co.za/dspace/bitstream/handle/10204/11176/Muronga_2019.pdf?sequence=1&isAllowed=y, accessed on 6 December 2021.

Internet sources

Baltic and International Maritime Council(BIMCO) 'News and trends' (2021) available at *https://www.bimco.org/news-and-trends/security*, accessed on 6 August 2021.

Cengage 'Electronic Banking' (2019) *Encyclopedia.com* available at *https://www.encyclopedia.com/finance/encyclopedias-almanacs-transcripts-and-maps/electronic-banking*, accessed on 7 February 2023.

Dodson, Brian 'University of Texas team takes control of a yacht by spoofing its GPS' available at *https://newatlas.com/gps-spoofing-yacht-control/28644/*, accessed on 7 February 2022.

Gard ' Piracy and armed robbery at sea' available at *https://www.gard.no/web/content/piracy-and-armed-robbery-at-sea*, accessed on 12 July 2022.

Goward, Dana 'Mass GPS Spoofing Attack in Black Sea?' available at *https://www.maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea,* accessed on 8 July 2022.

International Maritime Organisation 'International Convention for the Prevention of Pollution from Ships(MARPOL), and International Convention on Standards of Training, Certification and Watchkeeping for Seafarers' available at *https://www.imo.org/en/KnowledgeCentre/ConferencesMeetings/Pages/Marpol.aspx*, accessed on 12 July 2022.

International Monetary Fund 'The Global cyber threat' available at *https://www.imf.org/external/pubs/ft/fandd/2021/03/global-cyber-threat-to-financial-systems-maurer.htm,* accessed on 7 February 2023

IBM Corporation 'ATM security: Identify and fix critical flaws in machines and the connected infrastructure -Remediate exploitable vulnerabilities by understanding how attackers can compromise machines' available at *https://www.ibm.com/case-studies/large-commercial-bank?cm_sp=CTO-_-en_US-_-OYDG2REZ*, accessed on 06 Oct 2022.

King, Justin 'The Story You Aren't Being Told About Iran Capturing Two American Vessels' *MPM News* 2016/1// 2016 available at *https://www.mintpressnews.com/the-story-you-arent-being-told-about-iran-capturing-two-american-vessels/212937/*, accessed on 7 February 2022.

Nedbank 'online banking' available at *https://personal.nedbank.co.za/bank/digital-banking/channels/online-banking.html*, accessed on 6 April 2023.

Nedbank 'How to withdraw at an ATM' available at *https://personal.nedbank.co.za/bank/digital-banking/needs/payments/cardless-withdrawls/withdraw-money-at-an-atm.html*, accessed on 8 October 2022.

Nedbank 'Security is a top priority for Nedbank electronic banking channels' available at *https://businessbanking.nedsecure.co.za/download.aspx?tp=302&id=124*, accessed on 6 April 2023.

Omholt-Jensen, Kristin & Engnæs, Pål-Robert 'AIS and the main categories of AIS challenges' *Maritime Optima*, available at *https://www.maritimeoptima.com/blogdata/ais-and-the-main-categories-of-ais-challenges*, accessed on 6 February 2023.

Oxford dictionary 'Readiness meaning' available at *https://www.oxfordlearnersdictionaries.com*, accessed on 12 July 2022.

Safety4Sea 'Maersk Line: Surviving from a cyber-attack' (2018) available at *https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/?__cf_chl_jschl_tk__=pmd_wQ_M2KXj4d7U9zR4A6o3LdPdflLkOzL5pP4YZY1y99k-1631091035-0-gqNtZGzNAhCjcnBszQlR*, accessed on 6 February 2022.

Saito, Naoki Capt. 'Cyber Security Onboard' (2022) Tokyo,Japan, Nippon Kaiji Kyokai (ClassNK), available at *https://www.classnk.com*, accessed on 14 September 2022.

Smith, Carin 'SA ports in crisis as Transnet cyberattack creates 'total nightmare' for exporters' (2021) available at *https://www.news24.com/fin24/companies/sa-ports-in-crisis-as-transnet-cyberattack-creates-total-nightmare-for-exporters-20210728*, accessed on 28 March 2022

U.S Coast Guards '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 on 5 July 2022.

Yatsenko, Nick 'Why are lifeboats killing seafarers' available at *https://gcaptain.com/why-are-lifeboats-killing-seafarers/*, accessed on 12 September 2022.