ISSN 2464-9724

Maritime Safety and Security Law Journal

2021
Issue 9

Maritime Safety and Security Law Journal

International Maritime Organisation Framework on Cyber Risk Management - a Case for a Comprehensive Legal Framework

*Bisola OGUNDARE and Gbenga AKINWANDE**

Abstract

The global maritime industry continues to embrace information technology and operational technology in automating its processes. Increased digitalisation has brought about cyber vulnerabilities, opening the door for cyber-attacks. Cyber-attacks can have serious consequences for crews, ships, and cargos, including casualties, loss of control of ship and ship or cargo hijacking. This research paper examines and discusses the limitations of the current IMO framework. The paper calls for a comprehensive legal framework on cyber risk management through the strengthening of the ISM Code and potentially through creation of a Cyber Code.

Keywords: cyber code, cyber-attacks, cyber security, cyber risk management, international maritime organisation, safety management system

First published online: 31 December 2021

1. Introduction

Digitalisation has become an important part of maritime business operations, improving safety, efficiency, and maximising productivity and cost-effectiveness.[1] Digitalisation is the application of digital technology to all things used in daily life.[2] In the maritime industry, digitalisation has had a huge impact because of the continuous advancement of satellite communication and data generators.[3] Daily information exchange takes place between ships and ports, or companies and agents. The implementation of this technology and network, cyber structure has increased the likelihood of cyber-attacks.[4] Despite this, the maritime industry has been slow to recognise the impact

* Bisola Ogundare, LL.M in Ocean governance at Dalhousie University and Gbenga Akinwande LLM at the University of Western Ontario. We are very grateful for excellent feedback of the reviewers and the editorial board of the Maritime Safety and Security Journal for their contributions to this paper.

1 Vivian Louis Forbes, 'The Global Maritime Industry Remained Unprepared for Future Cybersecurity Challenge', (Future Directions International, 21 August 2018) <www.futuredirections.org.au/publication/the-global-maritime-industry-remains-unprepared-for-future-cybersecurity-challenges/> accessed 1 August 2021.

2 David Silgado, 'Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry' (2018) 663 WMU Dissertation 2.

3 DNV.GL, 'Digitalisation in the Maritime Industry' <www.dnvgl.com/maritime/insights/topics/digitalisation-in-the-maritime-industry/index.html> accessed 1 November 2020.

4 Constantinos Varouxis, 'Cyber Maritime Security Vulnerabilities Prospect for EU' (SCRIBD, 2019) <www.scribd.com/document/468659061/CyberMaritimeSecurity> accessed 27 October 2020.

of cyber-attacks on the industry.[5] According to a Global Maritime Issue monitor survey,[6] for the next ten years, cyber-attacks and data theft rank fifth in terms of their impact in the maritime sector, while in terms of likelihood of an issue and disaster preparedness, cyber-attack and data theft rank third.[7]

Cyber-attacks can threaten lives, the environment, lead to financial losses, and can significantly disrupt the movement of maritime trade.[8] In view of the devastating impact of cyber-attacks on global trade, the International Maritime Organisation (IMO)[9] recognises cyber-attacks as a problem in the maritime industry and has proposed a regulatory framework to address cybersecurity threats.

The IMO developed regulations and guidance through the subcommittee Maritime Safety Committee (MSC). The MSC, during its 96th session on 11 to 20 May 2016 adopted provisional cybersecurity Guidelines (MSC.1/Circ.1526).[10] This provisional response was necessary due to increased cyber-attacks in the maritime industry. In June 2017, the MSC adopted Resolution MSC.428(98),[11] which mandates the incorporation of cyber risk management in the company's existing Safety Management System (SMS) in compliance with the ISM Code.[12]

Lastly, the MSC in July 2017 adopted the (MSC-FAL.1/Circ.3)[13]Guidelines on the maritime cyber risk management. These Guidelines provide recommendations for effective cyber risk management and supersede earlier Guidelines (MSC.1/Circ.1526) though they remain non-mandatory.

This paper analyses the limitations of the MSC-FAL.1/Circ.3 Guidelines, MSC.428(98) Resolution and the ISM Code provisions on maritime cyber risk management.[14] Therefore, the study seeks to answer the following questions:

i) What are the limitations of the IMO current legal framework on cyber risk management?
ii) Could a stand-alone Cyber Code address the limitations of the IMO's legal framework on cyber risk management?

---

5 Kala Baskar and Mahesh Balakrishnan, 'Cyber Preparedness in Maritime Industry' (2019) 5(2) IJSTA 19.

6 Global Maritime Issues Monitor 2020 is based on research among senior leaders around the world, it explores the impact, likelihood, and preparedness of 19 global issues potentially affecting the maritime industry in the coming decade.

7 Global Maritime Form, MARSH and International Union of Marine Insurance, 'Global Maritime issue Monitor 2020' (2020) <www.maritimeissues.org/#overview> accessed 27 October 2020.

8 SAFETY4SEA, 'How IMO Addresses Cyber Risk: An Overview' (2020) <https://safety4sea.com/cmhow-imo-addresses-cyber-risk-an-overview/> accessed 27 October 2020.

9 IMO is a specialised agency of the United Nations (UN) and a competent international organisation, which according to the United Nations Convention on the Law of the Sea (UNCLOS), has the mandate to regulate international trade and voyage by sea as safe and secure as possible.

10 IMO, 'Interim Guidelines on Maritime Cyber Risk Management' (1 June 2016) MSC. 1/Circ1526(E).

11 IMO 'Maritime Cyber Risk Management in Safety Management Systems' (16 June 2017) Resolution MSC.428 (98), MSC 98/23/Annex 10.

12 IMO, 'Maritime Cyber Risk' (2018) <www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx> accessed 27 October 2020.

13 IMO 'Guidelines on Maritime Cyber Risk Management' (5 July 2017) MSC-FAL.1/Circ.3, para 1.

14 IMO 'International Safety Management Code (ISM) Code) International Management Code for the Safe Operation of Ships and for Pollution Prevention' (amended by Resolution MSC.353(92), entered into force 1 January 2015).

1.1 Aim / literature review

Cyber-attacks in the maritime industry are a recognised problem. Chalermpong Senerak,[15] using Leam Chabang Port as a case study, established through a questionnaire that ports are attractive to cyber-attacks because they are the key nodes of global trade and hold a lot of data. According to Juan Ignacio and Ruth Garcia,[16] cyber incidents can cause major environmental and economic disasters, and loss of human life. David Silgado[17] emphasised that the economic consequence of cyber-attacks on the maritime industry is the loss of intellectual property, the biggest threat to business.

William Stahl[18] canvassed for the adoption of the principle of universal jurisdiction embedded in UNCLOS to solve the problem of cybercrime.[19]

In response, the IMO adopted the Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3) and Maritime Cyber Risk Management in Safety Management Systems Resolution, MSC.428(98). Researchers have commented on the response of the IMO to cybersecurity threats. Oliver Daum[20] called for sanctions embedded in the ISM Code to apply for breach of the IMO's cybersecurity standards after examining how cyber-attacks could impede the safe operation of ships. Rory Hopcraft and Keith Martin,[21] called for the creation of a cyber code on cyber risk management in the manner of the Polar Code.[22] They concluded that a single benchmark code would be easier to update and enforce. The Polar Code is discussed in more detail in part four of this paper.

The approach in this paper is to argue for the strengthening of the ISM Code in the short term, since it is the basis on which the IMO seeks to repel cyber-attacks and the industry is not yet receptive to the idea of a cyber code.[23]

1.2 Structure

The paper is structured in three subsequent parts. Part Two details the cybersecurity landscape. Part Three discusses the role of IMO as a norm-maker in the maritime industry and argues that the IMO's regulatory framework on cyber risk management is an example of this. This part also analyses the legal status / effect of the framework.

---

15 Chalermpong Senerak, 'Port Cybersecurity and Threat: A Structural Model for Prevention and Policy Development' (2020) 247 AJSL 17.

16 Juan Ignacio Alcaide and Ruth Garcia Llave, 'Critical Infrastructure Cybersecurity and the Maritime Sector' (2020) 45 TRP 547.

17 Silgado (n 2) 26.

18 William Stahl, 'The Uncharted Waters of Cyberspace- Applying the Principles of International Maritime Law to the Problem of Cyber Security' (2011) 40(1) GJICLL 273.

19 ibid.

20 Oliver Daum, 'Cybersecurity in the Maritime Sector' (2019) 50(1) J Mar. L Com 19.

21 Rory Hopcraft and Keith Martin 'Effective Maritime Cybersecurity Regulation - The Case for a Cyber Code' (2018) 14(3) JIOR.

22 International Code for Ships Operating in Polar Waters (Polar Code) was developed to supplement existing IMO instruments such as the International Convention for Safety of Life at Sea (SOLAS) 1974 and the International Convention for the Prevention of Pollution from Ships 1973, to increase the safety of ships operating in polar waters and to mitigate the impact on the people and the environment close to the polar waters. See the preamble to the Polar Code.

23 Stahl (n 18) 273.

Part Four analyses the limitations of IMO's regulatory framework and argues for a stand-alone cyber code in the future and immediate stronger enforcement of the ISM Code.

2. Maritime cybersecurity and entities responsible for cyber-attacks

2.1 Definitions

Although there is no universally agreed definition, the term maritime cyber security has been used to describe measures taken to protect networks and computer assets both on ships, in terminals, at ports, and equipment supporting maritime operations.[24]A cyber-attack is an offensive exercise initiated by cybercriminals/attackers using one or more computer against multiple computers or networks on ships, in terminals, at ports, and all computerised equipment supporting maritime operations.[25]

Due to the nature of its operations, the maritime industry is highly vulnerable to cyber-attacks. As illustrated by Jensen,[26] a large shipping line would typically be operating a fleet of 300 vessels of which they own 150 and the other 150 chartered from a wide range of vessel-owning companies for a period of time. In this scenario, the shipping line will not have the capacity to control the IT-structure onboard chartered vessels, instead relying upon the defences put in place by the charter vessel owners.[27]

In addition, due to reduced access costs and anonymous global access, there is ever greater internet access.[28] Individual internet usage is difficult to trace as the internet was designed to facilitate information flow and collaboration. Thus, cyber attackers can operate free from scrutiny of their internet use and behaviour.[29]

Cyber-attacks can be classified into three major categories: (a)Automated malicious software delivered over the internet (b) Denial of service attacks (DOS) and (c) Unauthorised remote intrusions into a computer system (hacking).[30]

The first type utilises malware, which is classified as either a virus or worm.[31] Malware usually in-

24 Christopher Hayes, 'Maritime Cybersecurity: The Future of the National Security' (Dudley Knox Library, June 2016) <https://calhoun.nps.edu/handle/10945/49484> accessed 8 November 2020.

25 Josh Fruhlinger, 'What is a Cyber Attack? Recent Examples Show Disturbing Trends' (CSO, 27 February 2020) <www.csoonline.com/article/3237324/what-is-a-cyber-attack-recent-examples-showdisturbing-trends.html> accessed 7 November 2020.

26 Lars Jensen, 'Challenges in Maritime Cyber-Resilience' (Technology Innovation Management Review, April 2015) <https://timreview.ca/article/889> accessed 8 November 2020.

27 ibid.

28 Stahl (n 23) 254.

29 Sharon Stevens, 'Internet War Crimes Tribunals and Security in an Interconnected World' (2009) 18 Transnat'l L. & Contemp. Probs. 657.

30 Stahl (n 28) 254.

31 ibid 255.

fects a computer system through email or when a user visits an infected site.[32] A DOS attack is initiated from a single computer and overwhelms a target system with requests until the system can no longer function properly, denying users access to and use of the targeted system or site.[33] Hacking is the process of gaining unauthorised access into a computer system or group of computer systems, usually through the cracking of passwords to access systems.[34]

2.2 Cybercriminals / attackers and their motivation

Cybercriminals / attackers are those who attempt to gain unauthorised access to data, functions, or other restricted areas of the system (perhaps for malicious purpose).[35]

Baskar and Balakrishnan[36] divide cybercriminals into two categories: 'outsiders' and 'insiders.' Outsiders include hacktivist, state-sponsored groups, criminal groups, and terrorist organisations. Insiders are those interested in espionage, or disgruntled employees.

The third category is criminal groups, either individuals or criminal organisations that carry out cyber-attacks on interconnected systems and networks. Their intention is to carry out criminal activities, focusing on fraudulent operations, extortion, or misappropriation of intellectual property rights. These groups are mainly financially motivated. Finally, terrorist organisations are motivated by ideology or religion, or they have political interests in carrying out attacks on countries and companies to gain access to confidential data, spread malware and interrupt the operating system. Insider attacks are mostly perpetrated through espionage with the main objective of obtaining access to confidential information in order to use that information for competitive advantage or to disrupt business operations.[37]

2.3 Cybersecurity vulnerabilities in maritime infrastructure

The maritime industry has embraced digitalisation in all its operations. According to Professor Forbes, maritime companies are now exploring the opportunities presented by the 'Internet of Things' and artificial intelligence to boost their performance and cut costs.[38]

The number of maritime cyber-attacks is unknown, because reports are often ignored or not re-

32 ibid.

33 ibid.

34 Noam Judah, 'What is Hacking? Common Objectives, Types, and How to Guard Against It'(The Hacker Noon Newsletter, 4 March 2019) <https://hackernoon.com/what-is-hacking-common-objectives-types-and-how-to-guard-against-it-ab99897ff00b> accessed 20 August 2020.

35 Baskar and Balakrishnan (n 5) 19.

36 ibid 9.

37 Danish Defence Intelligence Service, 'Threat assessment: The cyber threat against the Danish maritime industry and ports' (Center for Cybersecurity, October 2020) <https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cfcs-cyber-threat-danish-maritimeindustry-and-ports-.pdf> accessed 8 November 2020.

38 Forbes (n 1) 5.

ported due to reputational implications.[39] Vulnerable maritime infrastructure subject to cyber-attacks are addressed below.

2.3.1 Ship-based cyber vulnerabilities

Ships navigation aids include but are not limited to the Global Positioning System (GPS), the Automatic Identification System (AIS), and the Electronic Chart Display Information System (ECDIS). These navigation aids are part of the maritime operational technology (OT). GPS is important to maintain safety at sea and for efficient navigation. However, this system is vulnerable to techniques such as spoofing and jamming, which cause a breakdown if used successfully by the hackers. AIS allows ships to obtain necessary data about other ships in transit. It is used for ship positioning and tracking.[40] However, AIS is not protected by complex encryption or authentication. Therefore, spoofed AIS signals may be used by ship operators to conceal their location or used to create a false navigation obstacle. Finally, ECDIS is a computer based navigational chart that displays nautical charts and the precise location and tracking information of ships.[41] It works by receiving information from AIS and GPS data, speed, course, and radar. Since the ECDIS receives information, it is potentially susceptible to cyber-attack as it is vulnerable to malware. In addition, the ECDIS navigation charts are updated through removable media, which can be easily infected by viruses.

In July 2013, a radio navigation research team from the University of Texas successfully proved the weaknesses and imperfections of GPS as they hacked the GPS signal of an US$80 million, 210-foot yacht in the Mediterranean taking control of the ship's navigation system, which enabled them to steer the vessel as they saw fit.[42] The purpose of the experiment was to expose the weaknesses of GPS.

2.3.2 The threat to ports

Ports are critical to maritime operations, and digitalisation has been integrated into port activity for many years.[43] Unfortunately, this digitalisation has become a major vulnerability, as cyber-attacks on ports can have negative impacts on the maritime supply chain. This was demonstrated by an incident at the port of Antwerp (Belgium). In the period 2011 to 2013, the computerised cargo tracking system at the port was hacked by hackers working with drug smuggling gangs. Hackers sought to breach IT systems that control the movement and location of containers to identify the shipping containers in which consignments of drugs were hidden. Then the gang stole the compromised containers to re-

39 Ivan Mrakovic and Ranko Vojinovic, 'Maritime Cybersecurity Analysis – How to Reduce Threats?' (2019) 8(1) TOMS 132.

40 Singh Hansdeep, 'Cyber Security in Maritime Industry: The Exposure, Risks, Prevention and Legal Scenario' (UIO DUO Research Achieve, 1 December 2019) <www.duo.uio.no/handle/10852/73742> accessed 10 November 2020.

41 Lagouvardou Sotiria, 'Maritime Cybersecurity: Concepts, Problems and Models' (Technical University of Denmark, 5 July 2018) <https://seatracker.ru/viewtopic.php?t=38182> accessed 8 November 2020.

42 Bob Brewin, 'Grad Students Gain Control of Navigation System to Veer Ship Of Course' (Nextgov, 29 July 2020) <www.nextgov.com/cio-briefing/2013/07/university-texas-team-hijacks-80-million-yachtcheap-gps-spoofing-gear/67625/> accessed 13 November 2020.

43 Senerak Chalermpong, 'Port Cybersecurity and Threat: A Structural Model for Prevention and Policy Development' (2020) 37(1) AJSL 20.

trieve the drugs.[44] The hackers obtained remote access through phishing emails sent to port employees. This breach was discovered after an entire container disappeared, resulting in a firewall being installed in the system. The hackers then broke into the port office and installed key logging software on a legitimate computer to intercept data from the system.

2.3.3 The threat to maritime companies

Cyber-attacks affect maritime companies. A.P. Moller –Maersk, the world's largest shipping firm is one of the many international companies that were hit by the ransomware malware 'NotPetya' on 27 June 2017. This ransomware affected all Maersk business units.[45] The company was forced to shut down all systems in order to contain the cyber incident. The NotPetya incident triggered the need to rebuild the entire network of 4,000 servers and 45,000 PCs. This attack cost the company approximately US$300 million.[46] Security specialist Ken Munro[47] opined that the attack may draw the attention of more cybercriminals, who realise that the maritime industry is acutely exposed.[48]

Also, in 2020, the Mediterranean Shipping Company suffered an attack that caused its data centre to close for several days.[49]

The above highlights that the maritime industry is heavily dependent on technology. Since the maritime industry is not immune to cyber-attacks, the steps the IMO takes to respond to cyber-attacks are crucial.

3. IMO cybersecurity framework

The IMO was established by the adoption of a convention at the UN maritime Conference in 1948.[50] The Convention[51] came into force on 17 March 1958. Article 1 (a) of the Convention provides for the purpose of IMO, which is to promote cooperation among governments and ensure the highest practicable standards are met in matters pertaining to maritime safety.[52] Also, in order to fulfil its purpose

---

44 Chronis Kapalidis, '4 Cases of Cybersecurity Failures in Shipping History' (Linkedin,31 March 2018) <www.linkedin.com/pulse/4-cases-cyber-security-failures-shipping-history-chronis-kapalidis> accessed 10 November 2020.

45 Jacob Gronholt-Pedersen, 'Maersk Says Global IT Breakdown Caused by Cyber Attack' (Thomas Reuters, 27 June 2020) <www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19I1NO> accessed 13 November 2020.

46 Mike Mcquade, 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History' (Wired, 22 August 2018) <www.wired.com/story/notpetya-cyberattack-ukraine-russia-Code-crashed-the-world/> accessed 13 November 2020.

47 Ken Munro is a Partner and founder of Pen Test Partners. See ICCC 2022, 'Ken Munro- Founder and Partner, Pen Test Partners' (15-17 November 2022) <https://iccconference.org/?speaker=kenmunro> accessed 1 November 2021.

48 Bloomberg, 'Cyber Pirates: Shipping Industry Under Second IT attack in a week' (Aljazeera, 2 October 2020) <www.aljazeera.com/economy/2020/10/2/cyber-pirates-shipping-body-suffers-second-it-attack-in-aweek> accessed 13 November 2020.

49 ibid.

50 IMO, 'Brief History of IMO' <www.imo.org/en/About/HistoryOf IMO/Pages/Default.aspx> accessed 28 October 2020.

51 Convention on the International Maritime Organization (adopted 6 March 1948, entered into force 17 March 1958), 289 UNTS 3, art 48.

52 ibid art 1(a).

as a standard-setting organisation, it provides for the drafting of agreements, conventions or other suitable instruments, and makes recommendations regarding maritime safety to governments and intergovernmental organisations.[53] It also provides a forum for consultation among members and exchange of information among Governments.[54]

The IMO's standard setting role makes its a legislative authority, but not in the traditional sense of a parliament, as the IMO does not have power to enforce its instruments but rather relies on member states for enforcement and acceptance.[55]

The IMO's milestones in maritime cybersecurity can be divided into four stages. First, in November 2014, the MSC supported a Canada / United States proposal on establishing voluntary Guidelines on the maritime cybersecurity practices.[56] Four years later, on 1 June 2016, the MSC approved the 'Interim Guidelines on Maritime Cyber Risk Management' (MSC.1/Circ.1526)[57] at its ninety sixth session, which put forward recommendations for protecting shipping from widespread cyber threats. The reason for releasing this interim Guidelines was due to the urgent need to raise awareness on cyber risk and vulnerabilities.[58]

Subsequently, in 2 June 2017, the MSC, during its ninety eighth session resolved that all companies should incorporate cyber risk management in their approved SMS in accordance to the functional requirements of the ISM Code (MSC.428 (98)).[59] Less than a month later, in 3 July 2017, the Guidelines (MSC-FAL.1/Cir.3) on maritime cyber risk management was approved at the ninety eighth session of the MSC.[60] The Guidelines are voluntary and supersedes the interim Guidelines contained in MSC. 1/Circ. 1526.[61] The IMO framework for cybersecurity described above, consists of the ISM Code, a Resolution and Guidelines which the research addresses in detail below.

3.1 Resolution MSC.428(98) and ISM Code

The IMO Resolution MSC.428(98) was adopted by the MSC on 16 June 2020.[62] This Resolution scaled up the level of authoritativeness of IMO measures on cybersecurity. The Resolution makes the following points regarding cyber risk management:

53 ibid art 2(b).

54 ibid art 2(b) and (c).

55 Robert Beckman and Zhen Sun 'The Relationship between UNCLOS and IMO Instruments' (2017) 2(2) APOC.

56 SAFETY4SEA, 'Regulatory Update: Cyber security risks' (Safety4Sea, 25 May 2018), <www.safety4sea.com/cmregulatory-update-cyber-security-risks/> accessed 28 October 2020.

57 IMO, 'Interim Guidelines on Maritime Cyber Risk Management' (1 June 2016) MSC.1/Circ. 1526(E).

58 Rachel Foote, 'Cybersecurity in the Marine Transportation Sector: Protecting Intellectual Property to Keep Our Ports, Facilities, and Vessels Safe from Cyber Threats' (2017) 8(2) Cybaris.

59 Resolution (n 11).

60 Guidelines (n 13).

61 ibid para 4.

62 Resolution (n 59) para 3.

1.The need to increase awareness of cyber risk threats in the maritime industry.[63]

2. The need for stakeholders to take quick actions toward safeguarding ships from current cyber threats.[64]

3. In respect to the 'Guidelines on maritime cyber risk management' as providing high-level recommendation for maritime cyber risk management.[65]

4. Recalls the goal of the ISM Code and encourage all organisations in the maritime industry to ensure that cyber risks are rightly addressed in Safety Management Systems before, the first annual verification (1 January 2021) of a company's Document of Compliance.[66]

As earlier noted, the Resolution MSC.428(98) encourages companies to address and incorporate cyber risk management into their Safety Management System.

The ISM Code[67] is a mandatory international instrument which provides standards for the management and operation of ships and for pollution prevention. The Code establishes a broad framework for managing operational risks with the aim of maintaining high standards for safety and environmental protection.

The ISM Code dates back to the 1980s, when there were rising concern regarding poor management standards in shipping.[68] The ISM Code is a crucial element of Chapter IX of the 1974 Convention for the Safety of Life at Sea (SOLAS),[69] an international maritime treaty which establishes the minimum safety measures for equipment and operation, construction, and merchant ships.[70]

Resolution MSC.428(98) paragraph seven affirms that the objectives and functional elements of the ISM Code must be considered in an approved SMS cyber risk management.[71] The approach adopted here is goal-based regulation. The following questions then become necessary: 'what is the objective of the ISM Code?' 'What is SMS?' and what are its functional requirements?'.

The objectives of the ISM Code are provided in No. 1.2.1 of the Code which are: 'to ensure safety at sea, preventing human injury or loss of life, and preventing damage to the environment, specifically the marine environment'.[72] The regulatee of the ISM Code is a 'Company', which pursuant to provision No. 1.1.2 means 'the owner of a ship or any organisation or person who has assumed responsibility for the

63 ibid para 1.

64 ibid para 2.

65 ibid para 3.

66 ibid para 4.

67 ISM Code (n 14).

68 Vandenborn Yves, 'Twenty Years of ISM Code' (SAEFTY4SEA, 3 July 2018) <www.safety4sea.com/twenty-years-of-the-ism-Code/> accessed 28 October 2020.

69 ibid.

70 Anish Wankhede, 'Safety of Life at Sea (SOLAS)- The Ultimate Guide' (Maritime Insight, 3 January 2020) <www.marineinsight.com/maritime-law/safety-of-life-at-sea-solas-convention-for-prevention-ofmarine-pollution-marpol-a-general-overview/> accessed 28 October 2020.

71 ibid para 7.

72 ISM Code (n 67) no 1.2.1.

operation of the ship'.[73] According to No. 1.2.3 of the Code, 'the SMS of the shipping company must ensure safety and environmental protection through compliance with international and flag administration requirements, classification society or maritime industry organisation'.[74] In this regard, companies may find that the non-mandatory Guidelines of IMO MSC-FAL.1/Circ.3 nonetheless provide useful procedures for assessing risks and implementing risk mitigation measures.

Similarly, companies may find the standards established by recognised organisations and non-governmental organisations to be also helpful and are encouraged to refer to the Guidelines for the development of their SMS. The SMS is defined in the ISM Code as a 'structured and documented system enabling company personnel to effectively implement the company safety and environmental protection policy'.[75] The SMS should include the following functional requirements:

1. A safety and environmental protection policy;
2. Instructions and procedures to ensure safe operation of ships and protection of the environment in compliance with relevant international and flag state legislation;
3. Defined levels of authority and lines of communication between, and amongst, shore and shipboard personnel;
4. Procedures for reporting accidents and non-conformities with the provisions of the Code;
5. Procedures to prepare for and respond to emergency situations; and procedures for internal audits and management reviews.[76]

Therefore, in compliance with the IMO Resolution, the SMS must adequately address the ISM Code objectives and functional elements in an ongoing manner. The document used to describe and implement the SMS may be referred to as the 'Safety Management Manual'.[77]

In addition, a company should periodically verify whether SMS measures put in place are effective and meet the objectives of the Code.[78] The verification of a company's incorporation and implementation of cyber risk mitigation into the SMS will occur during internal and external audit in accordance with the requirements of the ISM Code.[79]

3.2 MSC-Fal.1/Circ.3 guidelines

The MSC-FAL.1/Circ.3 Guidelines propose that the best practices of cyber risk management be adopted into a company's risk management framework while recognising that no two companies in the maritime industry are alike. It also advocates for a holistic approach to managing cyber risk by advising stakeholders to refer to specific member government and flag administrations' require-

73 ibid no 1.1.2.
74 ibid no 1.2.3.
75 ibid no. 1.1.4.
76 ibid no1.4.
77 ibid no 11.3.
78 ibid no12.2.
79 ibid no 12.1.

ments as well as relevant international and industry standards.[80]

The Guidelines also reference different standards that could serve as guidance to a company on cyber risk management.[81] These standards are also non-binding in nature. Moreover, these standards provide a risk-based approach to detecting and solving cyber risk issues.[82]

The IMO MSC-FAL.1/Circ.3 Guidelines include five elements that are also identified in the NIST framework: identify, protect, detect, respond, and recover. Bobyx[83] stated that the IMO MSC-FAL.1/Circ.3 Guidelines are structured on the NIST cybersecurity framework because the functional elements in the IMO Guidelines are similar to that of NIST framework.[84]

The contents of the Guidelines are analysed under three categories: scope, intent/motive and functional elements.

3.2.1 Scope

The Guidelines cover high-level recommendations for functional elements to be incorporated by all stakeholders in the maritime industry. The IMO stressed that the Guidelines were complementary to safety and security management practices it had already established: the ISM Code.[85]

The Guidelines provide definitions of some terms: IT, OT, maritime cyber risk, and cyber risk management. The Guidelines defined 'IT' as the use of data as information,[86] whereas 'OT' system is defined as the use of data to control and monitor physical processes.[87] Also, maritime cyber risk is defined in the Guidelines as a potential circumstance or event that could threaten a technology asset, which could result in shipping-related operational, safety or security failures as a consequence of IT or OT system being corrupted, lost or compromised.[88] These 'circumstances' or 'events' are vulnerabilities in cyber technology (digitalisation, integration, and automation). These vulnerabilities are created by accessing, interconnecting, or networking cyber technologies, which includes and are not limited to: 'bridge systems, cargo handling and management systems, propulsion, machinery management and power control systems, access control systems, passenger servicing and management systems, passenger facing public networks, administrative and crew welfare systems and communication systems'.[89]

---

80 ibid nos 1.3, 2.2.2 and 4.1.

81 The Baltic and International Maritime Council (BIMCO), see *Guidelines* (n 60) no 1.5

82 ISM Code (n 72) no 4.2.

83 Max Bobyx, 'Safety4Sea: The Cyber Risk Landscape' (YouTube, 21 May 2018) at 13 minutes 12 seconds <www.youtube.com/watch?v=cYte29pHTLE&feature=emb_logo> accessed 27 October 2020.

84 ibid.

85 Guidelines (n 60),no 1.5.

86 ibid no 21.2.

87 ibid no 21.2.

88 ibid no 1.1.

89 ibid no 2.1.1.

Lastly, the Guidelines define cyber risk management as the 'process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering the costs and benefits of actions taken to stakeholders.[90]

3.2.2 Intent/motive

The IMO Guidelines are intended for all shipping organisations in order to strengthen safety and security management practices in the cyber domain (digitalisation, integration, and automation), which are resilient to cyber risks.[91] Specifically, it emphasises the need to protect both the OT and IT on board a vessel.[92] The Guidelines' main focus is on the risk management approach to cyber risks; this should be incorporated in existing industry safety and security procedures.[93]

3.2.3 Functional elements

The Guidelines outline important recommendations for cyber risk management across maritime companies. It highlights some functional elements that can be implemented concurrently on a continuing basis within an organisation's risk management framework. These functional elements are identify, protect, detect, respond, recover.

The 'identify' element suggests that all personnel roles and responsibilities related to cyber risk management should be identified. Vulnerable systems, assets, data, and capabilities should also be identified.[94] The 'protect' element proposes implementing risk control processes and measures that focus on cyber-attack prevention and contingency planning that ensure continuity regardless of cyber-attack.[95] The 'detect', 'respond' and 'recover' elements are in a sense interrelated with a focus on developing and implementing operations that enable an organisation to detect cyber-attacks, timely respond and restore cyber system impaired due to cyber-attack.[96]

3.3 Legal effect of the MSC-Fal.1/Circ.3 guidelines /IMO framework

UNCLOS is the landmark law of the sea instrument. There are many references to 'competent' or 'appropriate' international organisations in UNCLOS.[97] It is generally understood that the various references to 'competent international organisation' in UNCLOS refers to the IMO.[98]

---

90 ibid no 3.1.

91 Dromon Bureau of Shipping, 'Guidelines on Maritime Cyber Risk Management' (DBS, 23 October 2018) <www.maritime-cyprus.files.wordpress.com/2018/11/dromon-Guidelines-on-maritime-cyber-riskmanagement.pdf> accessed 27 October 2020.

92 Guidelines (n 85) nos 2.1.2 and 2.1.5.

93 ibid no 2.1.8.

94 Guidelines (n 92), no 3.5(1).

95 ibid no 3.5(2).

96 ibid no 3.5(3-5).

97 Beckman and Sun (n 55) 218.

98 ibid.

UNCLOS imposes a duty on states to respect and apply generally accepted international standards,[99] otherwise known as customary international law. According to Sohn there are different ways that customary international law is updated.[100] One is when an international agreement incorporates certain rules considered to be generally accepted or an agreement is considered as declaratory of certain generally accepted rules binding on all states.[101] It has been argued that the source of IMO instruments' legitimacy derives from UNCLOS tacit reference to IMO as a 'competent international organisation' and the duty on states to apply and respect generally accepted international standards and rules.[102]

It could therefore be argued that the IMO Guidelines on Maritime Cyber Risk Management derives its legitimacy from UNCLOS, and that the IMO and its instruments have been incorporated into UNCLOS by reference.[103] The IMO Guidelines and Resolution can be described as international soft law. Soft law has been described as an international instrument that has some attributes of a formal treaty but however falls short of the legal requirements to be one.[104]

The implementation of IMO circulars, guidelines, resolutions by a majority of industry actors creates a norm. This is because it is obvious that 'the accumulation of recurrent resolutions can generally contribute to the creation of such a new general customary rule'.[105] Soft law gives industry actors a way to be proactive and to continually improve and stay ahead of the competition.[106] One of the ways to achieve this is in improving safety and utilising new technologies. Compliance with the IMO Guidelines on Cyber Risk Management is a way for maritime companies to show that they take safety seriously.

3.4. Positive attributes of the IMO framework on cyber risk management

One of the positive attributes of the IMO's framework on cyber risk management is that it recognises the link between cybersecurity and maritime safety. It is a fact that the maritime industry relies heavily on satel-

99 Convention on the Law of the Sea (adopted 10 December 1982, entered into force 16 November 1994) 1833 UNTS. 397, arts 21(2), 211(2), 211(5), 211(6) and 226(1).

100 Louis Sohn, 'Generally Accepted International Rules' (1986) 61(3) Wash L Rev.

101 Another way is when international agreements provide those rules to be adopted by an international organisation, shall be considered as generally accepted unless a state expressly opts out.

102 Beckman and Sun (n 97) 221.

103 Another rule incorporated by reference into UNCLOS is the rule that "foreign ships exercising right of innocent passage through the territorial sea shall comply with all... generally accepted international regulations relating to the prevention of collision at sea." This rule is binding on flag states of ships that did not ratify the convention to which those regulations are annexed. Louis Sohn (n 100) 1075.

104 Andrew Guzman and Timothy Meyer, 'International Soft Law' (2011) 2(1) J. Leg. Anal.

105 ibid 9.

106 ibid 10.

lite-based navigation systems, which are increasingly susceptible to spoofing.[107] Spoofing attacks may paralyse shipping lanes and cause collisions between ships, resulting in injury or loss of human lives and cargo.[108] It was in furtherance of this agenda that Resolution MSC.428(98) encouraged 'all organisations in the maritime industry to ensure that cyber risks are rightly addressed in their Safety Management Systems.'[109]

Another positive attribute of the IMO's regulatory framework on cyber risk management is that it has increased the awareness level of cyber vulnerabilities among the maritime industry. The key to addressing cyber vulnerabilities in the maritime industry is to first identify and acknowledge that maritime infrastructures are susceptible to cyber-attacks (the first functional element of the MSC-FAL.1/CIRC.3) and then to address it.

Maritime companies are expected to file Document of Compliance which will detail cyber awareness level, cyber vulnerabilities identified, and measures taken to build a cyber risk resilient operation. The Document of Compliance are meant to be annually verified. The Guidelines recognise that one of the vulnerable points of attack related to cybersecurity are people. Therefore, it places the responsibility of cybersecurity management on everyone in the organisation.

Incorporating the cybersecurity standards in the ISM Code will ensure that in the event of non-compliance, the appropriate sanctions in the ISM Code can be followed. There are two types of audits,[110] envisaged under the ISM Code: External Audit by the Class on behalf of Flag of the Ship and Internal Audit by the Company. During these audits, the auditor may find some deficiencies and shortcomings. The ISM Code categorises these shortcomings as: observation, minor non-conformity, and major non-conformity.[111] Under the ISM Code, ships cannot sail with a major non-conformity. It can only sail once it has been downgraded to a minor non-conformity after corrective actions must have been taken.[112] Another sanction in the SMS Code is that if the major non-conformity is very serious, the Safety Management Certificate of the ship may be withdrawn.[113] These sanctions would apply if a company breached the cybersecurity standards.[114]

---

107 Global Navigation Satellite System (GNSS) spoofing involve an actor replicating satellite navigation signals with an identical signal that is strong enough to force out the original transmission. Once the spoof signal is in place, rogue transmissions can mislead onboard navigation systems such as location, velocity and heading. See Chris Lo, 'GPS Spoofing: What's the risk for ship navigation?' (Ship Technology, 15 April 2019), <www.ship-technology.com/features/shipnavigation-risks/?utm_source=Army%20Technology&utmmedium=website&utm_campaign=Must%20Read&utm_content=Image> accessed 31 October 2020.

108 Resolution (n 62) para 4.

109 ibid.

110 ISM Code (n 82), arts 12 and 15.

111 ibid nos 1.1.8, 1.1.9 and 1.1.10.

112 IMO, 'Procedures Concerning Observed ISM Code Major Nonconformities' (16 December 2002) MSC/Circ 1059 and MEPC/Circ 401, Ref. T4/8.01.

113 ibid.

114 SAFETY4SEA, 'Failing to address cyber risk in SMS may lead to detention in US ports' (SAFETY4SEA, 25 November 2020) <https://safety4sea.com/failing-to-address-cyber-risk-in-sms-may-lead-to-detention-in-us-ports/#:~:text=Failure%20to%20ensure%20cyber%20risk,in%20US%20port%2C%20BIMCO%20warned> accessed 25 November 2020.

4. The case for a comprehensive legal framework on cyber risk management

4.1 A critical analysis of the IMO's regulatory framework on cybersecurity

By design, the MSC-FAL.1/CIRC.3 Guidelines, Resolution MSC.428(98), and the ISM Code are meant to be complementary. However, in practice, ship owners tend to apply only parts of the framework.[115] Currently, there is a lack of uniformity in the application of standards.[116]

Part Four critically analyses the current IMO regulatory framework. Then, it makes a case for a comprehensive legal framework on cyber risk management and discusses general recommendations for the industry.

4.2 Gaps / limitations in the IMO's framework

4.2.1 Outdated rules

One of the criticisms of the IMO framework is that the cybersecurity rules that came into force in 2021 are outdated. MSC-FAL.1/CIRC.3 Guidelines[117] state as follows:

> Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operation personnel or third parties, which may compromise these systems (e.g., inappropriate use of removable media such as memory stick).

The cloud and artificial intelligence systems are now more prevalent in the maritime industry than when MSC-FAL.1/CIRC.3 was introduced, although the 'Guidelines on Cybersecurity Onboard Ships' (incorporated by reference in the MSC-FAL.1/CIRC.3)[118] address the cyber risk posed by cloud-based storage devices. It is possible that the national maritime administrations, while evaluating companies for compliance, will be more focused on the standards set in the MSC-FAL.1/CIRC.3 or more focused on those set out in the 'Cyber Security Onboard Ships' or other standards like the 'ISO/IEC 27001 standard on information technology-security techniques information security management systems- requirements or the standard outlined in the United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity (NIST Framework), all referenced in no. 4.2 and 4.3 of the MSC-FAL.1/CIRC.3 Guidelines.

Certainly, MSC-FAL.1/CIRC.3 supersedes all the other standards referenced within it. This is made clear by the disclaimer at the end of the MSC-FAL.1/CIRC.3 Guidelines indicating that in addition

115 James Rundle, 'Maritime Cyber Rules Coming in 2021 Are Outdated, Critics Say' (Wall Street Journal, 18 June 2019) <www.google.com/amp/s/www.wsj.com/amp/articles/matitime-cyber-rules-coming-in2021-are-outdated-critics-say-11563442201> accessed 17 November 2020.

116 ibid.

117 Guidelines (n 94), no 2.1.6.

118 Guidelines (n 117), nos 4.2 and 4.3. The MSC-FAL.1/CIRC.3 does not address the modern cybersecurity exposures created by mobility, applications, and the cloud.

to the Guidelines, companies are at liberty to adopt any of the aforementioned three standards when preparing their Document of Compliance.

4.2.2 Lack of uniformity

There has been a noticeable inconsistency in the implementation of the requirements embodied in the IMO's regulatory framework on cyber risk management. National and regional institutions are necessary partners in the implementation of IMO's agenda on cyber risk management. Some national institutions, through their port authorities, prioritise the provisions of the International Ship and Port Facility Security Code (ISPS) over those of the ISM Code on cyber risk management.[119]

The ISPS Code requires that companies take appropriate measures on all ships to identify and assess threats and prevent and recover from security incidents.[120] The focus of the ISPS Code is on physical security threats and related protective measures. However, the non- mandatory part B, paragraph 8.3 of the ISPS Code refers to 'computer systems and networks' as elements on board or within the ship that should be addressed in the context of ship security assessments and safeguard against unauthorised access. The ISM Code provides a comprehensive framework for addressing cyber risks that affect the safe and environmentally sound operation of ships, while the ISPS Code focuses on dealing with external threats, malicious actions, and physical security.[121] The cyber risk provisions in the ISPS Code are tied to the approved ship security plan.[122]

In MSC/101/4/4, it was argued that for the sake of uniformity in applying cyber risk management, port authorities should adopt and prioritise the ISM Code instead of the ISPS Code.[123]

Yet, the fact that companies are free to adopt industry developed cybersecurity standards, such as ISO 27001/27002 and the BIMCO standard may lead to uneven application of the rules. The nature of a company's cyber vulnerabilities should determine the type of industry cybersecurity standards the company adopts, it would nonetheless be better if there were more guidance from the IMO regarding the type of cybersecurity standards that should be applied.[124] The BIMCO standard is more tailored towards the maritime industry while ISO 27002 takes a generic approach that can be applied to all industries.[125] The BIMCO standard is more focused on OT while the ISO 27002 is more focused

119 IMO, MSC 101

120 International Ship and Port Facility Security (ISPS) Code (1 July 2004) SOLAS/CONF.5/34 Annex 1, part a, Section 7-9.

121 MSC101/4/4 (n 119) para 9.

122 ibid para 11.

123 ibid para 15.

124 Matthew Allport, 'ISO 27001 vs NIST Cybersecurity Framework' (Compliance Council Blog, 21 December 2018) <https://blog.compliancecouncil.com.au/blog/iso-27001-vs-nist-cybersecurityframework> accessed 7 November 2021. ISO 27001 is an internationally recognised approach for establishing and maintaining an SMS and is geared towards meeting the demands of the General Data Protection Regulation (GDPR). NIST, on the other hand was created primarily to help US federal agencies and organizations better manage their cybersecurity risk, ISO 27001.

125 Stefanos Spanos, 'Cyber Security in the Maritime Industry-A Comparative Study' (Isonike, 13 January 2021) <https://www.isonike.com/?q=node/121> accessed 29 August 2021.

on IT and indirectly focuses on OT.[126] The BIMCO standard applies directly to ships, while ISO 27002 focuses on the organisation and their operating sites.[127]

There are common grounds between the two cybersecurity frameworks and they can be integrated.[128] For instance, the elements of ISO 27002 can be leveraged upon for IT vulnerabilities while the BIMCO standard can be leveraged to address OT vulnerabilities.

Permission to adopt different cyber security standards could constitute a problem if a wrong standard is applied for a particular vulnerability. The essence of the Guidelines is that the right standard is deployed for the right vulnerability. The IMO offering additional guidance or clarity on this would really help maritime companies to know what standard to deploy for a particular vulnerability. Central to the success of the framework is uniformity, in ensuring that like problems or threats are addressed in the same manner.

4.2.3 Lack of crew training

Many crew members do not understand basic cybersecurity requirements or how to recognise / respond threats.[129] 'Without this rudimentary understanding, it is impossible to train crews or take actions to protect assets'.[130] The crew of a ship bears great responsibility under the ISM Code,[131] but the overall responsibility lies with the master.[132] According to the ISM Code, one of the duties of the master is to review the effectiveness of the SMS and verify compliance with specific requirements.[133] The master is required to report any noted deficiencies in the SMS to the shore-based management.[134] More training is needed for crew so they know how to comply with cybersecurity protocols through prevention, response and recovery in event of cyber disruption. Although there are now Standards of Training, Certification, and Watchkeeping (STCW) designed cybersecurity courses for crew members, a lot of companies are yet to take advantage of this, for example the Nautical Institute provides training courses.[135]

126 ibid.

127 ibid.

128 ibid.

129 According to Andrew Kinsey, Marine consultant at Allianz, see *Rundle* (n 115) para 19.

130 ibid.

131 ISM Code (n 110) no 6.

132 ibid no 5.

133 ibid no 5.1.4.

134 ibid no 5.1.5.

135 The Nautical Institute, 'Cyber Security at Sea' (Institute News, 25 May 2021) <www.nautinst.org/career-development/ni-academy/online-courses/cyber-security-at-sea.html> accessed 11 January 2021.

4.2.4 Sanctions

Another criticism is the question of liability that might arise out of a company's failure to adhere to the IMO Framework. For example, ships use AIS, which means that ships are increasingly connected to each other and to port terminals.[136] As stated earlier in this paper,[137] sanctions embedded in the ISM Code such as withdrawal of SMS certificate are now applicable in the event of failure of a maritime company to comply with the framework. Suppose a chartered ship linked with the fleet of a maritime company was hacked due to the failure of the owner of the chartered ship to effectively address its cyber vulnerabilities. In this case, there are no sanctions in the ISM Code for the chartered ship. Another illustration is when a maritime company IT infrastructure was hacked but the fault is that of the IT support services provider who failed to address its cyber vulnerabilities. There are no assigned roles or sanctions for IT support service providers in the maritime industry in the IMO framework.

4.2.5 The IMO framework appears very ship-focused

An integral part of the IMO framework on cyber risk management is the mandate for 'companies to address and incorporate cyber risk management into their SMS'. As stated earlier, the goal of the ISM Code is to ensure safety of life (marine and non-marine) at sea. Asking maritime companies to anchor their cyber defence on the SMS suggests that the priority of the IMO framework on cyber risk management is to prevent cyber-attacks on board a ship or when a ship is at sea. However, the most devastating cyber-attacks (NotPetya ransomware attack suffered by Maersk, data centre attack on the Mediterranean Shipping Company, COSCO and CMA CGM) so far suffered by the maritime industry have targeted shore-based systems such as offices, data centres and container booking systems.[138] As rightly stated by Ken Munro[139] 'if you can't book a container, there's no point in having the ship'. A cyber defence strategy anchored on the SMS, will ensure that prevention of cyber-attacks on board ships is prioritised more than the shore-based systems. Admittedly, a successful cyber-attack at sea, as shown later in this paper, could prove more devastating than reported attacks to date. However, equal attention must be paid to shore-based systems.

4.3 The case for a comprehensive legal framework on cyber risk management

Although progress has been made by incorporating cybersecurity into the ISM Code, some experts believe that work remains to be done to avoid catastrophic effects of cyber-attacks on the maritime industry. The maritime industry lags behind other industries in terms of cyber threat preparedness. According to Rory Hopcraft and Martin Keith, in the aviation industry, cyber threat is approached

136 Hassiba Benamara, Jan Hoffman, Luisa Rodriguez and Frida Youssef, 'Container Ports: The Fastest, the Busiest, and the Best Connected' (UNCTAD, 07 August 2019) <https://unctad.org/news/container-portsfastest-busiest-and-best-connected> accessed 13 December 2020.

137 ISM Code (n 131) no 3.4.

138 Catalin Cimpanu, 'All Four of the world's largest shipping companies have now been hit by cyber-attacks' (ZDNet, 28 September 2020) <www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/> accessed 2 December 2020.

139 A cyber security researcher at Pen Test Partners, ibid.

from a security perspective rather than through the lenses of insurance.[140] In other words, the aviation industry does not allow increased cost of insurance to influence its cyber defence or resilience strategy.

According to a survey of more than 2400 risk management experts in the maritime sector conducted in 2019 by Allianz in its Allianz Risk Barometer 2019, cyber incidents are the second most significant risk in the maritime sector.[141] The study estimated that a cyber-attack at sea in a worst-case scenario leading to collision and grounding of two large vessels in an environmentally sensitive location could result in the significant loss of life, untold environmental damage and financial losses totalling as much as US$4 billion, which includes wreck removal expenses of the two ships, passenger, and crew liabilities of the two vessels, litigation costs for the two vessels, and cargo liabilities etc.[142]

The role for the IMO to create a comprehensive legal framework on cyber risk management is challenged by the complicated nature of cyber risk. The linkage between onboard and terrestrial systems creates problems for the IMO.[143] Although UNCLOS has created obligations for flag and non-flag states, much of the infrastructure that enables communication between ships and control towers is land based, which means it is outside the control of the IMO. This land-sea infrastructure interdependence makes it more challenging for the IMO to address cyber risk alone without the involvement of sovereign states which regulate and own the infrastructure. For instance, the issue of submarine cabling is often met with resistance and outright rejection within IMO discussions.[144] This demonstrates the fact that the cybersecurity challenge is an interdependent global challenge which requires international collaboration, coordination and communication to resolve.[145]

Another complexity is that many ships are equipped with specialist equipment not designed with cybersecurity in mind. The different OT found on ships has made it difficult for the IMO to formulate uniform cybersecurity Guidelines, especially since the manufacturers of the OT are also different.

The above complexities likely account for the IMO's ad hoc and perhaps soft approach to the issue

140 Hopcraft Rory and Martin Keith, 'Effective Maritime Cybersecurity Regulation - The Case for a Cyber Code'(2018) 14(3) JIOR; The One Brief, 'Finding the Weak Link in the Supply Chain: Cyber Lessons from the Aviation and Marine Industries' (2017) <https://theonebrief.com/supply-chain-cyber-lessons-aviationmarine/> accessed 2 December 2020. tries' (2017) <https://theonebrief.com/supply-chain-cyber-lessons-aviationmarine/> accessed 2 December 2020.

141 In a survey of over 2400 risk management experts in the maritime sector conducted in 2019 by Allianz in its Allianz Risk Barometer 2019, cyber-attacks were ranked second next to natural catastrophe as the most important threats to the maritime industry. See Allianz Global Corporate and Specialty, 'Safety and Shipping Review 2019' (2019) <www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review2019.pdf> accessed 11 November 2020.

142 ibid 6.

143 Hopcraft and Martin (n 140).

144 ibid 3 and 9.

145 ibid 9.

of cybersecurity.[146] Legislation in this industry tends to be passed at an alarmingly slow pace.[147] Often, it is hardly possible to negotiate a new convention or amendment to an existing convention without running into conflicts with existing conventions.[148] The 'Tacit Acceptance Procedure' is used by the IMO to fast track the amendment of an instrument. This procedure allows an amendment to take effect on a specific date unless objections from a specified number of parties are received.[149] Tacit acceptance procedure has been criticised for deviating from the general principle of international law, which only allows a treaty to be binding on the States that expressly consent to it.[150]

In response to this bureaucratic challenge, the IMO uses codes to enforce regulations and ensure safe shipping. The IMO derives its authority from SOLAS to use codes to enforce safe shipping.[151] SOLAS among others[152] is the umbrella instrument for codes, which are adopted under its authority through a provision in the convention as amended by an MSC resolution, which provides authority for the code. These Codes are ISM Code, International Code for Ships Operating in Polar waters 2017 (this falls under both SOLAS and MARPOL) and the International Ship and Port Facility Security (ISPS) Code 2004.

Some scholars,[153] have called for the creation of a cyber code, a necessity in the maritime industry, which would create independent guidance and regulations to comprehensively address cyber risk management in the maritime industry in the manner of the Polar Code. The Polar Code stipulates regulations applicable to ships working in polar waters and includes mandatory provisions enforceable under the SOLAS convention and MARPOL for the Part II provisions. The goal of the Polar Code is to promote maritime safety in polar waters, preservation of marine environment and protection of local economies from potential casualties.[154]

---

146 The IMO's legal framework on cyber risk management can be described as soft. According to Shaffer and Pollack, "the realm of soft law begins once legal arrangements are weakened… if an arrangement is formally binding but its content is vague…[and] if an agreement does not delegate authority to a third party to monitor its implementation or to interpret or enforce it"; Gregory C Shaffer and Mark A Pollack, 'Hard vs Soft Law: Alternatives, Complements and Antagonists in International Governance' (2010) 94 (706) MLR, 715.

147 A good example is The International Convention for Control and Management of Ships 2004.

148 Erik Rosaeg, 'Soft Law in the Conventions of Maritime Law' (1996-2015) Sc. St. L 270.

149 Capt Rajeev Jassal, 'Understanding IMO Conventions, Resolutions and Circulars' (MySeaTime, 25 January 2016) <www.myseatime.com/blog/detail/understanding-imo-conventions-resolutions-andcirculars> accessed 3 December 2020.

150 Shi Le, 'Successful Use of the Tacit Acceptance Procedure to Effectuate Progress in International Maritime Law' (2016) 11(2) U.S.F MLJ.

151 The International Convention for the Safety of Life at Sea Convention (adopted 1 November 1974, entered into force 25 May 1980) 1184 UNTS 3, SOLAS vests the IMO with the authority to regulate maritime shipping to ensure safety, security, legal and efficiency standards.

152 SOLAS is not the only one; we have the STCW Convention too.

153 Hopcraft and Martin (n 143) 7.

154 Aldo Chircop, 'Sustainable Arctic Shipping- Are Current International Rules for Polar Shipping Sufficient?' (2016) 11(3) JOT 39-51.

4.3.1 The Polar Code as a model

The Polar Code is a good example to follow because it is 'holistic, goal-oriented and risk- based'.[155] It is a functional based regulation model in that 'the rules are goal oriented so that ship owners are expected not to simply comply with a standard or rule but also to produce the expected safety and environmental outcomes'.[156]

The Polar Code is divided into two parts: maritime safety and marine environment protection. Each part has separate section of mandatory rules (Part IA and Part IB and recommendations (Part IB and IIB).[157] Part I covers a broad range of matters such as design, construction, and equipping(certification and surveying, ship structure, stability and subdivision, watertight and weathertight integrity, machinery installations, fire safety, life-saving appliances and arrangements), operations (manual on board, safety of navigation, communication, voyage planning), and crewing (manning and training familiarity)[158] It also provides for the training of polar seafarers in accordance with the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers 1978 (STCW).[159]

4.3.2 A Standalone cyber code

A standalone cyber code that provides for the phasing out of ships and ship designs incompatible with modern cyber defences, periodic mandatory training for crew on cyber security, and a forum for dispute settlement will go a long way in addressing the threat posed to global trade by cyber-attacks.

It has been argued that the use of a cyber code would allow the IMO to emphasise the long-term and specific risks of cybersecurity.[160] It has also been argued that a cyber code will allow for the harmonisation of the different and discrete rules that regulate shipping and the various technical councils that form the IMO. Inputs from different ship registries and administrations, local authority and expertise formed part of the making of the Polar Code. Therefore, a single standalone cyber code would allow for the harmonisation of different regulations into one benchmark document, making it easier to implement and update according to current cyber risk realities.[161] Creating a standalone cyber code that would create responsibilities for the International Association of Classification Societies (IACS) would assist in addressing the challenge. IACS members are engineering organisations who regulate ship design. Creating a role for classification societies in the framework would aid addressing of the problem of cyber security within the maritime industry. IACS can assist the phasing out of ships that are vulnerable to cyber-attacks and lead to the introduction of cyber resilient ships that will meet the requirements of the framework. Classification societies have been involved informally in the process of preparing the

155 ibid 46.

156 ibid.

157 ibid.

158 ibid.

159 ibid 47.

160 Hopcraft and Martin (n 153) 7.

161 ibid 7.

maritime industry for a cyber resilient future. For instance, Classification Society DNVGL on 1 July 2018 published its first-class notations called 'Cyber Secure', aiming to help ship owners and operators protect their assets from cyber security threats.[162] This informal role of classification societies could be formalised under a standalone cyber code.

The IMO drawing from the lessons learnt from the application of the ISM and ISPS Codes on cyber risk management should promote the formulation of a cyber code.[163] The maritime industry is not yet receptive to the idea of a cyber code. In fact, the prevailing view is that the ISM Code and SOLAS Chapter IX support effective cyber risk management, and that the ISM Code, more than the ISPS Code, should take the lead in combating cyber-attacks.[164]

Over the past two decades, the ISM Code has made shipping safer and cleaner. In a study commissioned by the IMO in 2005, a group of experts concluded that: 'where the Code is embraced as a positive step toward efficiency through a safety culture, tangible positive benefits are evident.'[165] The ISM Code is not without its critics. One of the criticisms is that the SMS documentation is too lengthy, and contains too much unnecessary text, that could be easily replaced by flow charts and diagrams.[166] The second criticism is that SMS documentation should be ship specific, rather than one size fits all documentation.[167]

An effective legal framework must have a strong enforcement regime. If a code contains sanctions and the sanctions are not enforced, the code is useless. In the maritime industry, flag administrations, classification societies and port state controls are the enforcement authorities. The ISM Code faces implementation challenges. However, if implemented effectively, it would bring many benefits.[168]

This implementation challenge must be addressed by the IMO since the ISM Code is a part of the ground on which the fight against cyber-attacks is based. The IMO should encourage the various port state controls to buy into the IMO's agenda on cyber risk management. Port state control provides inspection of foreign ships in national ports to verify that the condition of the ships complies with international requirements such as the ISM Code among others. The Memoranda of Understanding on Port State Control is the instrument that authorises national port authorities to enforce internation-

---

162 SAFETY4SEA, 'DNVGL issues cyber security class notations' (SAFETY4SEA, 8 June 2018) <https://safety4sea.com/dnv-gl-issues-cyber-security-class-notations/> accessed 10 December 2020.

163 ibid 11.

164 MSC101/4/4 (n 121). It was agreed that all aspects of cyber risk management, including physical security aspects of cybersecurity, should be addressed in Ship Security Plans under the ISPS Code. However, this should not be deemed as requiring a company to establish a separate cybersecurity management system operating in parallel with the company SMS.

165 Vandenborn (n 68).

166 ibid.

167 ibid.

168 Captain Rajeev Jassal 'Seven Important Elements of ISM Code every seafarer must know about' (Seatime Blog, 4 December 2016) <www.myseatime.com/blog/detail/7-important-elements-of-ism-Codeevery-seafarer-must-know-about> accessed 12

al maritime regulations/instruments through inspection of ships.[169] By establishing more consensus among IMO member states, the IMO can address the likely enforcement challenge that may beset cybersecurity standards in the ISM Code.

4.4 Conclusion and recommendations

As it has been shown, the IMO needed to react to the spate of cyber-attacks by coming up with a framework on cyber risk management. The IMO's framework can be described as preliminary and evolving because it started as voluntary and eventually has an ISM Code dimension and may evolve further.

Cybersecurity in the maritime industry is very important, the IMO and the industry cannot afford to be lax about cyber defence. Though full cyber resilience is not realistic or achievable, the industry can do more to improve its cyber defences. The maritime industry continues to rely on artificial intelligence, autonomous systems, and other emerging technologies, with the ultimate goal of deploying ships that can roam the seas uncrewed.[170] To be able to effectively respond to cybersecurity challenge, the maritime industry needs to invest heavily in cyber defence technologies, such as anti-spoofing technology among others.

It has also been shown that the current legal framework on cyber risk management is inadequate. The maritime industry needs a strengthened comprehensive legal framework for cyber risk management. In this article, suggestions for improving the ISM Code have been proposed. However, the ideal course of action is to have a dedicated cyber code adopted to the SOLAS Convention. It is clear from the analysis in this paper, that the approach of the industry to cyber risk management is still lax and could be improved. The IMO should not wait for a major disaster to occur.[171] The approach to cyber risk management should be proactive not reactive.

169 There are ten Port State Control regimes that have been signed thus far. They are: Europe and the North Atlantic (Paris Memorandum of Understanding); Asia and the Pacific (Tokyo Memorandum of Understanding); Latin America (Acuerdo de Viña del Mar); Caribbean (Caribbean Memorandum of Understanding); West and Central Africa (Abuja Memorandum of Understanding); the Black Sea region (Black Sea Memorandum of Understanding); the Mediterranean (Mediterranean Memorandum of Understanding); the Indian Ocean (Indian Ocean Memorandum of Understanding); and the Riyadh Memorandum of Understanding. The United States Coast Guard maintains the tenth PSC regime.

170 Rundle (n 115).

171 It appears that the IMO has formed the habit of waiting for a major disaster to happen before stepping up to address the problem. It was a series of serious shipping accidents in the 1980s, the worst of which was the roll-off ferry Herald of Free Enterprise that capsized at Zeebrugga in 1987, killing 193 of its 539 passengers and crew that led to the enactment of the ISM Code. See Vandenborn (n 165).