UiO : Faculty of Law
University of Oslo

Cyber-worthiness:

The duty to make the vessel seaworthy with respect to cybersecurity

Candidate number: 510

Submission deadline: 1 December 2021

Number of words: 17,865 words

TABLE OF CONTENTS

1. Introduction

Maritime transport and port operations play a crucial role in world trade. The exposure of the vessels, ports or offshore entities (like oil and gas rigs and drilling platforms) to different threats can lead to devastating consequences for the shipping industry and jeopardize the supply chains of several sectors. The implication of such threats could have a tremendous outcome on international trade. Information technology has become the utmost important part of every industry, and the shipping sector is no exception. Indeed, in the past decade, there has been an exponential increase in the use of computer-based technologies.[1] It was the transport sector that was among the first industries to experience the introduction of new technologies. Nevertheless, along with its advantages, digitalization brought many risks and challenges. The growth of computer-based systems causes an increase in sophisticated malware, in addition to ever-persistent cyber threats. As technology has advanced, the physical hazards to ships are no longer the greatest threat a vessel may face. Technological threats are now those that outshine the classic physical dangers (such as piracy, armed robbery, or drug smuggling). Hence, one can argue that the threats have shifted from physical space to cyberspace. As well as many other sectors, the shipping industry is no exception and thus can also be vulnerable to cyber-attacks. Cyber-attacks can have many targets. Among others, the perpetrator can attack ports and disrupt their safe operation, or else he can target businesses and steal valuable information. He can as well target offshore entities such as oil and gas industry rigs or drilling platforms. Or what, may be worse, the attacker can target vessels themselves. Therefore, ships and their safe operation can fall into the category of targets that are most vulnerable to cyber-attacks. Additionally, shipowners often underestimate the power of cyber-attacks because no direct threat to the organization is visible. To prevent attacks and to protect his property, it is the shipowner's responsibility to ensure that his ships are cyber-resilient against cyber-attacks. According to Resolution MSC. 428(98)[2] produced by the International Maritime Organization (hereinafter 'IMO'), shipowners and ship operators are required to take into account cyber risk management. Hence, they should be able to identify cyber-related risks and avoid, transfer, or mitigate their

[1] SHM, 'Impact of maritime security on the global maritime industry' (*shmgroup*, 12th May 2019) <https://www.shmgroup.com/blog/impact-of-maritime-security-on-the-global-maritime-industry/> accessed 19 November 2021.
[2] International Maritime Organization, Maritime Cyber Risk Management in Safety Management Systems, 16 June 2017 (Resolution MSC.428(98)).

impact.[3] Thus, cyber risk management is becoming a natural extension of existing safety and security management practices. Therefore, a shipowner's risk management system should now include some level of cyber risk management.

Since cyber risk management in maritime transport should now be integrated into existing risk management processes, as set out in the IMO Resolution MSC. 428(98). When we look at the matter in a narrower context, one could debate that the carrier has an implicit obligation to take all reasonable measures to protect the ship, together with its cargo, from cyber-attacks.[4] In this manner, we can assume that this obligation could fall under the scope of the duty of the carrier to make the ship seaworthy.[5] Thus, a question arises of whether cybersecurity and cyber risk management form part of the carrier's duty to make the vessel seaworthy, and hence, whether a failure to exercise cyber risk management renders a ship unseaworthy.[6] Consequently, could the failure of the carrier to take measures against cyber risk to be equal to failure to exercise due diligence in making the vessel seaworthy?[7] As will the following chapters of this work specify. Exercising due diligence means taking all reasonable precautions so that the ship is fit for the voyage contemplated. So, if the carrier does not have proper cyber risk management in place, does it mean that he did not take all reasonable precautions so that the vessel is ready for the voyage? Furthermore, could cyber threats result in the carrier being exempt from liability under Art. IV of the Hague-Visby Rules? The following chapter will seek to answer these questions and examine whether or not cyber security indeed forms a part of seaworthiness and whether a failure of the owner to exercise cyber risk management mean that the carrier failed to exercise due diligence hence rendering the vessel unseaworthy.

[3] ibid.
[4] Dr iur Bűlent Sőzer, 'Seaworthiness: In the context of cyber-risk or "cyberworthiness"' in Barış Soyer and Andrew Tettenborn (eds), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (1st edn, Informa Law from Routledge 2020).
[5] ibid.
[6] ibid.
[7] ibid.

Chapter Review

The following thesis consists of three chapters. The first chapter aims to describe what does the notion of seaworthiness entails. The objective of this chapter is to introduce the concept. Hence, the chapter focuses on the definition of seaworthiness, the elements of seaworthiness, and the inherent duty that the shipowner must make the vessel seaworthy. The second chapter introduces the concept of cybersecurity in the maritime sector. The focus of this chapter is on different cyber security threats that are endangering the shipping sector. Furthermore, the chapter pays attention to the international framework addressing cybersecurity-related issues in the maritime industry and addresses whether this framework is efficient in what is said to do. Finally, the third chapter focuses on cybersecurity and cyber risk management. This chapter aims to address whether cyber risk management forms part of seaworthiness. It furthermore examines whether a failure of the carrier to take measures to protect the ship, together with its cargo from cyber-attacks, equals a failure of the carrier to exercise due diligence.

Methodology and Sources

Throughout the analysis, various statutory instruments and sources are utilized. These are applied to affirm a point or provide examples. Concerning seaworthiness, the majority of sources relate to case law. The primary purpose of use of this source is to give examples of situations where the vessel might be unseaworthy. The second type of source used in the analysis of seaworthiness are rules related to the Carriage of Goods by sea. These include, for example, the Hague-Visby Rules, the Hamburg Rules, or the Rotterdam Rules. These introduce the nature of the duty to make the vessel seaworthy. Concerning cyber security, the primary source is international legislation. Here the main focus falls on international legal documents produced by the United Nations and International Maritime Organization. Their central purpose is to introduce the concept of cybersecurity and the recommendation that the international community proposes to raise awareness of cyber-related threats. While the first two chapters were descriptive, the last chapter is more analytical. It analyses whether the shipowners' duty to make the vessel seaworthy encompasses cybersecurity and cyber risk management. Here it once again resorts to the Hague-Visby rules and elaborates on the work of Dr iur Bűlent Sőzer on Seaworthiness in the context of cyber-risks or “cyberworthiness”.

2. Chapter I: The concept of seaworthiness

Marine transport, in particular, the carriage of goods by sea, forms an integral part of the supply chain for many industries.[8] Ergo it is deemed to be a foundation of world commerce. Since the early 1990s, the volume of worldwide seaborne trade has grown exponentially from 4.1 billion tons in 1990 to an astounding 11.08 billion tons in 2019.[9] Unsurprisingly, it is now estimated that the vast majority of goods, around 80 percent, are transported by sea.[10] Hence, it is essential to ensure that such a highly profitable industry function efficiently, is kept safe and well-protected against outside threats, and does not pose any risk to the environment.[11] Therefore, it is necessary to guarantee that the maritime transport sector is constantly regulated. So, it can keep pace with technological developments in industry and world trade.[12] The shipping industry is fully aware of the growing risks to cyber security and has taken several steps to combat these threats.[13] However, the importance of cybersecurity in building a safe and sustainable maritime environment is expected to increase even further in the upcoming years.[14] There are many causes as to why cyber security breaches occur. The most common causes of cyber security breaches relate to a lack of knowledge or negligence on the part of the staff, shortcomings in equipment such as missing updates, or outdated software. So, to keep the marine industry safe and environmentally friendly, it is crucial to ensure that all ships maintain the highest possible standards relating to their construction and maintenance, quality of equipment, crew competence and training, and safety standards.[15] Otherwise, not following the appropriate regulations could have an enormous consequence and impact on the functioning of the industry

---

[8] Young-Chan Lee, Sang-Kyun Park, Woo-Kun Lee, Jun Kang, 'Improving cyber security awareness in maritime transport: A way forward' [2017] 41(8) Journal of the Korean Society of Maritime Engineering 738.
[9] Statista Research Department, 'Transport volume of seaborne trade from 1990 to 2020' (*statista*, 22 November 2021) <https://www.statista.com/statistics/264117/tonnage-of-worldwide-maritime-trade-since-1990/> accessed 19 November 2021.
[10] Martin Placek, 'Ocean shipping worldwide – statistics & facts' (*statista*, 9 August 2021) <https://www.statista.com/topics/1728/ocean-shipping/> accessed 19 November 2021.
[11] Ahman Hussam Kassem, 'The Legal Aspects of Seaworthiness: Current Law and Development' (DPhil thesis, University of Wales 2006).
[12] ibid.
[13] SHM (n. 1).
[14] ibid.
[15] Kassem (n 11).

and the marine environment. Hence, a great duty arises for the shipowner to make the vessel seaworthy. To protect the ship and its cargo from unwanted threats and thus defend the industry and the environment.

Historically, under common law, the shipowner's duty to provide a seaworthy vessel has been one of the most fundamental principles of maritime law.[16] Therefore, this obligation had and still does form a vital part of every carriage of goods contract.[17] Depending upon rules applicable to the situation in question, the shipowner or the carrier has an important obligation to provide a seaworthy vessel.[18] Because if he does not provide a seaworthy vessel, it can have terrible consequences for himself. Or it may endanger the interests of the cargo owner, employees, the environment, and other directly or indirectly involved parties. Over the decades, the definition of seaworthiness has been a subject of many discussions. Yet, even now, there is a lack of consensus in this respect.[19]

2.1. The notion of the carrier and the shipowner

In cases where the transportation of goods is at stake, the party that assumes responsibility for the goods in issue is the carrier.[20] Making a vessel seaworthy is a unique obligation inherent in maritime law and hence is closely linked to contracts for the carriage of goods by sea.[21] In this sense, it imposes an obligation on the carrier who is a party to the contract to make the ship seaworthy. Hence the carrier is consequently held accountable if he does not discharge this obligation properly.[22] In many of the decisions adjudicated by the English Courts[23] or in the

[16] Yilmaz Mustafa, 'Legal Assessment of Seaworthiness in Autonomous Cargo Ships: Is It Time for a Change?' 2020 3(2) DEHUKAMDER 803-866.
[17] ibid.
[18] Indicated will be analyzed further in detail in the following section.
[19] Mustafa (n 16).
[20] Here, the carrier may or may not be the shipowner.
[21] Sőzer (n 4).
[22] ibid.
[23] An example of the shipowner being the responsible party can be found, in *Union Steamship Co. of British Columbia v. Drysdale* [1902] 32 SCR 379. Where Lord Blackburn remarked that "In the case of *Kopitoff v. Wilson*, where I had directed the jury that there was an obligation, I did certainly conceive the law to be that the shipowner in such a case warranted the fitness of the ship when she sailed, and not merely that he had loyally, honestly and bonâ fide endeavored to make her fit."

English literature,[24] the authors indicate that the party that has an absolute duty to provide a seaworthy vessel is the shipowner. Yet, the international conventions[25] governing this subject, as well as several domestic laws,[26] suggest otherwise. These indicate that the obligation to exercise due diligence to provide a seaworthy vessel falls within the competence of the carrier. Hence, making him accountable for taking all measures necessary to make the vessel seaworthy. All this follows from the fact that the carrier is a contractual party to the contract of carriage of goods by sea. Given the above, based on the context, the words carrier and shipowner will be used interchangeably.

2.2. Nature of the Duty

The obligation to provide a seaworthy vessel that is seaworthy is a personal responsibility.[27] Thus, it falls within the competence of the shipowner or the carrier. However, the center of duty to make a ship seaworthy does not lie merely in the fact that the shipowner is personally diligent.[28] It further requires that diligence is exercised by the shipowner or by those whom he employs for that purpose.[29] The personal nature of the duty is the same under common law, the Hague-Visby Rules, Hamburg Rules of the Rotterdam Rules. But what is changing is its nature. On the one hand, under common law, the shipowner has an absolute obligation to provide a seaworthy vessel. Such entails that the shipowner has a strict obligation to provide that the vessel is seaworthy.[30] However, this does not mean that the ship must be perfect in all circumstances. It does not require that the vessel can withstand any danger during its voyage.

---

[24] Concerning English literature, Carver on Charterparties makes a great example of a shipowner being the responsible party. Here Carver states the following: "Unless there is an express term to the contrary, every charter party contains an implied undertaking by the shipowner that the ship is seaworthy, which arises by reason of his acting as shipowner."
[25] HVR, Art. I(a), Art. III (1).
[26] The Norwegian Maritime Code (1994), Chapter 6, Section 131, The master shall before a voyage begins ensure that the ship is seaworthy," or The Croatian Maritime Code (1994), Article 479, "The ship operator of a sea-going ship shall be bound in due time, before commencing the voyage, to exercise the due diligence of a conscientious ship operator in making the ship seaworthy."
[27] Kassem (n 11) p. 71-87; *Paterson Steamship Ltd. v. Robin Hood Mills Ltd*, (The Thordoc), (1973) 58 LI.L. Rep. 33.
[28] Kassem (n 11) p. 71-87.
[29] ibid.
[30] ibid.

It merely implies that the ship must be fit for the purpose of its contracted voyage.[31] Therefore, it must be reasonably fit in all respects to meet the ordinary perils of the seas that she is likely to encounter on her journey. The shipowner must prove not only that he has done everything in his power to make the vessel seaworthy. But that also the vessel is genuinely fit for the purpose of her voyage.[32] Consequently, if the carrier violates his obligation, he would be held liable whether or not he was to blame.[33] But, on the other hand, if the shipowner can prove that he indeed provided a seaworthy ship, he would be discharged from his obligation and thus would not be responsible for any loss. The concept of due diligence has a different nature from the absolute duty to provide a seaworthy vessel as introduced in the common law. The following section examines the history of the concept of due diligence. For the time being, it is necessary to mention that the notion of due diligence was for the first time introduced by the Harter Act in 1893.[34] It was then later adopted by the Hague/Hague-Visby Rules, Hamburg Rules, and the Rotterdam Rules.[35] According to the Cambridge Dictionary, diligent means being "careful and using a lot of effort." Therefore, in maritime law, in the context of seaworthiness, due care means that the carrier must take all reasonable measures at his disposal to ensure that he, his servants, or agents did everything to make the vessel seaworthy in all respects.[36] Thus, the carrier must be careful, rational, and honest in his duty to make the ship seaworthy.[37] Unlike common law, the concept of due diligence as introduced in the Hague-Visby Rules does not provide an absolute obligation. It stipulates a positive obligation for the carrier,[38] which he must exercise if he wants to enjoy the protection of the Rules in Art. IV(1)[39]. If, in any case, the carrier fails to provide a seaworthy vessel but has reasonable grounds to do so and can

---

[31] In *President of India By and Through Director of India Supply Mission v. West Coast S. S. Co*. [1964] 327 F/2d 638 (9th Cir. 1964), the court stated the following "Duty to furnish seaworthy ship is absolute and limited neither by concepts of negligence nor contract, but obligation does not require furnishing accident-free ship or ship or gear which may withstand all conceivable hazards, but only to furnish ship and equipment reasonably suitable for intended use or service."

[32] Kassem (n 11) p. 71-87.

[33] ibid.

[34] ibid.

[35] ibid.

[36] ibid.

[37] 'Due diligence' (*Ship Inspection*, date unknown) <http://shipinspection.eu/due-diligence/> accessed 19 November 2021.

[38] Kassem (n 11) p. 71-87.

[39] Art. IV(1) of the HVR, "Neither the carrier nor the ship shall be liable for loss or damage arising or resulting from unseaworthiness unless caused by want of due diligence on the part of the carrier to make the ship seaworthy."

demonstrate that he has exercised due diligence, he may not be liable for a breach of the obligation and exempt himself from the liability.[40] However, if the shipowner has not exercised due diligence, he will not be able to benefit from the protection provided by Art. IV(2).[41] The burden of proof, therefore, lies with the carrier or another person claiming exemption.[42] Who must prove that he or the persons for whom he is responsible have taken due care to make the ship seaworthy.[43] Furthermore, the carrier is legally responsible for the failure of his employees to exercise due diligence.[44] Hence, if the authorized person was not diligent, then this will cause the carrier to fail to show his diligence.[45]

2.3. Definition of seaworthiness

The definition of seaworthiness does not differ much between the various sectors of the law of the sea. In fact, it is comparable in all respects. Nevertheless, depending on the type of contract between the interested parties, two main concepts of seaworthiness exist. One exists in the field of Marine Insurance and the other in the Carriage of Goods by Sea. Nonetheless, both branches of law accept the notion of seaworthiness as relative and quite complex. The following section provides a closer look at both definitions. The review will begin with an explanation of seaworthiness under the Carriage of Goods by Sea. Which then will be followed by the definition of seaworthiness under Marine Insurance Law.

---

[40] 'Duty to provide a seaworthy vessel' (*Ship Inspection*, date unknown) <http://shipinspection.eu/duty-to-provide-a-seaworthy-vessel/> accessed 19 November 2021.
[41] HVR, Art. IV(2) provides an extensive list of exemptions to carrier's liability.
[42] HVR, Art. IV(1).
[43] *Papera Traders Co Ltd. v. Hyundai Merchant Marine Co Ltd.* [2002] EWCH 253 (Comm).
[44] *Maxine Footwear Company Ltd. v. Canadian Government Merchant Marine Ltd. (The Maurienne)* [1959] 2 Lloyd's. Rep. 105., "It is not enough to satisfy the condition that the shipowner has been personally diligent, as by employing competent men to do the work. The condition requires that diligence to make her fit shall, in fact, have been exercised, by the shipowner himself, or by those whom he employs for the purpose."
[45] *Riverstone Meat Co Pty Ltd. v. Lancashire Shipping Co ('The Muncaster Castle') [*1961] A.C 807.

2.3.1. Definition of seaworthiness under Carriage of Goods by Sea

Since 1876,[46] the applicable laws and standards concerning seaworthiness in the maritime transport of goods have changed considerably. Initially, seaworthiness was a subject that fell under the ambit of common law.[47] It later became the main topic of the Harter Act in 1893. And its importance has grown ever since it became part of the International Convention on the Unification of Certain Laws Relating to the Bill of Lading (also known as the Hague Rules of 1924).[48] It was later adopted by the Brussels Protocols in 1968 that brought additional amendments to the Hague Rules, bringing them to the current version colloquially referred to as the Hague-Visby Rules (hereinafter 'HVR'). In addition to the Hague-Visby Rules, seaworthiness is now part of the 1978 United Nations Convention on the Carriage of Goods by Sea of (the Hamburg Rules) and the 2009 United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea of (the Rotterdam Rules). Despite all the changes and developments, the definition of seaworthiness did not change much as it still includes the same core principles. However, where there has been a change, is within the underlying duty of the shipowner or carrier to secure a seaworthy vessel.

Kopitoff v. Wilson[49] (1876) provides one of the oldest and widely recognized descriptions of seaworthiness under common law. Here the definition reads as follows: the vessel needs to be "...fit to meet and undergo the perils of the sea and other incidental risks to which of necessity she must be exposed in the course of the voyage."[50] Noticeably, the wording suggests that the concept of seaworthiness is limited to the condition of the vessel itself. It does not attempt to go beyond to cover other aspects that now form classic elements of seaworthiness, such as its cargo-worthiness or the competency of the crew. In *McFadden v. Blue Star Line*,[51] judge Channell J went a step further when defining seaworthiness. In his judgement, he identified seaworthiness as "... that degree of fitness which an ordinary careful and prudent owner would require his vessel to have at the commencement of her voyage having regard to all the probable circumstances of it."[52] In his opinion, he decided to cite Carver on Carriage by Sea, who

[46] *Kopitoff v. Wilson* (1987) 1 Q.B.D. 377.
[47] Kassem (n 11) p. 1-12.
[48] ibid.
[49] *Kopitoff v. Wilson* (1987).
[50] ibid p. 380.
[51] *McFadden v. Blue Star Line* [1905] 1 KB 697.
[52] ibid p. 706.

introduced a test to determine whether or not the shipowner exercised his duty to provide a seaworthy vessel.[53] The test produced by Carver is objective and reads as follows: "Would a prudent owner who knew about a defect on a vessel have required the defect to be fixed before sending the ship on her voyage?"[54] If the owner would indeed require the correction of the defect, then the ship was not seaworthy within the meaning of the test. Hence the test is impartial, as it takes into consideration the conduct of a prudent shipowner. In addition, to the decision made by the shipowner, the circumstances surrounding the ships' situation at the time of voyage also shall be considered.[55] As well as the degree of knowledge and standards available and prevailed at the time when the condition occurred.[56]

The introduction of the Harter Act in 1893[57] did not amend the definition of seaworthiness itself. However, it has changed the nature of the obligation.[58] It introduced a so-called minimum requirement for the shipowner to exercise due diligence in order for the vessel to be able to navigate.[59] Unlike, under the traditional definition provided in *Kopitoff v. Wilson*, under Section 191[60] of the Harter Act, the conditions of seaworthiness go further beyond the state of the vessel itself and include other aspects.[61] Per Section 191, the owner is under the obligation to "exercise due diligence and properly equip, man, provision, and outfit his vessel to make her seaworthy and capable of performing her intended voyage."[62] The Act did not make the exercising of due diligence an obligation. However, it provided a means to prevent the carrier from contracting himself out of his duty to provide a seaworthy vessel and exercise due care concerning the cargo.[63] The Harter Act can be consequently seen as a compromise between the interests of the cargo owner and the carrier and provided the first step towards increasing the carrier's liability.[64]

---

[53] Kassem (n 11) p. 15.
[54] ibid.
[55] In deciding the seaworthy condition of the vessel, the court, in addition to the prudent owner test, examines, for example, the type of ship, the intended route, type of cargo planned to transport, the season of the year, or the type of waterway.
[56] Kassem (n 11) p. 16.
[57] Harter Act 1893.
[58] Kassem (n 11) p. 16-17.
[59] ibid.
[60] Harter Act 1893, Section 191.
[61] ibid.
[62] ibid.
[63] Kassem (n 11) p. 17.
[64] ibid.

The approach to the shipowner's duty exercise due diligence to make the vessel seaworthy that the Harter Act introduced was so successful that it was later elaborated on and adopted in the Hague Rules in 1921 and its Visby Amendments in 1968.[65] The Hague Visby Rules took a step forward and provided a detailed article about what factors constitute seaworthiness. Art. III(1)(a) of the Hague Visby Rules states that the carrier shall before and at the beginning of the voyage exercise due diligence to make the ship seaworthy. As it was explained above, to exercise due diligence means that the carrier is "taking all reasonable precautions to see that the vessel is fit for the voyage contemplated."[66] In addition, the carrier is bound to properly man, equip and supply the vessel, in addition to making the vessel cargo worthy.[67] Hence, it follows that the Hague-Visby Rules have replaced the absolute obligation to provide a seaworthy vessel with the duty to exercise due diligence to make the ship seaworthy.[68] Due to its wording, many scholars criticized the Hague-Visby Rules as the decision to specify what constitutes a seaworthy vessel might be considered as limiting to the ability of the courts to expand on the meaning of seaworthiness following the future developments of the shipping industry.[69]Nevertheless, the Hamburg Rules went beyond the scope of the Hague-Visby Rules and further increased the carrier's liability.[70] The Rules adopted the same approach but did not use the term "due diligence" but instead used the term "all reasonable measures."[71] Article 5,[72] referring to seaworthiness, combines the duty to provide a seaworthy vessel with negligence. Making the shipper responsible unless he can prove that there was no fault or neglect on his part or part of his servants or agents in taking all measures that could reasonably be required.[73] Thus, the Regulation is based on the "principle of presumed fault or neglect."[74] Similarly to the HVR the Hamburg Rules also provide for an exception from liability.[75] Furthermore, by not including specific elements of seaworthiness, the drafters left it open for the courts to define and elaborate on the concept of seaworthiness. The Rotterdam Rules, in effect, proceed to

---

[65] ibid.
[66] The Shipowner's Club, 'Continuing Warranty of Seaworthiness' (*shiponwersclub*, 9 October 2018) <https://www.shipownersclub.com/continuing-warranty-of-seaworthiness/> accessed 19 November 2021.
[67] Kassem (n 11) p. 52.
[68] ibid p. 17.
[69] ibid.
[70] ibid p. 18.
[71] ibid.
[72] Hamburg Rules, Art. 5.
[73] ibid.
[74] Kassem (n 11) p. 154.
[75] The exemptions from liability can be found in Art. 5(5)(6)(7) of Hamburg Rules.

encompass roughly the same principle concerning the concept of seaworthiness as laid down in the Hague-Visby or Hamburg Rules. However, on the other hand, contrary to the HVR and the HR, the Rotterdam Rules expand on the period of time when the carrier is bound to exercise due diligence to make the ship seaworthy.[76] According to Article 14 of the Rotterdam Rules, the shipowner is bound before, at the beginning of, and *during* the voyage by sea to exercise due diligence. Hence, it turns out to be a continuous obligation that persists throughout the journey. Besides, is this duty confirmed in Article 14(a), where the Rotterdam Rules set forth the requirement to "make and keep the ship seaworthy" as opposed to "make the ship seaworthy" as stated in Article III(1)(a) of the Hague-Visby Rules.

2.3.2. Definition of seaworthiness under Marine Insurance Law

Under Marine Insurance Law, the shipowner must provide a vessel capable of performing its expected voyage. Failure to do so will otherwise have a serious implication on his right to claim compensation for the loss suffered.[77] Section 39(4) of the Marine Insurance Act 1906 states, 'A ship is deemed to be seaworthy when she is reasonably fit in all respects to encounter the ordinary perils of the seas of the adventure insured." In this respect, the drafters did not identify what constitutes seaworthiness.[78] Instead, they emphasized that at the commencement of the voyage, the vessel should be reasonably fit in all respect to encounter the ordinary perils of the seas. In addition, the words used in the Act to describe seaworthiness are stated in general, allowing the courts to identify what a seaworthy vessel means according to the facts and circumstances surrounding each case.[79] The concept of seaworthiness as it is laid down in the MIA is derived from the *Dixon v. Sadler* case,[80] in which the court specified that for the vessel to become seaworthy, she "shall be in a fit state as to repairs equipment, and crew and in all respects, to encounter the ordinary perils of the voyage insured, at the time of sailing."[81] Hence, the Marine Insurance Act definition of the duty to provide a seaworthy vessel is contingent on the capability of the ship to encounter the ordinary perils of the sea.[82] On the contrary, in terms

[76] Rotterdam Rules, Art. 14.
[77] Kassem (n 11) p. 19.
[78] ibid p. 20.
[79] ibid.
[80] *Dixon v. Sadler,* 5 M. & W. 405.
[81] ibid.
[82] In *Hedley v. The Pinkney and Sons Steamship Company, Limited* [1892] 1 Q.B. 58, at p. 64; the court ruled that "[…] there is an implied warranty that the vessel shall be seaworthy, by

of Carriage of Goods by Sea, the definition of seaworthiness is subject to the prudent carrier test. Such might indicate that seaworthiness does not mean the same under different divisions of maritime law. However, that is not the case. The negligible differences between the two definitions do not affect the concept of seaworthiness itself, but they only appear where there is a breach of duty. Besides, the meaning of the term seaworthiness is identical under both Marine Insurance and Carriage of Goods contracts. Such was the situation in *Hedley v. Pinkney* (1903), where Lord Esher stated that seaworthiness should mean the same in both insurance and carriage contracts and any other branch of maritime law.[83] Ultimately, seaworthiness can be defined as the overall fitness of the vessel in all respects, to encounter the ordinary perils of the sea that could be expected on her voyage and deliver the cargo safely to its destination.

2.4. Vessel seaworthiness and Cargo-worthiness

As illustrated above, the term of seaworthiness is quite comprehensive and encompasses not only worthiness regarding the physical state of the ship (vessel-worthiness) but also the vessel's fitness to encounter the voyage (voyage-worthiness) and its ability to deliver the cargo safely to its final destination (cargo-worthiness).[84] Consequently, the concept of seaworthiness is composed of several aspects, which are often divided into two elements: 1) seaworthiness of the vessel itself and 2) cargo-worthiness. The first element of seaworthiness pertains to the seaworthiness of the vessel itself. This aspect relates to the vessels' overall condition and readiness to undertake the voyage. It also includes the crews' training and competence to operate the ship and the minimum number of crew members that must be always present on board. Furthermore, the concept seaworthiness also covers the documents and certificates required onboard by national and international authorities to operate legally, trade openly, and move freely. Therefore, all these requirements must be satisfied for the ship to operate safely and be considered seaworthy. The second aspect of seaworthiness concerns the vessels' ability to carry and deliver the agreed cargo. This requirement does not only cover the ability to transport the freight in general. But also, any special arrangements that need to be in place for the safe

---

which it is meant that she shall be in a fit state as to repairs, equipment, and crew, and in all other respects, to encounter the ordinary perils of the voyage insured, at the time of sailing upon it."

[83] ibid.

[84] Kassem (n 11) p. 24.

carriage of the agreed cargo.[85] Hence, it follows that a vessel may be seaworthy to withstand the ordinary perils of the sea; however, it might not be cargo-worthy to carry the agreed cargo and vice-versa.[86] The following section will provide a closer look at these two aspects of seaworthiness. It will first examine the vessel's seaworthiness regarding physical, human, and documentary components. And secondly, it will analyze when the ship is considered cargo worthy. An examination of all elements of seaworthiness is necessary for the analysis of cyber-worthiness, which forms the core of the third chapter.

2.4.1. Vessel Seaworthiness

The physical fitness of the vessel does not limit the concept of the vessel's seaworthiness. Meaning, it does not only confine to the actual body of the ship (being the hull, hold, compartments, or the equipment), but it further extends to cover the equipment, master & crew, and proper documentation.

2.4.1.1. Physical Seaworthiness

The element of physical seaworthiness covers the assumption that the vessel itself is seaworthy. It attends to the physical state of the ship herself, i.e., its readiness to encounter the ordinary perils of the seas that she might encounter during her voyage.[87] Additionally, it considers the type of vessel, the age, the type of navigational water, the intended route, the time of the year, the available knowledge at the time of the voyage, and the nature of the cargo.[88] Underlines the carrier duty to ensure that the vessel is fit for the planned journey, or where he is under the obligation to exercise due diligence, and the ship is not seaworthy, he must prove that he indeed exercised due diligence to make it so. Only that will protect him from incurring liability for any loss or damage sustained. Hence, it follows that the structural condition of the hull must be perfect, and the functionality of the machinery must be in order, i.e., vessels' engines, holds,

[85] Examples include providing the ship with a proper functioning refrigeration system; to supply the vessel with specialized drying units that constantly monitor the air to prevent corrosion and damage that may occur; or when transporting livestock, to provide mechanisms that ensure proper ventilation, clean living holds and nutrition. Hence, if the carrier agrees to transport cargo with special requirements, he must ensure that his vessel can carry the freight and deliver it safely.
[86] Kassem (n 11) p. 25.
[87] ibid.
[88] ibid.

pipes, bunkers, tackles, and other machinery are in perfect condition without the need for additional repairs or maintenance.[89] Consequently, the ship must be "sufficiently tight, staunch, and strong to resist the ordinary attacks of winds and seas."[90] Eventually, there cannot be any damage to the vessel or the equipment before she commences her voyage. To a large extend, physical seaworthiness depends on the circumstance surrounding each individual journey. For these reasons, seaworthiness depends on several different factors. For instance, it takes into consideration the time of the voyage; the route the ship is going to sail; the kind of water she is going to navigate through (e.g., ocean, sea, river, lake, canal); the type of vessel (container vessel, bulk carrier, tanker ship, etc.); the available knowledge at the time of voyage; or the type of cargo she is going to carry.[91] Hence, this means that even if the vessel is seaworthy to perform a particular trip, she might not be if she were to execute the same voyage but in a different season or transport another type of cargo.[92] Similarly, the vessel might be seaworthy to sail in the ocean but may not have the ability to navigate through a lake or a river.[93]

2.4.1.2. Human Seaworthiness

The human factor forms another essential element of seaworthiness. It is a well-known fact that most marine accidents are a result of human error. Whether it's due to fatigue, inattention, over-dependence on technology, or a failure of organization and behavior, human error continues to be an essential safety issue. Even though the ship might be physically fit for the voyage, she might not be, in relation to its masters' or crews' proficiency or competency.[94] Inadequacy in crews training, certification, or professional behavior can increase the likelihood of the vessels' involvement in an accident, leading to further damage or loss of the cargo, property, or in the worse scenario, result in casualties on human lives. Therefore, each vessel must have a crew that has proper qualifications, certification, and professional behavior. The same applies to the master.

---

[89] Guenter H. Treitel and Francis M.B. Reynolds, 'Chapter 9: Section 1. (b)(i) – Seaworthiness' in *Carver on Bills of Lading* (4th edn, Sweet & Maxwell Ltd 2017).
[90] *Minister of Materials v. World Steamship Company Ltd.,* [1952] 1 Lloyd's Rep. 485.
[91] Kassem (n 11) p. 25-26.
[92] ibid.
[93] ibid.
[94] ibid p. 36.

2.4.1.3. Documentary Seaworthiness

At last, even though the carrier has provided an overall physically seaworthy vessel with a competent, well-trained, and adequately staffed crew, the ship still might be considered unseaworthy. The thing is that certain documents must be always present on board of vessel to ensure its safe sailing and compliance with both international and national rules and regulations.[95] Corresponding documentation is necessary to authorize the ship to enter or leave ports, load and unload cargo, or sail to its destination. There are three categories of documents that are mandatory onboard the ship. In particular, these include navigation documents, ship plans, and "any other documents which are important for the vessel to be able to load, unload or sail to its destination."[96] Navigation documents are necessary for safe sailing. They must be up to date[97], and should, among others, include appropriate charts[98] or maps with alternative routes in case of emergency. Furthermore, it is necessary to always have the plans of the ship available at hand.[99] These are important for the crew to know how parts of the vessel work and where to find them. Such can be helpful when the staff lacks knowledge and thus can refer to the ship's manuals to minimize any potential loss or damage to cargo or the boat itself and ensure that the vessel operates correctly. Finally, are other documents that are important for the vessel's performance. These include records that are not per se related to the safety of the ship but that are nonetheless mandated by the flag state, port authorities, or the international Shipping Industry.[100] In the case where the master is not able to present such certificates, the vessel might not be allowed to enter or leave the port and/or load or unload cargo. Failure to provide such documents, hence, might render the vessel unseaworthy.[101]

---

[95] ibid p. 45.
[96] ibid p. 45-46.
[97] In *Grand Champion Tankers Ltd. v. Norpipe A/S (The Marion)*, the court held that the vessel was unseaworthy due to lack of up-to-date charts.
[98] In *The Marion* case the court affirmed that "there had been failure by a director of the ship's management company to ensure that proper charts were kept […]."
[99] *Robin Hood Flour Mills, Ltd. v. N. M. Paterson & Sons, Ltd, (The Farrandoc*), [1967] 2 Lloyd's Rep. 276.
[100] Kassem (n 11) p. 48-49.
[101] These documents can include fumigation certificates, health authority certificates, or deratization certificates.

2.4.2. Cargo Worthiness

"The phrase unseaworthiness should be given its ordinary and wide meaning, embracing cargoworthiness."[102] Thus, as mentioned above, two elements form the carriers' duty to provide a seaworthy vessel. The first relates to the vessel's physical seaworthiness, its crew, and documentation. The second element addresses the ability of the ship to receive, carry and deliver cargo to its final destination safely. In principle, this applies to passengers as well.[103] The carrier shall not only guarantee that the vessel is physically seaworthy before and at the beginning of the voyage but also that she is able to receive and carry the agreed cargo. Therefore, the carrier shall not only provide a seaworthy vessel in the context of men, equipment, and documents, but he must also supply a cargo-worthy vessel.

Cargo-worthiness deals with the condition of the ship itself to carry the cargo. For the carrier to be discharged from his obligation to provide a seaworthy vessel, he is obliged to provide a vessel that is fit to carry the contracted cargo.[104] This in general includes for example, the obligation to prepare the cargo holds to receive the cargo.[105] Furthermore, the owner must make sure that the vessel is equipped with proper pumps to drain surplus water to avoid damage of the cargo.[106] Overall, the owner must make sure that all the measures are taken in order not to endanger cargo.[107] Similarly, the carrier has a duty to provide his vessel with special equipment if the contracted cargo needs such arrangements. Failure to do so might be considered as failing to provide a seaworthy vessel. Such might include for example to equip the vessel with proper refrigeration systems,[108] or proper ventilation systems[109] as failure to do so might render the

---

[102] *Ben Line Steamers Ltd. v. Pacific Steam Navigation Co* ('The Benlawers'), [1989] 2 Lloyd's Rep. 51.
[103] Stevens F., 'Seaworthiness and good seamanship in the age of autonomous vessels' in *Henrik Ringbom, Erik Røsæg* and Trond Solvang (eds), *Autonomous Ships and the Law* (1st edn, Routledge 2020).
[104] Kassem (n 11) p. 52.
[105] Such might include prior disinfection, deratization, fumigation or cleaning of hatches, cargo holds or other places.
[106] *Burges v. Wickham* (1863) 3 B & S 669 at 693.
[107] This can include closing air strikes to prevent the water from pouring inside the vessel during storm. As held in *The Oakley C. Curtis*, 4 F.2d 979 (2d Cir. 1924).
[108] Under the decision in *Martin v. Southwark*, 191 U.S. 1, 24 S. Ct. 1, 48 L. Ed. 65 (1903), the owner has a duty to furnish a vessel with a refrigerating apparatus in good order and repair, competent for the safe transportation of cargo.
[109] *M.D.C. Ltd. v. N.V. Zeevart Maatschappij Beursstraat*, [1962] 1 Lloyd's Rep. 180.

vessel unseaworthy. In general, the owner should follow any special practice to protect the cargo. Furthermore, besides making the vessel fit to carry the contracted cargo, the owner must ensure that the cargo is properly stowed. "A bad stowage may be the cause of instability of the ship or damage to the cargo wrongly stowed or to other cargo."[110] It might hence affect the safety of the vessel itself or affect the safety of the cargo without endangering the safety of the vessel.

2.5. Conclusion

Unseaworthiness - from a practical point of view - arises as a result of a lack or deficiency, which creates a risk that then threatens the safety of the ship or cargo.[111] As demonstrated above, for the vessel not to be seaworthy, what is missing is important. However, what is increasingly important, is that as long as it is missing and as a consequence of its absence - the vessel or cargo is in danger.[112] Hence, for now, if such is correct. One may safely propose a concept stating that lack or inadequacy, or inefficiency of necessary protective measures against cyberattacks amounts to unseaworthiness.[113] Such is since it can amount to a factor affecting the safety of the ship and its cargo.[114] Hence, while looking at cyber-risk-related issues, one might suggest that a failure of the owner to adopt necessary protective measures can amount to a failure to make the vessel seaworthy. Such, of course, relates to taking appropriate protective measures in relation to all elements of seaworthiness, starting with the ship itself, its equipment, crew, and documents. Since the issue of cyberworthiness has just been outlined and its deeper analysis is the main topic of the third chapter. The following chapter will provide a closer look at the concept of cyber security in the maritime sector. Moreover, the chapter examines how the shipping sector implements rules on cyber security. What are the rules and, how are they incorporated.

[110] *The Sagamore*, (1924), 300 Fed. 701, 1924 A.M.C. 961 (2nd Cir. 1924).
[111] Sőzer (n 4).
[112] ibid.
[113] ibid.
[114] ibid.

3. Chapter II: The concept of cyber security in maritime sector:

The reaction of international community to cyber threats

3.1. What cyber security threats are endangering maritime sector?

During the long history of maritime operations, the shipping sector has faced various physical threats. Traditionally, the main focus of these dangers were the vessels themselves. The attacks ranged from terrorism to piracy, from illicit trafficking of goods and people to drug smuggling or cargo theft, arm robbery, and damage or destruction of cargo or the ship itself, causing environmental pollution.[115] Still, all these attacks were of physical nature. And often, these advancements were successful, as it is difficult to call and receive help quickly while traveling across high seas.[116] While these threats are still present and ongoing, they are more or less well understood, and the international community has years of experience in mitigating and combating such crimes.[117] However, with the increased use of digitalization and technology and its heavy dependence on it in the maritime sector, it all changes. And the shipping industry comes face to face with a new invisible threat. The threat against which no industry is immune, a so-called 'cyber security threat.' Until relatively recently, cyber security has not been a real issue for ships, ports, and the maritime sector in general.[118] Since the vessels were relatively self-sufficient and not connected to the outside world, there was no risk of cyber-related threats. However, with the advancements in technology, ships, and their systems are gradually linking to the world wide web, which means that vessels are now more vulnerable to cyber-related threats than before.

A cybersecurity threat or a cyber-attack can, in general, can be defined as a malicious act mounted against another entity by means of cyberspace that seeks to damage and steal data or

---

[115] Kimberly Tam, Kevin Jones, Maria Papadaki, 'Threats and Impacts in Maritime Cyber Security' (Engineering & Technology Reference, January 2016) <https://www.researchgate.net/publication/304263412_Threats_and_Impacts_in_Maritime_Cyber_Security> accessed 19 November 2021.

[116] ibid.

[117] ibid.

[118] Loomis W, Singh V.V, Kessler G.C, Bellekens X, 'RAISING THE COLORS: Signaling for Cooperating on Maritime Cybersecurity' (Atlantic Council, Scowcroft Center for Strategy and Security, October 2021).

disrupt digital life.[119] Hence, one could argue that the threats moved from physical space to cyberspace. Thus, nowadays, cyber-attacks include threats like computer viruses, malware, ransomware, data breaches, and much more. The potential dangers that cyber-attacks can bring are endless. Contrary to traditional crimes, cyber-attacks are often hidden and hard to be discovered. Their goal is to exploit or control the compromised system or gain confidential information for as long as possible.[120] Hence, it is essential to be aware of such potential threats, know how to protect yourself, and be ready to face them.

There is no denying that the maritime industry is vulnerable to cyber-attacks. Indeed, all maritime stakeholders (including shipowners, cargo-owners, carriers, port operators, and many more) are potential targets of these invisible threats. Hence, they cannot disregard them or avoid them. On the contrary, they must be prepared to face them. Indeed, to prevent attacks and to protect his property, it is the shipowner's responsibility to ensure that his ships are cyber-resilient against cyberattacks. Such follows from the IMO Resolution MSC 428(98) according to which, shipowners and ship operators are required to take into account cyber risk management. Hence, they should be able to identify cyber-related-risks and avoid, transfer, or mitigate their effect. However, it is only recently that the international shipping community has begun to pay closer attention to cyber security and preventive measures against cyber threats. Therefore, this chapter aims to introduce the current international framework addressing cyber-related threats. In addition, the focus is on how the current Rules and Regulations are implemented and whether they are efficient enough and hence can protect the maritime sector and the entities involved in it from unwanted cyber-attacks.

3.2. Maritime cyber risk

Since cyber-attacks are a real threat that endangers the maritime industry, the International Maritime Organization has developed a definition of what a cyber risk in the shipping sector entails. Hence a maritime cyber risk is a measure of the extent to which a potential technology asset could be threatened or interfered with by a probable circumstance or event, which may

[119] Hugh Taylor, 'What Are Cyber Threats and What to Do About Them' (THE MISSING REPORT, 16 June 2021) <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/> accessed 19 November 2021.
[120] Tam, Jones, Papadaki (n.115).

result in shipping-related operational, safety, or security systems failures as a consequence of which information or systems are being corrupted, lost or compromised.[121]

3.2.1. Difference between OT & IT systems

To better understand the dangers cyberattacks pose to ships and maritime operations. The following section will describe the difference between the OT and IT systems of the vessel as these are often the usual targets of cyber-criminals. Hence their maintenance should form the main focus of the owner. In general, vessels should be resilient to attacks that target their IT systems, along with attacks targeting their OT systems.[122] From a cyber security perspective, OT and IT are different in several ways.[123] While the IT systems manage data and support various business functions,[124] the OT systems are the hardware and software that directly control physical devices onboard ships and monitor many processes aboard the vessel.[125] The IT and OT systems are an integral part of the ship and must function independently.[126] However, with the increase of dependency on technology and digitalization, these two systems are becoming integrated.[127] The primary purpose behind their interconnection is for the IT systems is to process information, monitor the performance of OT systems, or remotely support the OT network.[128] In a scenario where the two systems are connected, the owner must ensure that the interface connecting the two systems is sufficiently secure by a firewall, and potential vulnerabilities in the OT systems are well hidden in the IT network.[129] This protection is vital, as disruption of the operation of OT systems may impose a significant risk to the safety of onboard personnel, cargo, damage to the marine environment, or significantly impede ships'

---

[121] International Maritime Organization, 'Maritime cyber risk' (*imo*, 2019) <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> accessed 19 November 2021.
[122] BIMCO, The Guidelines on Cyber Security Onboard Ships (Version 4), Section 1.4. <https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf> accessed 19 November 2021.
[123] ibid.
[124] International Maritime Organization, Guidelines on maritime cyber risk management, 5 July 2017 (MSC-FAL1./Circ.3), Art. 2.1.2 "IT systems may be thought of as focusing on the use of data as information."
[125] ibid., Art. 2.1.2 "OT systems may be thought of as focusing on the use of data to control or monitor physical processes."
[126] BIMCO, Guidelines, Section 1.4.
[127] ibid.
[128] ibid.
[129] ibid.

service.[130] Vulnerabilities can arise from inadequacies in the design, integration, or maintenance of systems or a lack of cyber hygiene.[131] Hence, an effective cyber risk management should consider safety and security impact of all vulnerabilities resulting from the exposure or exploitation of IT and its subsequent effect on OT systems.[132]

3.3. Types of Cyber Attacks

Cyberattacks pose a significant threat to many industries, and the maritime sector is no exception. Current implications of cyberattacks on the maritime industry include financial loss, damage to reputation, business disruption, damage to goods or the environment, human injury or loss of life, incident response cost, salvage cost, and fines or legal costs.[133] To achieve a better understanding of the following chapters. The present section describes the types of attacks cybercriminals are capable of and their consequences. The following sub-section will describe various types of cyberattacks as presented in The Guidelines on Cyber Security Onboard Ships. Furthermore, it provides a couple of examples of cyber-attacks that already took place in the maritime sector. The reason behind this analysis is to affirm the importance of cyber-threats awareness and of proper cyber risk management.

The Guidelines on Cyber Security Onboard of Ships identify two categories of cyber threats that may affect companies engaged in maritime operations, ships, and ports:

1. Untargeted attacks,[134]
2. Targeted attacks.[135]

As the name implies, untargeted attacks do not target a specific company, vessel, or port. The attacker often uses tools and techniques that are freely available and accessible on the Internet.[136] He can then use them to locate, discover and exploit vulnerabilities that may exist

[130] ibid.
[131] IMO, Guidelines on maritime cyber risk management, Art. 2.1.5.
[132] ibid, Art. 2.1.8.
[133] Andrej Androjna, Tanja Brcko, Ivica Pavic, Harm Greidanus, 'Assessing Cyber Challenges of Maritime Navigation' [2020] 8(10) Journal of Marine Science and Engineering 1.
[134] BIMCO Guidelines, Untargeted attack refers to attacks where different vessel systems or company data are one of many potential targets of the attackers.
[135] BIMCO Guidelines, Targeted attack refers to attacks where ship's systems or confidential company data and information are the direct targets or one of the multiple integral targets.
[136] BIMCO Guidelines, 2.2.

in a company.[137] Untargeted attacks are more common, as they are simpler to execute, easily accessible, and the attacker does not need to have specific knowledge.[138] Examples of tools and techniques that perpetrators may use include malware, water-holding, scanning, or typosquatting.[139] Targeted attacks, on the other hand, are a more sophisticated and complex form of cyber-attacks.[140] Often, they use tools and techniques that are created especially for targeting a specific company, vessel, or port.[141] Examples of devices or methods that attackers may use to take advantage of their victims include, for example, social engineering, brute force, credential stuffing, denial of service, phishing, spear-phishing, or subverting the supply chain.[142] The list of examples provided above is not exhaustive. There are many other methods and tricks, which perpetrators may use to deceive and exploit the shipping companies, vessels, or ports. Consequently, with the increase of digitalization and knowledge that attackers have, the potential number and sophistication of mechanisms and techniques used in cyberattacks by cybercriminals will continue to rise.

3.3.1. Possible Cyber-Attacks on Vessels

Cybercriminal attacks can affect companies, ports, and the vessels themselves. Therefore, business owners need to know how to protect their business from easily avoidable cyber-attacks. They should as well understand the importance of cyber risk management. And be ready to manage different forms of cyber threats. However, the burden does not rest on the owner's shoulders alone. Other directly involved parties should also understand the risks of cyber threats and the importance of their mitigation. Hence, for example, the personnel working onboard the vessel, such as the master and crew, should also be educated and have at least a minimal understanding of cyber security to be able to make a correct decision when a critical situation arises. As mentioned above, with the increase of digitalization and use of technology in maritime sector, and mainly with the increased reliance on technology onboard vessels, it is now much easier for cyber criminals to attack ships IT and OT systems. Once the attacker gets

---

[137] ibid.
[138] Kayla Elliott, 'Targeted Attacks or Untargeted Attacks – Which is Most Common' (*TechTalk*, 13 September 2018) <https://techtalk.pcmatic.com/2018/09/13/untargeted-targeted-attacks-untargeted/> accessed 19 November 2021.
[139] ibid.
[140] ibid.
[141] ibid.
[142] ibid.

an access to vessels IT systems it is very easy for him to control the OT systems such as the navigation systems, power control systems, access control systems, passenger servicing and management systems, administrative and crew welfare systems and much more.[143] Presumably, one of most likely and threatening attacks on vessels is to disrupt their navigation systems. The attacked can hack to vessels Global Positioning Sytem (GPS) or Automatic Identification System (AIS)[144] systems and manipulate the Electronic Chart Display and Information System (ECDIS) data.[145] In general, AIS is considered to be one of most vulnerable systems on the ships.[146] The AIS modification of all ships data is in particular dangerous and can have terrible consequences. The attacker has plenty of options on how to compromise or tamper with data. The perpetrator can for example modify data regarding vessels position, course, cargo, speed, name.[147] He can impersonate port authorities, communicate with other ships, or shut down ship to ship, or port to ship communications.[148] Furthermore, once the vessels systems are accessed the attacker can easily modify the systems and send fake weather forecast information or create so called "ghost" vessels at any location in the ocean.[149] The creation of 'ghost' vessels could trigger the AIS receivers and mistake the signal as a genuine vessel, causing a false collision warning alert, resulting in a course adjustment.[150] This then could result in a terrible consequence where the vessel could be subject to more traditional threats or used as a weapon to crash into ships, ports, oil rings or other vulnerable targets.[151] Another type of a potential attack is for the attacker to access the vessels IT system and encrypt it through use of ransomware.[152] Resulting in attacker gaining full control of the ship until ransom is paid.[153]

---

[143] Olivia Delagrance, Jose Pellicer, 'Assessing the cyber risks of maritime navigation' (*kennedyslaw*, December 2017) <https://kennedyslaw.com/media/3288/kennedys_assessingthecyberrisksofmaritimenavigation.pdf> accessed 19 November 2021.

[144] Mednikarov Boyan and others, 'Analysis of Cybersecurity Issues in the Maritime Industry' [2021] 47(1) Information & Security: An International Journal 27, 'Automatic Identification System enables ships to communicate with other ships, exchange positional data, and avoid collisions with other ships, reefs, floating objects, etc.', p. 32.

[145] ibid.

[146] ibid, p.32.

[147] ibid.

[148] ibid.

[149] ibid, p.34.

[150] ibid.

[151] ibid.

[152] Maurantonio Caprolu and others, 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead' [2020] 58(6) IEEE Communications Magazine 90 <10.1109/MCOM.001.1900632> accessed 19 November 2021.

[153] ibid.

Furthermore, humans are regarded as one of the prime weaknesses of any cybersecurity architecture. User errors can easily expose sensitive information or create access points for attackers.[154] Furthermore, people are now more dependent on technology and cannot keep their hands from their personal devices. It is more than likely that an attack on the vessel starts after a crew member downloads a corrupted file from the internet or plugs infected USB stick into onboard computers used for administrative management and hence provides the attacker access to vulnerable data. [155] In case of cruise ships or other vessels transporting passengers, the attacks are likely to occur because of passengers themselves. Passengers often have access to local internet networks that are available onboard vessels which create a potential risk to the ship's cybersecurity.[156] As it is case with the crew, the passengers can also download corrupted file or even explore the vessels vulnerabilities and attack the vessel on their own initiative. Besides the potential attacks on vessels navigation, communication, and passenger welfare systems. The attacker can also interfere with cargo and loading management systems. The crew uses different digital systems on the vessel during loading, management, and control of cargo. These systems may interface with various networks ashore, making them more accessible and vulnerable to cyber incidents. [157] For instance, the cybercriminal could connect to the vessels' cargo management system through the port's computer network and manipulate cargo documentation[158] or check the cargo information to see whether there is anything valuable to take. The Port of Antwerp cyber-attack is a beautiful example of how attackers can infiltrate systems and take full advantage of them. From 2011 until 2013, a drug cartel penetrated computer systems at the port and took control of containers systems.[159] Such action enabled them to locate specific containers, change the location and scheduled delivery time, and smuggle drugs without anyone noticing.[160] Another example of a successful cyber-attack is the attack on the A.P. Moller-Maersk in June 2017.[161] The company fell victim to a large cyber-

[154] Boyan and others (n. 144).
[155] ibid, p 32.
[156] ibid, p. 34-35.
[157] ibid.
[158] ibid, p.31.
[159] Lee and others (n.8).
[160] ibid.
[161] The Editorial Team, 'Maersk Line: Surviving from a cyber attack' (*SAFETY4SEA*, 31 May 2018) <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/> accessed 19 November 2021.

incident that affected its transport operations and logistic business, due to which the company suffered tremendous financial loss.[162]

The cyber-attack at Port of Antwerp of the A.P. Moller-Maersk attack are prime examples of the importance of a cyber risk management system. As the vessels' IT and OT systems are increasingly becoming connected to each other and to the internet, the possibilities of cyber-attacks are endless. The examples mentioned above are only a small number of all possible cyber-attacks that are likely to occur onboard vessels. Companies need to be cyber resilient and be able to respond and recover from cyber-attacks. They must be proactive in the sense that they should invest in the organization's protection and educate their employees about potential cyber threats. Hence, to raise the awareness of the potential dangers of cyber-attacks, the international community started to produce regulations and guidelines to educate and guide ship and business owners on how to exercise cyber risk management. However, are these rules, regulations, and strategies efficient and clear enough for the stakeholders to understand, do they provide an incentive for the shipowners to follow them, are they binding? That is the intention of the following section.

3.4. International framework addressing cyber security in maritime sector

The connectivity to and reliance on the internet now forms a fundamental part of many technologies essential to the operation and management of vessels, and their security and safety. As a result of many ocean-based activities are being conducted remotely, with network systems connecting ships, ports, and cargo. The maritime industry is now, like never before, exposed to hidden but increasingly urgent threats: cyber-attacks. The international maritime community is under pressure to deliver policy documents that can guide various maritime stakeholders on how to approach those threats. Yet, only recently has the international community started to recognize the need for cybersecurity oversight to ensure the effective management and mitigation of evolving cyber threats in the maritime sector.[163] Until the last couple of years, from the perspective of regulatory context for the shipping industry on global, regional, and

[162] ibid.
[163] The European Network and Information Security Agency (ENISA), 'Cyber Security Aspects in the Maritime Sector' (The European Union Agency for Cybersecurity, November 2011).

national levels, there was very little consideration given to cyber security elements.[164] Most security-related regulations only included provisions relating to safety and physical security concepts.[165] Such form part of the International Safety Management Code or the International Ship and Port Facility Security Code and other maritime security and safety regulations. These regulations, however, do not consider cyber-attacks as possible threats of unlawful acts.[166] Hence, it was up to the international community to produce new rules or amend the current ones to include these threats. Some of such documents, for example, include the IMO Resolution MSC 424(98) or the IMO Guidelines on Maritime Cyber Risk Management. The following section will provide a deeper look into these documents.

3.4.1. International Management Code for the Safe Operation of Ships and for Pollution Prevention - (International Safety Management (ISM) Code)

The ISM Code as it is known today was adopted in 1993 by resolution A.741(18).[167] It was made mandatory with the entry into force of the 1994 amendments to the SOLAS Convention (which introduced a new chapter IX into the Convention) on 1 July 1998.[168] The purpose of this Code is to provide an international standard for the safe management and operation of ships and pollution prevention.[169] The Code is based on general principles and objectives, as it recognizes that no two shipping companies or shipowners are the same and that ships operate under a wide range of different conditions.[170] The ISM Code recognizes that the cornerstone of good safety management is a commitment that starts at the senior level.[171] Hence, every company should develop, implement, and maintain a safety management system (SMS).[172] The goal of safety management, according to the Code, is to continuously improve the safety-management skills of personnel ashore and aboard ships.[173] Concepts such as safety at sea,

---

[164] ibid.
[165] ibid.
[166] ibid.
[167] International Maritime Organization, 'The International Safety Management (ISM) Code' (*IMO*, 2019) <https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx> accessed 19 November 2021.
[168] ibid.
[169] ISM Code, Preamble (1).
[170] ISM Code, Preamble (4).
[171] ISM Code, Preamble (6).
[172] ISM Code, Article 1.4.
[173] ISM Code, Article 1.2.2.3

prevention of human injury or loss of life, and prevention of damage to the environment form the primary objectives of the ISM Code.[174] Nevertheless, none of the security regulations included in the ISM Code include provisions related to cyber-attacks. The Code only contains provisions that relate to safety and physical security. Thus, does not consider cyber-attacks as a possible threat. That is not enough for the shipowners to know what measures they can take to protect their assets and how to fight against cyber-attacks. However, to compensate for the lack of such provisions in the ISM Code, the International Maritime Organization developed Resolution MSC.428(98). Such requires shipowners and managers to assess cyber risk and implement relevant measures across all functions of their safety management system. The IMO agreed that cyber risk management should be integrated into existing management systems under the ISM Code and ISPS Code.

3.4.2. IMO Resolution MSC 428(98)

Hence, concerning the current situation and the fact that technology has become essential to the operation and management of systems critical to the safety and security of shipping operation, the International Maritime Organization adopted Resolution MSC.428 (98) (hereinafter 'Resolution') to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping.[175] The Resolution requires all stakeholders involved in the maritime operations to expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities.[176] Hence it demands that shipping companies incorporate Maritime Cyber Risk Management into their existing safety management processes.[177] To encourage the shipping companies to comply with the requirements (of the Resolution), the IMO set a timeline for the flag states to ensure that companies addressed cyber risks appropriately.[178] Such shall be no later than the first annual verification of the company's Document of Compliance (DOC) after 1 January 2021.[179] Even though the Resolution only encourages that cyber risks are appropriately complied with, it makes cyber risk management onboard ships mandatory. Hence, creates an incentive for all the stakeholders involved in maritime operations to understand that

[174] ISM Code, Article 1.2.1
[175] IMO Resolution MSC 428(98) (n 2).
[176] ibid.
[177] ibid.
[178] IMO, 'Maritime cyber risk' (n. 121).
[179] ibid.

cyber risks pose a real threat to the shipping sector and must be addressed adequately. Furthermore, according to the Resolution, the effective cyber risk management should start at the senior management level.[180] Such should hence raise awareness of cyber risks and embed it as an organizational culture[181] at all levels of an organization.[182] Each stakeholder should be aware of their role and responsibilities in the cyber risk management system. Furthermore, they should be prepared to address any vulnerability and threat effectively and promptly. However, the Resolution only provides a recommendation for cyber risk management, it does not define appropriate measures that can be taken to achieve the protection against cyber threats. Hence, that's why the IMO produced Guidelines on Maritime Cyber Risk Management (MSC-FAL. 1/Circ.3), providing a high-level recommendation for maritime cyber risk management.[183]

3.4.3. IMO Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Cir.3)

These Guidelines are recommendatory in nature, hence non-binding. Nonetheless, they consider risk management as fundamental to the safe and secure business operations of every company.[184] With the greater dependence on digitalization, industrialization, automation, and network-based systems within the shipping industry, the maritime sector has created an increasing need for cyber risk management. Consequently, these Guidelines present five functional elements supporting effective cyber risk management:

1. identify the risk;[185]
2. protect business assets;[186]
3. detect the threat;[187]
4. respond to the risk;[188] and,

[180] IMO Resolution MSC 428(98), Article 3.3.
[181] Captain Akshat Arora, Eleni Antoniadou, 'Maritime Cyber Risk Management Guidelines' (*Standard Club*, October 2020) <https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/loss-prevention-industry-expertise-handouts/3365323-sc_ie_cyber_risks_20201117_final.pdf> accessed 19 November 2021.
[182] IMO Resolution MSC 428(98), Article 3.7.
[183] IMO, Guidelines on maritime cyber risk management, Art. 1.1.
[184] ibid Art. 1.4.
[185] ibid Art. 3.5(1).
[186] ibid Art. 3.5(2).
[187] ibid Art. 3.5(3).
[188] ibid Art. 3.5(4).

5. recover from the attack.[189]

The Guidelines are drafted in broad terms. Nonetheless, for companies, it is *recommended* to implement risk control processes and measures to protect their business from cyber risks and ensure the safe operation of their ships.[190] In addition, all organizations in the shipping industry are encouraged to undergo a cyber risk analysis to assess their vulnerabilities and potential threats endangering their operations.[191] Based on the results of the investigation, the companies should develop and implement activities and create an effective plan to provide resilience to their systems[192] and implement mitigation strategies to strengthen their assets.[193]

However, similarly like the Resolution, the IMO Guidelines do not prescribe how its high-level recommendations for maritime cyber risk management shall be implemented, it only talks about the importance of cyber risk management. Therefore, it recommends additional guidance and standards for the implementation of cyber risk management and refers to:

1. *Guidelines on Cyber Security Onboard Ships* (produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, and UIMI); and,
2. *ISO/IEC 27001 standard on information technology*.

So, we can summarize that IMO produced two different documents affirming the importance of maritime cyber risk management (of which only one is binding), but none of them actually prescribe how to implement these recommendations for cyber risk management. And thus, it relies on and recommends additional guidance and standards for its implementation.

3.4.4. Guidelines on Cyber Security on Board of Ships

To further elaborate on the notion of maritime cyber risk management, it is essential to look at the "Guidelines on Cyber Security on Board of Ships" (addressing the cyber-security-related issues onboard vessels) produced by the leaders of the shipping industry BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF, and UIMI. Even though the Guidelines are not mandatory, they are essential as they were drafted by the industry representatives and provide

[189] ibid Art. 3.5(5).
[190] ibid Art. 1.1.
[191] Aurora, Antoniadou (n 181).
[192] ibid (n 124) Art. 3.4.
[193] Aurora, Antoniadou (n 181).

insight into how the industry intends to respond to cyber risks.[194] The Guidelines are very comprehensive and explain why and how to manage different forms of cyber risks.[195] They provide a complete outline of the risk assessment process.[196] The document closely defines threat actors,[197] types of cyber threats,[198] or common cyber vulnerabilities.[199] It highlights the importance of evaluating the likelihood of the risk and its impact on the business when conducting cyber risk management.[200] Information provided in the Guidelines is vital for shipping companies and other entities involved with maritime shipping operations, as they can learn how to conduct a proper risk assessment to protect their business from cyber-attacks. Nevertheless, as mentioned above, the Guidelines provided by the leaders in the industry are not-binding. They are merely a recommendation and an actual guideline of how to conduct proper cyber risk management.

3.5. Conclusion

As mentioned above, in response to all technological developments and changes in the shipping sector, the maritime industry produced a comprehensive solution for enhancing cyber security and safety for all vessels. In June 2017, the IMO adopted Resolution MSC.428(98) for Maritime Cyber Risk Management. This resolution aims to protect the ship from cyber-attacks by requiring shipowners to account for cyber risk management in their safety management system, which should all comply with the ISM Code.[201] The resolution is now officially valid and mandatory for all signatories. In addition, the IMO has published general guidelines to help shipowners identify and detect risks, protect their assets, and respond to attacks. The IMO's resolution is a positive step forward for the industry.[202] It ensures that the entire industry works together to minimize and overcome the effects of cyber-attacks.[203] However, despite the efforts

---

[194] ibid.
[195] BIMCO, Guidelines, (n 122).
[196] ibid.
[197] ibid Section 2.1.
[198] ibid Section 2.2.
[199] ibid Section 3.
[200] ibid Section 5.
[201] '**A SHIPOWNER'S GUIDE** TO ACHIEVING CYBER SECURITY' (*Bureau Veritas*, 2021) <https://marine-offshore.bureauveritas.com/ship-owners-guide-achieving-cyber-security> accessed 19 November 2021.
[202] ibid.
[203] ibid.

of the international community, defenses remain weak.[204] On the one hand, many companies are proactive in adopting maritime cyber risk management practices and strengthening their response to cyber-attacks. However, on the other many are not, where their vessel's cybersecurity defenses are practically nonexistent. Furthermore, even though these international regulations are in place, the key stakeholders of the maritime sector still lack the necessary incentives to improve their overall cyber security posture. Hence, as the IMO has no enforcement power, it is up to individual countries to propose rules that the shipowners must follow. Hence, the enforcement varies. Among flag administrators taking a particularly rigorous approach to cyber security, enforcement is the US Coast Guard or the French administration.[205] However, many other countries did not put much effort into enforcing cybersecurity rules. Hence, it all rests in the hands of individual jurisdictions to propose standards that shipowners must follow. And on the shipowners to implement these cyber risk management practices to avoid unnecessary threats. As long as the international rules are not binding, it will be difficult to get the stakeholders to do the risk assessment process and have proper cyber risk management in place. Thus, the international community can only continue to raise public awareness of various cyber threats and educate of their importance. Thus, the rules put forward by the international community are effective in raising awareness of various cyber-related threats and form a positive step forward in the development of the maritime industry. They ensure that the entire shipping sector works together to minimize and overcome cyber threats. They do not have any mandatory effect and do not propose an incentive encouraging the shipowners to abide by their rules.

[204] SHM (n 1).
[205] Bureau Veritas (n 201).

4. Chapter III: Cyber-worthiness

4.1. Does cyber security and maritime cyber risk management form part of seaworthiness?

As discussed in the previous chapter, the transition to digitalization and automatization of the shipping industry, developments in technology, and their increased use in the maritime sector bring many advantages for shipowners, business owners, and the shipping industry overall. With the increase in automatization of various processes, the evolution of autonomous vessels, and interconnection between vessel's IT and OT systems, the industry has opened to an entirely new category of risk.[206] The risk moved from physical threats such as piracy or drug trafficking to cyber related threats. While the threat of cyber-attacks has been present since the early 1970s when early computerized phone systems became a target of hackers, cyber security and cyber risk management are relatively new concepts that are slowly becoming major concerns for the shipping industry. In modern maritime history, cyber-security and cyber risk management have only begun to receive industry-wide attention over the past couple of years after several incidents that threatened safe handling in ports and disrupted the daily business operation of shipping companies. The infamous examples of shipping companies being targets of cyber-criminals include the multi-stage cyber-attack on Port of Antwerp or the NonPetya cyber-attack on A.P. Møller-Maersk. The two are excellent illustrations of what can happen when a company lacks a proper cyber risk management plan or when its employees are not adequately cyber-trained. With the growing development in technology is expected that such attacks are more likely to occur, and companies must, therefore, be ready to respond to these attacks and face their consequences. Nevertheless, the two examples presented above of Port of Antwerp and A.P. Møller-Maersk cover port security and cybersecurity at the company level. But what about the cyber security of vessels? As mentioned above, there are various hypothetical scenarios involving the invasion of a ship's cyber security. By way of illustration, the examples include a hacker tampering with a ship's ECDIS or AIS systems to accelerate piracy or other criminal objectives. A criminal making changes to ship's records to change the nature of shipped cargo from dangerous to non-dangerous, or electronically manipulating cargo handling system

[206] Karen Maxwell, 'Cyber-seaworthiness: the calm before the storm?' (*Twenty Essex*, 18 April 2018) <https://twentyessex.com/20-essex-street-bulletin-cyber-seaworthiness-the-calm-before-the-storm/> accessed 19 November 2021.

enabling his associates to steal high-value cargo. In each of these scenarios, there is a high likelihood of legal claims and counterclaims involving shipowners, charterers, cargo interests, insurers, and other parties involved in shipping operations increasing.[207] It is, therefore, necessary for the shipping industry that the shipowners are ready to deal with and respond to cyber-related issues by incorporating cybersecurity-related measures into their risk management processes. In the first chapter, we have learned what does the notion of seaworthiness entails. In the second chapter, among others, we have learned what cyber security is. How important cyber risk management is, and what are the current rules regulating this subject. Bearing all of this in mind, let's examine the issue of seaworthiness in the context of vessel's cyber preparedness to confront various cyber-attacks. Does, in fact, cyber security and cyber risk management fall under the notion of seaworthiness? Does non-implementation of maritime cyber risk management systems and protocols designated to avoid, transfer, and mitigate the risk of cyber-attacks renders the vessel unseaworthy? Should crewmembers have the training and proper education to identify and mitigate cyber risks? And if they do, should a non-compliance hence render the ship unseaworthy? What about the vessel's OT and IT systems? What if an update was not available before the voyage; thus, it was impossible to update these systems? Does it make the vessel physically unseaworthy? Finally, manage the rules put forward by the international community to raise awareness of cyber risk management, and do they play a role in whether the carrier has taken due care to make a vessel seaworthy? The following chapter will examine it all.

[207] Luke Parsons QC and Julian Clark, 'Can Cyber Risk Challenge Traditional Concepts such as Seaworthiness?' (*Quadrant Chambers*, 14 September 2017) <https://www.quadrantchambers.com/news/can-cyber-risk-challenge-traditional-concepts-such-seaworthiness-luke-parsons-qc-julian-clark> accessed 19 November 2021.

4.2. Seaworthiness in context of cyber security

Based on all available definitions, the term seaworthiness is possible to define as:

> "vessel's overall fitness in all respects to encounter the ordinary perils of the sea that she might expect on her voyage and hence to deliver the cargo safely to its ultimate destination."[208]

In this respect, it is worth reiterating the three central tenets of the traditional concept of vessels' seaworthiness:

1. Vessels' physical seaworthiness (including her state of her condition and the equipment),
2. Human element, and
3. Documentary worthiness.

Besides, it is significant to mention that the vessel must also be cargo worthy. So, the vessel is unseaworthy when there is a lack or deficiency of necessary protective measures, which creates a risk that threatens safety of the ship or cargo. For a deeper analysis of the notion of seaworthiness, see Chapter 1.

Hence, if we look at the matter in a narrower context, *the carrier must take all measures to protect the ship (together with her cargo) against the ordinary perils of the sea that she might encounter on her voyage*. Therefore, perhaps, the phrase "to take all measures necessary" (to protect the vessel) might be interpreted as taking all the necessary steps to protect the ship together with its cargo against potential cyber-attacks.[209] So, if this obligation to safeguard the vessel (thereby to have cyber risk management in place) falls within the scope of the responsibility of the carrier to make the ship seaworthy.[210] Then, if the owner fails to equip the vessel with adequate cyber-attack systems. As well as he does not educate and train the crew against cyber-risks. The ship would be unable to navigate at sea. Hence, it may mean that the owner failed to exercise due diligence to make the vessel seaworthy.[211]

It goes without saying, and we must keep in mind that all elements of seaworthiness need to be understood and examined in the context of the current state of knowledge in the maritime

---

[208] *McFadden v. Blue Star Line* [1905].
[209] Sőzer (n 4).
[210] bid.
[211] ibid.

sector.[212] So, since the shipping sector is developing very fast, and the international community keeps raising the awareness of dangers that cyber-related threats might bring. It will be increasingly difficult for the owner to argue a lack of knowledge about cyber-attack prevention or cyber-risk management.[213]

The following sub-sections will provide a deeper analysis of each element of seaworthiness separately and measure them against various cyber-related risks. The first sub-section will examine cyber-worthiness in the context of the vessel's hull and equipment. As there the integrity of the hull is unlikely to need special attention, the section will pay closer attention to the ship's equipment.[214] Besides the equipment, the sub-section will also explore the prudent owner standard. The second sub-section will explore the ship's cyber-worthiness in terms of proper training of the master and crew and their adequate cyber hygiene. In a situation of a cyber-attack, the response of the crew and the master to the attack will be of vital importance as they will be directly involved and present onboard the vessel when an attack occurs. Hence, they must be well educated to answer such threats. The third section will review proper documentation that with the increase occasions of cyber-attacks will likely need to be available onboard the vessel. The last part will examine if indeed cyber security falls to be included within the scope of the carrier to make the ship seaworthy, could the carrier then be exempt from liability under Art. IV of the HVR?

4.2.1. Hull and Equipment

As previously described, the term seaworthiness incorporates the physical state of the actual tangible body of the ship (its hull) and its equipment (such as GPS, AIS, steering mechanism, cargo-handling gear, communication systems, bridge systems, etc.). Therefore, both hull and equipment onboard the vessel must be working efficiently and be resilient against potential cybercrimes. As a part of vessels' cyberworthiness, hulls' integrity is unlikely to require special attention, as it would be rather difficult for criminals to attack the hull. There are, therefore, no special requirements that the shipowner must comply with. On the other hand, the same does not pertain to vessels' equipment. The owner should pay close attention and focus on the various

[212] Kassem (n 11) p. 33.
[213] Parsons and Clark (n 207).
[214] M. Bob Kao, 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' (2021) 45 Tul Mar LJ 467, p. 498.

equipment on board the ship and its workability. Under the notion of seaworthiness, to practice due diligence regarding equipment means that all equipment with its components must be in proper working condition.[215] The vessel must be "in a fit state as to repairs and equipment [...] to encounter the ordinary perils of the sea."[216] Said can be interpreted as all the equipment on board must be protected against the dangers of cyber-attack. Consequently, the owner must not only ensure that the equipment is in working order. But that it is well protected and secured against the risk of different types of cyber-attacks. Therefore, the owner must make sure that the ship's software, hardware, and other systems are up-to-date before starting the voyage, as they are more likely to become the target of an attack.[217] The consequence of not following such practice may result in vessels' unseaworthiness. However, what if software essential to cyber protection of the vessel is outdated and needs replacement?[218] The current market is full of different software and, there is no generally recognized standard to determine the most suitable one.[219] How does the carrier/shipowner know that he selected the correct one? And how can he be sure that he exercised due diligence and took measures to protect the ship?[220] In such situations it may be difficult for the court to determine whether the vessel was seaworthy or not. As long as the preferable standards are not determined by the international community. The shipowner can easily argue that the software he purchased is the most suitable, and hence he did indeed fulfill his obligation. Since techniques and methods that cybercriminals use change all the time, courts should not expect carriers to anticipate what new means of a cyber-attack might threaten their business. We cannot blame the shipowner because he did not conduct thorough research to find, purchase and install the most sophisticated software available on the market.[221] And even if he did find it, it might be too expensive for him to buy. Hence, the court should consider all facts before deciding in favor or against the shipowner. For now, such is very difficult to deliberate as yet there is not enough information and knowledge available in this field.

---

[215] *Martin v. Southwark* (n. 108).
[216] *Hedley v. The Pinkney* (n 82).
[217] BIMCO, Guidelines, Section 3.
[218] Sőzer (n 4).
[219] ibid.
[220] ibid.
[221] ibid.

4.2.1.1. "Before and at the beginning."

However, to follow up, we can focus on the time when the vessel must be seaworthy. Here we must pay closer attention to Common law and the Hague-Visby Rules which, state that: "The vessel must be deemed seaworthy before and at the beginning of the voyage."[222] So, could the fact that for example (before the start of the voyage) software has not been updated even though the update was available render the vessel unseaworthy? Of course, regarding a situation where it is later discovered that it was the absence of that particular update that made the vessel prone to cyber-attack. Could the court decide that the ship was not seaworthy due to the failure of the owner to ensure that the equipment was in proper working condition? Simply put, yes and no. The HV Rules clearly state that the vessel must be seaworthy before and at the beginning of the voyage. Hence, the obligation to exercise due diligence before the commencement of the journey is fulfilled if the carrier makes a reasonable determination regarding the plausible cyber-risk that his vessel could encounter during her trip and adopted all necessary measures to avoid it.[223] Thus, if the carrier at the commencement of the voyage believed that he did everything to make the vessel seaworthy and, as a result, made the reasonable decision that it was not necessary to update the software. He should then be deemed as having exercised his duty. It would be unreasonable to hold carrier liable for damage caused by a cyber-attack because it was later proved that it was necessary to update the software.[224]

4.2.1.2. "Ordinary careful and prudent owner" standard

According to Carver on Carriage of Goods by Sea: 'A vessel must have that degree of fitness which an *ordinary careful and prudent owner* would require his vessel to have at the commencement of her voyage, having regard to all the probable circumstances of it.'[225] Such implies that if the fault existed prior to the commencement of the voyage, would a prudent shipowner require to fix the damage before he sends the ship on its way had he has known of the defect.[226] Thus, the equipment must only be made secure to the extent that a prudent owner would do. However, how does the current prudent owner expect to behave concerning cyber

[222] HVR, Art. 3(1).
[223] Sőzer (n 4).
[224] ibid.
[225] Kassem (n 11) p. 14.
[226] Sőzer (n 4).

security and cyber risk management? In this respect, the technology used in the shipping industry is still new. Shipowners, masters, crew, and even judges lack experience in this regard. Therefore, for now, it might be difficult for the courts to assess what a prudent shipowner is expected to be, what he would do, or how he ought to behave.

4.2.1.3. Relevant practice and knowledge in the industry

"Standard of seaworthiness is not dependent on statutory enactment, but changes with advancing knowledge and experience."[227] The carrier is required to follow the developments that emerge in the shipping industry. However, precision is not required.[228] Therefore, for now, it might be easy for the shipowner to argue that he lacked the knowledge that permitted him to do nothing to address the potential cyber-attack. However, slowly when the technology becomes more familiar and more experience is gained, it will be increasingly more difficult for the shipowner to argue insufficient knowledge.

4.2.2. Master & crew

It is general knowledge that employees of an organization are often the weakest link in the protection of businesses' private information. The human factor hence plays a significant role in computer security. Among the most common causes of unintentional damage to the organization often belongs ignorance, lack of knowledge, or non-compliance with various regulations by employees.[229] In all industry sectors, the employees make mistakes that reveal company's' vulnerabilities and expose them to various cyber-risks. However, these errors are particularly serious in the maritime transport sector. Wherein non-compliance with regulations or employees' lack of knowledge can have terrible consequences not only on the business itself but can hugely disturb the life of the crewmen on board the vessel or affect the marine environment. Therefore, the master and the crew working onboard the vessel must receive appropriate training to deal with various incidents that may occur. On the same note, as mentioned in the previous chapter on seaworthiness, the human factor forms one of the essential elements of seaworthiness. Even though the vessels might be physically fit for the voyage, it

[227] *The T.J. Hooper,* 53 F.2d 107 (S.D.N.Y. 1931), aff'd, 60 F.2d 737 (2d Cir. 1932).
[228] Sőzer (n. 4).
[229] Efthymia Metalidou and others, 'The Human Factor of Information Security: Unintentional Damage Perspective' [2014] 147(1) Procedia - Social and Behavioral Sciences 424-428.

might not be, concerning the masters' or crews' proficiency or competency. Furthermore, if certain parts of the ship require special attention or operation, the shipowner must hire more qualified and skilled seafarers who have the necessary skills needed for that specific part of the equipment. Hence, with the increased digitalization, it is expected from the owner that the crew he hired is well-trained to respond effectively to cybercrimes.[230] Failure to do so may put the vessel into an unseaworthy position. The same criteria apply to the master, as seaworthiness requires the presence of a master of the competent skill. So, if an incident involving cybercrime occurs and the master does not have adequate training, the vessel may be rendered unseaworthy. Furthermore, there must be enough people on board to tackle the issue should cyber threats become a reality. To elaborate, if in any case, the owner can't have an adequate number of his crew cyber-trained.[231] It would be reasonable to appoint a designated cyber-officer on board the vessel.[232] This officer would have the essential cyber training. Moreover, he would be competent not only to recognize attacks but also to respond to them.[233]

4.2.2.1. Personnel physically working onboard vs. onshore staff

As far as we know, a ship is unseaworthy because of its crew if its members are incompetent or inefficient, and a prudent owner knowing this would not have allowed the vessel to venture on its voyage. Therefore, for the ship to be seaworthy, the crew must be trained specially to address incidents that might occur onboard the vessel. Thus, the owner must ensure that crew has proper knowledge and training. However, which personnel does the term 'crew' covers? In other words, does the expression covers personnel physically working on the ship, or does it also involve personnel working ashore? Generally, the onshore staff should have basic knowledge of vessels control systems and their characteristics and limitations.[234] They should also have a proper understanding of shipping and navigation in general. Nevertheless, Article III of the International Convention on Standards of Training, Certification and Watchkeeping

---

[230] Ngozi Medani, 'OF VESSELS, HACKERS & INSURANCE: SEAWORTHINESS & THE RISK OF CYBERATTACKS' (*linkedin*, 20 October 2017) <https://www.linkedin.com/pulse/vessels-hackers-insurance-seaworthiness-risk-ngozi-medani/> accessed 19 November 2021.
[231] Stevens (n. 103).
[232] Kao (n. 214) p. 501.
[233] ibid.
[234] Stevens (n. 103).

for Seafarers (STWC Convention) only applies to seafarers servicing onboard seagoing ships.[235] Thus, the training requirement for the onshore staff would therefore not apply.[236] Hence, in a situation of cyber-incident, it would not make the vessel unseaworthy if the onshore personnel would not have adequate cyber training. Nevertheless, as a suggestion, it is reasonable for the staff working onshore to have good cyber hygiene practices and have at least minimal understanding of what type of cyber risks may occur and how to detect, deal and recover from them.[237]

4.2.2.2. Appropriate training manuals for the crew

At the moment, there are no mandatory cyber security training requirements for the crew and the master under the STCW Convention.[238] However, according to the ISM Code, the crew should have an adequate understanding of relevant rules, regulations, codes, and guidelines, hence be adequately trained, and qualified for their task.[239] Proper training forms the backbone of cyber risk management. It is therefore essential and recommended that all company personnel should receive basic cyber training. Furthermore, nowadays, many organizations provide online courses educating about common cyber-attacks that crew can face. These include, for example, JWC International and ASPIDA that provide a maritime cyber security training program designated for ship personnel, shipping company employees, and relevant workers through E-learning.[240]

4.2.3. Documents and certificates

As for the problems related to the documentation and its availability on board, it is likely that the following. For the ship to be seaworthy, appropriate documentation needs to be always accessible onboard the vessel. This is true in the context of international and national standards. Perhaps for the foreseeable future, it will be an international standard to have documentation

[235] International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW Convention) 1978, Art. III.
[236] Stevens (n. 103) p. 249.
[237] ibid.
[238] Lee and others (n. 8).
[239] ISM Code, Art. 6.2, and Art. 6.4.
[240] ibid.

related to cyber risk available on board.[241] International Maritime Organization, BIMCO and other institutions directly involved in the maritime industry and shipping have already published numerous recommendations and documents relating to cyber risk management. It is a matter of time when these will become mandatory and thus will form part of various documents that already need to be available onboard the vessel. Hence, not having such documents on board can, in the future, render the ship unseaworthy. For now, it would be reasonable and beneficial for the boats to have copies of IMO Guidelines, BIMCO Guidelines, and other suggested guidelines that aid the response to cyber threats available at hand in any case of an unwanted cyber incident.[242] Furthermore, other documents that may become compulsory include certificates of training on cyber-attacks for the master and crew or certificates that confirm that onboard software is updated and tested regularly for vulnerabilities[243]. Port state control may require such documentation, and its inspectors may request information on cyber risk management for a vessel as a part of its seaworthiness.[244]

4.3. Can the carrier be exempt from liability under Art. IV of the HVR?

As discussed in Chapter 2 on Seaworthiness, the concept of due diligence as introduced in Art. III(1) of the Hague-Visby Rules does not provide an absolute obligation. On the contrary, it represents a positive obligation for the carrier if he wants to enjoy the protection of the Rules in Art. IV HVR. Therefore, if, in any case, the carrier does not provide a seaworthy vessel but has a reasonable reason why he does so and can prove that he has actually acted with due diligence, he may not be liable for the breach and thus be relieved of liability. However, if the shipowner has not exercised due care, he will not be able to benefit from the protection provided for in Art. IV. The burden of proof, therefore, lies with the carrier or another person requesting the exemption. Who must prove that he or the persons for whom he is responsible have exercised due care to make the ship seaworthy.

Hence, if cybersecurity forms a part of seaworthiness, could the carrier invoke one of the exceptions provided in Art. IV(2) of the HVR? Whether a cyber-attack could qualify as an exception under the HVR will depend on the previous level of cyber security imposed by the

[241] Kao (n. 214) p. 494.
[242] ibid.
[243] ibid.
[244] ibid.

IMO on each vessel. Hence, in the context of Art. IV(2), there are a couple of preliminary matters worth considering. These include errors in navigation or management, ordinary perils of the sea, the act of public enemies, latent defects, or any other cause. The following section will examine all these points in detail.

4.3.1. Art. IV(2)(a) Navigation errors

The carrier might seek to enforce the exception in Art. IV(2)(a) for errors (acts, neglect, or default) caused by personnel working onboard the vessel in the navigation or the management of the ship.[245] Here, the carrier might argue that even though all systems were working correctly and he took all measures to secure the vessel with appropriate software and hardware, a cyberattack has occurred due to some act or misconduct caused by a crewmember, as a result of which the system failed, and cyberattack struck.[246] It will be difficult for the carrier to argue that, for example, a vessel hit a quay or struck a reef due to misconduct caused by a crewmember. Due to his negligence that compromised the system and allowed the attack to enter and control the vessel. It might be challenging for the carrier to blame the crewmember, as the attacker was the actual cause of the fault in navigation. Therefore, although a crew member may be the one to blame (for compromising the system), the attacker caused the navigation error. In general, the exception is relatively complex and is difficult to apply. Courts are reluctant to excuse the carrier from the negligence of his employees.[247] In addition, this failure could also be interpreted as the inability of the carrier to exercise due diligence to make the vessel seaworthy in terms of crew training in order to avoid such situations.[248]

4.3.2. Art. IV(2)(c) Perils, dangers, and accidents of the sea or other navigable water

The vessel must be "...fit to meet and undergo the perils of the sea." Peril of the sea is a liability that might be excused under the HVR Art. IV(2)(c). What does this term entail regarding cyber security? Could cyber-attacks be considered as 'ordinary perils of the seas'? Well, the phrase

[245] Sőzer (n. 4).
[246] ibid.
[247] Claude Pohlit, 'New Developments in Maritime Security and Their Impact on International Shipping' (LL.M dissertation, University of Cape Town 2014).
[248] ibid.

does not necessarily cover all accidents or casualties that take place at sea.[249] "A peril whose only connection with the sea is that it arises on board ship is not necessarily a peril of the sea."[250] Often, these words cover only incidents directly related to the sea itself or incidents that could not have occurred on land.[251] Commonly, the term refers to ordinary actions of wind and waves, and cyber-attacks are not events peculiar to sea.[252] Therefore, with a high probability when the courts will interpret this phrase. Cyber-attacks will not be considered as ordinary perils of the sea.

4.3.3. Art. IV(2)(f) Act of public enemies

Another possibility for the carrier is to argue that the cyber-attack constituted piracy and could therefore escape liable under Art. IV(2)(f).[253] However, it is unlikely that cyberattacks are to be qualified as "piracy."[254] One of the defining elements of piracy is the use of physical force during a robbery at sea, whereas a cyber-attack is an attack that takes place in a virtual sphere.[255] Furthermore, Art. 101(a) of UNCLOS defines piracy as "any illegal acts of violence or detention, [...] committed [...] by the crew or the passengers of a private ship or a private aircraft, and directed on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft."[256] But a cyberattack is not violent nor carried out from a ship at sea (even though it technically might).[257] Cyberattacks might involve detention. However, when for example, the attackers detain a ship using ransomware, it will not be a violent act.[258] Thus, it is unlikely that the carrier might be able to invoke the exception of Art. IV(2)(f) and argue successfully that the cyberattack amounted to piracy.

---

[249] Wan Izatul Asma Wan Talaat, 'PERILS OF THE SEA: A CONLUSIVE DEFINITION?' [2003] XXXII (1) INSAF 55 p. 73.
[250] *Stott Steamers Ltd v. Marten* [1916] AC 304, p. 311.
[251] Sőzer (n. 4).
[252] ibid.
[253] ibid.
[254] ibid.
[255] ibid.
[256] United Nations Convention on the Law of the Sea (UNCLOS) 1982, Art. 101(a).
[257] Sőzer (n. 4).
[258] ibid.

4.3.4. Art. IV(2)(p) Latent defects not discoverable by due diligence

More realistically, the carrier might rely on the exception of Art. IV(2)(p). Under this exception, the carrier might be released from liability if a hidden error caused the loss or damage to the cargo.[259] And this defect could not have been discovered when the carrier exercised due diligence.[260] Federal Court of Australia considered this exception in the *Seafood Imports Pty Ltd v ANL Singapore Pte Ltd*. In this case, damage to the cargo amounted to incompatibility of software fitted in the refrigerated container supplied by the carrier.[261] The court, in the end, decided not to apply this exception and thus missed its opportunity to adjudicate on matters related to new technology. Yet, the exception of Art. IV(2)(p) can potentially provide a safe harbor for carriers in case of a software misfunction causing loss of or damage to cargo.[262] Nonetheless, it might not protect the carrier from liability when a cyberattack occurs due to the defect that made it possible to happen, as the exception covers the loss of or damage due to the defect. Furthermore, a cyberattack is not really a "defect."

4.3.5. Art. IV(2)(q) Any other cause

Last but not least is the exception of Art. IV(2)(q) for defects that command the required means of discharging the rather onerous onus of proof.[263] This clause is the so-called "catch-all" exemption. It depends upon the absence of actual fault or privity of the carrier, which he must explicitly prove.[264] As a result, the person claiming the exception must prove that the carrier or his staff were not at fault. There is a possibility that the cargo owner could demonstrate that the carrier was negligent in implementing cyber security procedures to deter cyber-attacks. In such a case, the carrier must prove that he has done everything that a reasonable prudent owner would do to protect the vessel and cargo from cyber-attacks and that the damage occurred despite all his efforts. For now, this exception has the highest chance of success. However, in the future,

---

[259] Melis Ozdel, 'Reconceptualising the Nautical Fault Exception in the Fog of Emerging Technologies' [2021] Industrial Law Journal <https://doi.org/10.1093/indlaw/dwab028> accessed 19 November 2021.
[260] ibid.
[261] *Seafood Imports Pty Ltd v ANL Singapore Pte Ltd* (2010) FCA 702.
[262] Ozdel (n. 259).
[263] Sőzer (n. 4).
[264] ibid.

when the awareness of the importance of cyberattacks and cybersecurity requirements will be defined better, it might be more difficult for the carrier to meet the burden of proof.

4.4. Conclusion

In light of the analysis, it can be concluded that with an increase of cyber-attacks and their awareness by the international community, cybersecurity and maritime cyber risk management will fall under the notion of seaworthiness. To make the vessel seaworthy is an inherent obligation that the carrier has and must fulfill. The ship is seaworthy if she has a degree of fitness that enables her to sustain the ordinary perils of the sea. Thus, the vessel is unseaworthy when a lack or deficiency threatens her safety (or safety of her cargo.) Hence, the shipowner should do everything in his power to protect the ship and her cargo. And this then also applies to taking all measures to protect her from cyber-attacks. Thus, if cybersecurity falls under the notion of seaworthiness, the carrier can use one of the exceptions from liability provided in the Art. IV of the Hague-Visby Rules. These exceptions are harder to be applied. However, they still might have a chance of success, and the carrier can rely on them.

5. Conclusion

The context of the threat of cybercrime in shipping and its parameters are currently unknown. However, what is known is that the number of attacks targeting the shipping industry will keep growing. Hence shipowners must do all that is in their power to comply with various practices proposed by the international community to implement cyber risk management systems and protocols into their current safety and security management practices to avoid, transfer or mitigate all cyber-related risks. Hence, since the awareness of cybersecurity-related matters is growing, does cyber security and maritime cyber risk management fall under the notion of seaworthiness? I say yes, it does.

In this respect, it is worth reiterating the three central tenets of the traditional concept of vessel's seaworthiness as expressed under the Carriage of Goods and Marine Insurance Law. Firstly, is the physical seaworthiness of the ship. A ship is seaworthy if it has a degree of fitness that the ordinary prudent owner would require her to have at the commencement of the voyage. Thus, accordingly, the vessel is seaworthy if she is able to sustain the usual perils of the sea. Secondly, the vessel's seaworthiness extends beyond her physical fitness. Thus, the owner must also ensure that the ship has an adequate, efficient, and competent crew. Each vessel must have crewmen that have proper qualifications, certifications, and professional behavior. Such is to ensure that they can deal with various contingencies arising at sea. Thirdly, the owner must secure that documentation and certification as required by international and national standards are always present onboard. These are equal to navigation documents, ship plans, and any other documents crucial for the vessel to load and unload cargo or sail to its destination. Lastly is the cargo-worthiness of the ship. Through which the owner must guarantee the vessel's ability to receive, transport, and deliver the agreed cargo to the designated destination. Ultimately, we must remember that all these elements are to be understood and examined in the context of the current state of knowledge in the industry.

Hence, looking at the matter in a narrower context. The carrier must take all measures to protect the ship (together with her cargo) against the ordinary perils of the sea that she might encounter on her voyage. Therefore, one could interpret this phrase as a duty of the owner to take all necessary steps to protect the vessel against potential cyber-attacks. Then, if the owner fails to equip the ship with adequate cyber-attack resilient systems, educate the crew on how to respond

to such attacks and carry required documentation. The vessel could be considered unseaworthy, and hence, the shipowner failed to exercise due diligence to make her seaworthy. Thus, with increasing knowledge of cyber-attacks and greater awareness of cyber threats and vulnerabilities. As well as with a higher risk and probability of cyber incidents, it is reasonable to conclude that cybersecurity falls under the notion of seaworthiness. And the shipowners' failure to implement cyber risk management can render the vessel unseaworthy. Shipowners are therefore expected to take positive steps to address the potential for cyberattacks that may arise during the voyage for the vessel to be considered seaworthy. Lastly, it will become increasingly difficult for the shipowners to argue successfully that the state of knowledge in the industry allows them to do nothing to address the potential of cyberattacks. As well as make use of Art. IV of the Hague-Visby Rules and thus limit his liability. He will be able to rely on the exceptions provided by the Hague-Visby Rules. Over time, however, the standards that courts will adhere to carriers will be higher. Therefore, it can be very tedious and difficult for the carrier to invoke any of the exceptions. The highest chance of success for the carrier lies in the exception enshrined in Art. IV (2)(q). This provision is a so-called "catch-all" exception, where the person claiming the exception must prove that the carrier or its employees have not been at fault. The best solution for a carrier on how to prevent its vessel from being unseaworthy is to comply with the maritime cyber risk management standards provided by the international community. Furthermore, he should provide proper training and education for his employees on the potential dangers of cyber-related threats and carry recommended documents on board. So, in case of an attack, the crew will be able to respond to the attacks. Hence, overall, as long as the carrier can demonstrate that he has exercised due diligence, he may not be held liable for a breach of his obligation and thus can exempt himself from liability.

Table of reference

Primary Sources:

Legislation

Harter Act 1893

Marine Insurance Act 1906

The Norwegian Maritime Code 1994

The Croatian Maritime Code 1994

International Convention for the Unification of certain Rules of Law relating to Bills of Lading ("Hague Rules", and Protocol of Signature (adopted 25 August 1924, Brussels)

The Hague Rules as Amended by the Brussels Protocol 1968 (The Hague-Visby Rules)

United Nations Convention on the Carriage of Goods by Sea, 1978 (Hamburg Rules) (adopted 9 December 1993, UNGA Res 48/34)

International Maritime Organization, and International Conference on Training and Certification of seafarers, International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW Convention) 1978 (adopted by the International Conference on training and Certification of Seafarers, London 1978)

International Maritime Organization, Interim Guidelines on Maritime Cyber Risk Management, 1 June 2016 (MSC.1/Circ 1526)

International Maritime Organization, Maritime Cyber Risk Management in Safety Management Systems, 16 June 2017 (Resolution MSC.428(98))

International Maritime Organization, International Safety Management Code (ISM Code) 1993 (IMO Assembly Resolution A.741(18))

Amendments to the Annex to the International Convention for the Safety of Life at Sea (SOLAS) 1974, appendix 5, International Ship and Port Facility Security (ISPS) Code 2002

United Nations Convention on the Law of the Sea (UNCLOS) 1982, 1833 U.N.T.S. 397.

Guidelines and Recommendations

BIMCO, The Guidelines on Cyber Security Onboard Ships (Version 4)

International Maritime Organization, Guidelines on maritime cyber risk management, 5 July 2017 (MSC-FAL1./Circ.3)

Case law

A. Meredith Jones & Co. Ltd. v. Vangemar Shipping Co. Ltd., ('The Apostolis') (No. 2), [1997] 2 Lloyd's Rep. 241, [1999] 2 Lloyd's Rep, [2002] 2 Lloyd's Rep. 337

Ben Line Steamers Ltd. v. Pacific Steam Navigation Co ('The Benlawers'), [1989] 2 Lloyd's Rep. 51

Burges v. Wickham (1863) 3 B & S 669

Cheick Boutros Selim El-Khoury and Others v. Ceylon Shipping Lines, Lld., ('The Madeleine'*), 2 Lloyd's Rep. 224*

Dixon v. Sadler, 5 M. & W. 405

F. C. Bradley & Sons Ltd. v. Federal Steam Navigation Co. Ltd. (1926) 24 Lloyd's List Rep. 446

Grand Champion Tankers Ltd. Appellants v. Norpipe A/S and Others Respondents, ('The Marion'), [1982] 2 Lloyd's Rep. 52

Hedley v. The Pinkney and Sons Steamship Company, Limited [1892] 1 Q.B. 58

Hong Kong Fir Shipping Co Ltd v Kawasaki Kisen Kaisha Ltd, ('The Hongkong Fir'), [1961] 1 Lloyd's Rep. 159

Kopitoff v. Wilson (1987) 1 Q.B.D. 377

Martin v. Southwark, 191 U.S. 1, 24 S. Ct. 1, 48 L. Ed. 65 (1903)

Maxine Footwear Company Ltd. v. Canadian Government Merchant Marine Ltd. (The Maurienne) [1959] 2 Lloyd's. Rep. 105

McFadden v. Blue Star Line [1905] 1 KB 697

M.D.C. Ltd. v. N.V. Zeevart Maatschappij Beursstraat, [1962] 1 Lloyd's Rep. 180

Minister of Materials v. World Steamship Company Ltd., [1952] 1 Lloyd's Rep. 485

Papera Traders Co. Ltd. v. Hyundai Merchant Marine Co. Ltd. ('The Eurasian Dream') [2002] EWHC 118 (Comm), [2002] WL 45386

Paterson Steamship Ltd. v. Robin Hood Mills Ltd, ('The Thordoc'), (1973) 58 LI.L. Rep. 33

President of India By and Through Director of India Supply Mission v. West Coast S. S. Co. [1964] 327 F/2d 638 (9th Cir. 1964)

Riverstone Meat Co Pty Ltd. v. Lancashire Shipping Co ('The Muncaster Castle'*) [*1961] A.C 807

Robin Hood Flour Mills, Ltd. v. N. M. Paterson & Sons, Ltd, ('The Farrandoc'), [1967] 2 Lloyd's Rep. 276

Seafood Imports Pty Ltd v ANL Singapore Pte Ltd (2010) FCA 702

Steel & Craig v. State Line Steamship Co., [1978] SLR 15

Stott Steamers Ltd v. Marten [1916] AC 304

The Oakley C. Curtis, 4 F.2d 979 (2d Cir. 1924)

The Sagamore, (1924), 300 Fed. 701, 1924 A.M.C. 961 (2nd Cir. 1924)

The T.J. Hooper, 53 F.2d 107 (S.D.N.Y. 1931), aff'd, 60 F.2d 737 (2d Cir. 1932)

Union Steamship Co. of British Columbia v. Drysdale [1902] 32 SCR 379

Secondary sources:

Books

Baughen S, *Shipping Law* (4th edn, Routledge-Cavendish 2009)

Singh L, *The Law of Carriage of Goods by Sea* (Bloomsbury Professional 2011)

Treitel G.H and Reynolds F.M.B, *Carver on Bills of Lading* (4th edn, Sweet & Maxwell Ltd 2017)

Margetson N.J., The system of liability of articles III and IV of The Hague [Visby] Rules (Paris Legal Publishers 2008)

Edited books (& chapters)

Chacón V.H, 'Chapter 2: The Origin of the Obligation of Practicing Due Diligence in Maritime Transportation' in *The Due Diligence in Maritime Transportation in the Technological Era* (1st edn, Springer, Cham 2017).

Chacón V.H, 'Chapter 4: The New Technologies Applied in Maritime Transportation' in *The Due Diligence in Maritime Transportation in the Technological Era* (1st edn, Springer, Cham 2017).

Lessa, J.C.C., and Bulut, B. 'A New Era, a New Risk! "A Study on the Impact of the Developments of New Technologies in the Shipping Industry and Marine Insurance Market"' in in Pierpaolo Marano and Kyriaki Noussia (eds), *InsurTech: A Legal and Regulatory View* (Springer, Cham 2020)

Otto L. (ed), *Global Challenges in Maritime Security* (1st edn, Springer, Cham 2020)

Sőzer D.B, 'Seaworthiness: In the context of cyber-risk or "cyberworthiness"' in Barış Soyer and Andrew Tettenborn (eds), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (1st edn, Informa Law from Routledge 2020)

Stevens F., 'Seaworthiness and good seamanship in the age of autonomous vessels' in ***Henrik Ringbom, Erik Røsæg*** and Trond Solvang (eds), *Autonomous Ships and the Law* (1th edn, Routledge 2020).

Treitel G.H and Reynolds F.M.B, 'Chapter 9: Section 1. (b)(i) – Seaworthiness' in *Carver on Bills of Lading* (4th edn, Sweet & Maxwell Ltd 2017)

Law Journals

Androjna A, Brcko T, Pavic I, Greidanus H, 'Assessing Cyber Challenges of Maritime Navigation' [2020] 8(10) Journal of Marine Science and Engineering 1

Cain P., 'The perils of the sea, proximity and seaworthiness: The loss of the *Marina Iris*' [2014] 1(3) Australian Journal of Maritime & Ocean Affairs 97-105

Kao M.B., 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' (2021) 45 Tul Mar LJ 467

Katsivela M, 'The Effect of Unmanned Vessels on Canadian Law: Some Basic Legal Concepts' [2018] 4 Maritime Safety and Security Law Journal 47

Lee Y.C, Park S.K, Lee W.K, Kang J, 'Improving cyber security awareness in maritime transport: A way forward' [2017] 41(8) Journal of the Korean Society of Maritime Engineering 738

Mashkina N.A, Belyaeva E.S, Obukhova A.S and Belyaeva O.V, 'Digitalization of The Transport Industry in The Context of Globalization of The World Economy' (2021) 92 SHS Web of Conferences 1

Meland P.H, Bernsmed K, Wille E, Rodseth O.J, Nesheim D.A, 'A Retrospective Analysis of Maritime Cyber Security Incidents' [2021] 15(3) TransNav the International Journal on Marine Navigation and Safety of Sea Transportation 519

Metalidou E. and others, 'The Human Factor of Information Security: Unintentional Damage Perspective' (2014) 147 Procedia - Social and Behavioral Sciences 424

Senarak C, 'Port cybersecurity and threat: A structural model for prevention and policy development' (2020) 37 The Asian Journal of Shipping and Logistics 20.

Suri M, 'Autonomous Ships and The Proximate Cause Conundrum - A Maritime and Insurance Law Tango' [2020] 51(2) Journal of Maritime Law & Commerce 163

Svilicic B, Kamahara J, Celic J, Bolmsten J, 'Assessing ship cyber risks: a framework and case study of ECDIS security' [2019] 18 WMU Journal of Maritime Affairs 509.

Wan Izatul Asma Wan Talaat, 'PERILS OF THE SEA: A CONLUSIVE DEFINITION?' [2003] XXXII (1) INSAF 55

Online Journals

Boyan M. and others, 'Analysis of Cybersecurity Issues in the Maritime Industry' [2021] 47(1) Information & Security: An International Journal 27

Caprolu M. and others, 'Vessels Cybersecurity: Issues, Challenges, and the Road Ahead' [2020] 58(6) IEEE Communications Magazine 90

Franchina F., 'THE SEAWORTHINESS: AN OLD WARRANTY FOR A NEW DUTY' [2017] XV Rivista di Diritto dell'Economica, dei tranporti e dell'Ambiente 73

Katsivela M,, 'The treatment of the sea peril exception of the Hague-Visby Rules in common law and civil law jurisdictions' [2017] 16 WMU J Marit Affairs <https://doi.org/10.1007/s13437-016-0103-y> accessed 19 November 2021

Mustafa Y., 'Legal Assessment of Seaworthiness in Autonomous Cargo Ships: Is It Time for a Change?' 2020 3(2) DEHUKAMDER 803 <https://www.researchgate.net/publication/352121588_LEGAL_ASSESSMENT_OF_SEAWORTHINESS_IN_AUTONOMOUS_CARGO_SHIPS_IS_IT_TIME_FOR_A_CHANGE> accessed 19 November 2021.

Ozdel M., 'Reconceptualising the Nautical Fault Exception in the Fog of Emerging Technologies' [2021] Industrial Law Journal <https://doi.org/10.1093/indlaw/dwab028> accessed 19 November 2021

Tsimplis M. and Papadas S., 'Information Technology in Navigation: Problems in Legal Implementation and Liability' [2019] 72(4) Journal of Navigation 833 <http://dx.doi.org/10.1017/S0373463318001030> accessed 19 November 2021

Yilmaz M., 'THE EVOLUTION OF THE OBLIGATION OF SEAWORTHINESS FROM THE HAGUE RULES TO THE ROTTERDAM RULES' [2021] 29(2) Selcuk Universitesi Hukuk Fakultesi Dergisi 881

Zarzuelo I., 'Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue' [2021] 100 Transport Policy 1

Other Resources

European Union Agency for Cybersecurity, 'DECISION No MB/2020/7 of the Management Board of the European Union Agency for Cybersecurity (ENISA) amending Section III "Work Programme Year 2020" of the ENISA Programming document 2020-2021' (ENISA, MB Decision/7/2020)

Conference papers

Joseph DiRenzo, Dana A. Goward and Tred S. Roberts, 'The Little-known Challenge of Maritime Cyber Security' (2015 6th International Conferece on Information, Intelligene, Systems and Applications (IISA), 2015)

Theses

Alifragki M.E, 'Cyber-Attacks: The new type of piracy in the Maritime World' (Master Thesis, University of Piraeus 2019)

Chacon V.H, 'Due Diligence in Maritime Transportation in the Technological Era' (DPhil dissertation, University of Hamburg 2016)

Dadiani D, 'Cyber-security and marine insurance' (Master of Science dissertation, World Maritime University 2018)

Kassem A.H, 'The Legal Aspects of Seaworthiness: Current Law and Development' (DPhil thesis, University of Wales 2006)

Kirchner A, 'Rise of the Machines – A Legal analysis of Seaworthiness in the context of autonomous shipping' (Master thesis, Lund University 2019).

Kothari B.S, 'The role of technology in maritime security: a survey of its development, application, and adequacy' (Master of Science dissertation, World Maritime University 2008).

Pohlit C., 'New Developments in Maritime Security and Their Impact on International Shipping' (LL.M dissertation, University of Cape Town 2014).

Quiong H., 'Research on the Carrier's Seaworthiness Obligation in *Rotterdam Rules* and the Influence on the *China Maritime Code*' (Master of Science thesis, World Maritime University 2015)

Yang Y., 'The abolition of the nautical fault exemption: to be or not to be' (Mater thesis, Lund University 2011).

Reports

European Cyber Security Organisation (ECSO), 'Transportation Sector Report – Cyber security for road, rail, air, and sea' (WG3 Sectoral Demand, March 2020)

The European Network and Information Security Agency (ENISA), 'Cyber Security Aspects in the Maritime Sector' (The European Union Agency for Cybersecurity, November 2011)

Loomis W, Singh V.V, Kessler G.C, Bellekens X, 'RAISING THE COLORS: Signaling for Cooperating on Maritime Cybersecurity' (Atlantic Council, Scowcroft Center for Strategy and Security, October 2021)

The European Network and Information Security Agency (ENISA), 'Port Cybersecurity: Good practices for cybersecurity in the maritime sector' (The European Union Agency for Cybersecurity, November 2019)

IMO, 'Measures to enhance maritime security' (Maritime Safety Committee, MSC 96/WP.9, 17 May 2016)

Online Resources (Websites)

'A Comprehensive Guide to Maritime Cybersecurity' (*Mission Secure* , 2021) <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach> accessed 19 November 2021

Ajay Menon, '8 Major Types of Cargo ransported Through the Shipping Industry' (*marineinsight,* 23 September 2021) <https://www.marineinsight.com/types-of-ships/8-major-types-of-cargo-transported-through-the-shipping-industry/> accessed 19 November 2021

All Answers ltd, 'The Role of Seaworthiness in Shipping Legislation' (*lawteacher.net,* November 2021) <https://www.lawteacher.net/free-law-essays/international-law/the-role-of-seaworthiness-in-shipping-legislation-international-law-essay.php#ftn2> accessed 19 November 2021

Arora C.A, Antoniadou E, 'Maritime Cyber Risk Management Guidelines' (*Standard Club*, October 2020) <https://www.standard-club.com/fileadmin/uploads/standardclub/Documents/Import/publications/loss-prevention-industry-expertise-handouts/3365323-sc_ie_cyber_risks_20201117_final.pdf> accessed 19 November 2021

Commander Michael C. Petta, 'The IMO 2021 Cyber Guidelines and the Need to Secure Seaports' (*The Maritime Executive,* 10 January 2021) <https://www.maritime-executive.com/editorials/the-imo-2021-cyber-guidelines-and-the-need-to-secure-seaports> accessed 19 November 2021

'Cybersecurity Policies' (European Comission, 2021) <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies> accessed 19 November 2021

'Digitalization in the maritime/shipping industry' (*Marine Digital*, 2021) <https://marine-digital.com/article_digitalization_in_the_maritime_industry> accessed 19 November 2021

'Due diligence to make a vessel seaworthy' (*Gard,* 1 December 2000) <https://www.gard.no/web/updates/content/52444/due-diligence-to-make-a-vessel-seaworthy> accessed 19 November 2021

'Due diligence' (*Ship Inspection*, date unknown) <http://shipinspection.eu/due-diligence/> accessed 19 November 2021

'Duty to provide a seaworthy vessel' (*Ship Inspection,* date unknown) <http://shipinspection.eu/duty-to-provide-a-seaworthy-vessel/> accessed 19 November 2021

Hugh Taylor, 'What Are Cyber Threats and What to Do About Them' (THE MISSING REPORT, 16 June 2021) <https://preyproject.com/blog/en/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them/> accessed 19 November 2021

'KEEPING CYBERSAFE' (*ISO*, 2021) https://www.iso.org/news/ref2629.html accessed 19 November 2021

'Maritime cyber security' (DNV 2021). <https://www.dnv.com/maritime/insights/topics/maritime-cyber-security/index.html> accessed 19 November 2021

Martin Placek, 'Ocean shipping worldwide – statistics & facts' (*statista*, 9 August 2021) <https://www.statista.com/topics/1728/ocean-shipping/#topicHeader__wrapper> accessed 19 November 2021

Nina Kollar, Sam J. Tangredi, and Chris C. Demchak, 'THE CYBER MARITIME ENVIRONMENT: A SHARED CRITICAL INFRASTRUCTURE AND TRUMP'S MARITIME CYBER SECURITY PLAN' (*warontherocks*, 4 February 2021) < https://warontherocks.com/2021/02/the-cyber-maritime-environment-a-shared-critical-infrastructure-and-trumps-maritime-cyber-security-plan/> accessed 19 November 2021

'Seaworthiness in Shipping and Carriage' (All Answers lts, 3rd July 2019) <https://www.lawteacher.net/free-law-essays/transportation-law/seaworthiness-in-shipping-and-carriage.php> accessed 19 November 2021

Shirish Nadkarni, 'Cyber attacks on the rise in shipping' (*Seatrade Maritime News*, 23 November 2020) <https://www.seatrade-maritime.com/technology/cyber-attacks-rise-shipping> accessed 19 November 2021

'Smart Containers' (Global Infrastructure Hub, 4 November 2020) < https://www.gihub.org/resources/showcase-projects/smart-containers/> accessed 19 November 2021

'The Shipping Revolution: 5 Technologies that are Transforming the Shipping Industry' (*cogoport*, April 29, 2020) <https://www.cogoport.com/blogs/technologies-transforming-shipping-industry> accessed 19 November 2021

'USING THE CYBERSECURITY FRAMEWORK' (*cisa*, 28 August 2020) <https://www.cisa.gov/using-cybersecurity-framework> accessed 19 November 2021

Philipp Stratmann and Zac Staples, 'We Cannot Afford to Wait to Bolster Maritime Cybersecurity' (*nextgov*, 15 September, 2021) <https://www.nextgov.com/ideas/2021/09/we-cannot-afford-wait-bolster-maritime-cybersecurity/185359/> accessed 19 November 2021

Ken Munro, 'Are you cyber seaworthy' *(Pan Test Partners,* 17 April 2020) <https://www.pentestpartners.com/security-blog/are-you-cyber-seaworthy/> accessed 19 November 2021

'Seaworthiness redefined in the new age? Interim guidelines on maritime cyber risk management' (*Norton Rose Fulbright,* November 2016) <https://www.nortonrosefulbright.com/es-es/knowledge/publications/96f95702/seaworthiness-redefined-in-the-new-age-interim-guidelines-on-maritime-cyber-risk-management> accessed 19 November 2021

Luke Parsons QC and Julian Clark, 'Can Cyber Risk Challenge Traditional Concepts such as Seaworthiness?' (*Quadrant Chambers*, 14 September 2017) <https://www.quadrantchambers.com/news/can-cyber-risk-challenge-traditional-concepts-such-seaworthiness-luke-parsons-qc-julian-clark> accessed 19 November 2021

Martyn Wingrove, 'Cyber security is part of seaworthiness' (*riviera*, 21 August 2020) <https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-security-is-part-of-seaworthiness-60671> accessed 19 November 2021

'Marine cyber risk and insurance' (*howden*, 6 November 2020) <https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden> accessed 19 November 2021

Julian Clark, 'The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels: Shipping Laws and Regulations 2021 (*ICLG*, 6 August 2021) <https://iclg.com/practice-areas/shipping-laws-and-regulations/1-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels> accessed 19 November 2021

Karen Maxwell, 'Cyber-seaworthiness: the calm before the storm?' (*Twenty Essex*, 18 April 2018) <https://twentyessex.com/20-essex-street-bulletin-cyber-seaworthiness-the-calm-before-the-storm/> accessed 19 November 2021

Svetlana Ormane, 'Cyber Security. Is the ship seaworthy?' (*Marine Underwriting Services*, date unknown) <https://marineservices.lv/wp-content/uploads/cyber-security-is-the-ship-seaworthy.pdf> accessed 19 November 2021

Ngozi Medani, 'OF VESSELS, HACKERS & INSURANCE: SEAWORTHINESS & THE RISK OF CYBERATTACKS' (*linkedin*, 20 October 2017) <https://www.linkedin.com/pulse/vessels-hackers-insurance-seaworthiness-risk-ngozi-medani/> accessed 19 November 2021

Rosehana Amin, Rory Duncan, Daniel Jones, 'Part 1: A very modern form of piracy: cybercrime against the shipping industry – Rapidly developing risks' (Clyde&Co, 23 March 2021 <https://www.clydeco.com/en/insights/2021/03/a-very-modern-form-of-piracy-cybercrime-against-th> accessed 19 November 2021

MI News Network, 'Cyber Risk Management Comes of Age' (*marineinsight*, 18 December 2020) <https://www.marineinsight.com/shipping-news/cyber-risk-management-comes-of-age/> accessed 19 November 2021

Olivia Delagrance, Jose Pellicer, 'Assessing the cyber risks of maritime navigation' (*kennedyslaw*, December 2017) <https://kennedyslaw.com/media/3288/kennedys_assessingthecyberrisksofmaritimenavigation.pdf> accessed 19 November 2021.

Kimberly Tam, Kevin Jones, Maria Papadaki, 'Threats and Impacts in Maritime Cyber Security' (Engineering & Technology Reference, January 2016) <https://www.researchgate.net/publication/304263412_Threats_and_Impacts_in_Maritime_Cyber_Security> accessed 19 November 2021.

Linda Jacques, 'The effect of cyber-attacks on the shipping industry' (*lesteraldridge*, 29 May 2018) <https://www.lesteraldridge.com/blog/marine/effect-of-cyber-attacks-on-shipping-industry/> accessed 19 November 2021

James Rundle, 'Maritime Cyber Rules Coming in 2021 Are Outdated, Critics Say' (*The Wall Street Journal*, 18 July 2019) <https://www.wsj.com/articles/maritime-cyber-rules-coming-in-2021-are-outdated-critics-say-11563442201> accessed 19 November 2021

The Editorial Team, 'Maersk Line: Surviving from a cyber attack' (*SAFETY4SEA*, 31 May 2018) <https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/> accessed 19 November 2021

International Maritime Organization, 'The International Safety Management (ISM) Code' (*IMO*, 2019) <https://www.imo.org/en/OurWork/HumanElement/Pages/ISMCode.aspx> accessed 19 November 2021

Martin Placek, 'Ocean shipping worldwide – statistics & facts' (*statista*, 9 August 2021) <https://www.statista.com/topics/1728/ocean-shipping/> accessed 19 November 2021

Statista Research Department, 'Transport volume of seaborne trade from 1990 to 2020' (*statista*, 22 November 2021) <https://www.statista.com/statistics/264117/tonnage-of-worldwide-maritime-trade-since-1990/> accessed 19 November 2021

International Maritime Organization, 'Maritime cyber risk' (*imo,* 2019) <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx> accessed 19 November 2021

Kayla Elliott, 'Targeted Attacks or Untargeted Attacks – Which is Most Common' (TechTalk, 13 September 2018) <https://techtalk.pcmatic.com/2018/09/13/untargeted-targeted-attacks-untargeted/> accessed 19 November 2021

The Shipowner's Club, 'Continuing Warranty of Seaworthiness' (*shiponwersclub*, 9 October 2018) <https://www.shipownersclub.com/continuing-warranty-of-seaworthiness/> accessed 19 November 2021

SHM, 'Impact of maritime security on the global maritime industry' (*shmgroup*, 12th May 2019) <https://www.shmgroup.com/blog/impact-of-maritime-security-on-the-global-maritime-industry/> accessed 19 November 2021

'**A SHIPOWNER'S GUIDE** TO ACHIEVING CYBER SECURITY' (*Bureau Veritas*, 2021) <https://marine-offshore.bureauveritas.com/ship-owners-guide-achieving-cyber-security> accessed 19 November 2021.