UiO : Faculty of Law
University of Oslo

A Dive into Cyber Attacks in Autonomous Vessels and the Hull Insurance Market

A round-up review of autonomous vessels, coverage of cyber-attacks under the Nordic Hull Insurance market as compared with the English position and management of cyber-attacks, including safety management systems.

Candidate number: 207

Submission deadline: June 1, 2023

Number of words: 17,342

Table of contents

1 INTRODUCTION

1.1 General Overview

The focus of this thesis is to explore the possible cyber threats facing autonomous vessels and the extent to which insurers, specifically those offering Hull and Machinery ("**H&M**") insurance in Norway, as compared with English jurisdiction, provide cover for cyber-attacks on autonomous ships. Furthermore, this thesis will explore the extent to which insurers can manage cyber threats onboard sophisticated autonomous vessels, by reference to insurance contracts, assureds duties and safety management systems. To understand these issues, the following areas will be explored:

1. The meaning of 'cyber threats' in autonomous vessels, as compared with traditional, manned vessels;

2. An analysis of whether the marine insurance market in Norway, as compared with England, caters for cyber threats by reference to H&M policies and insurance conditions typically contained therein; and

3. A consideration of assureds duties in both, Norwegian and English maritime insurance market and management of cyber risk, including compliance with safety management systems.

The above topics will be considered in order, following by an overarching conclusion regarding the extent to which H&M policies provide cover for cyber-attacks.

The concept of autonomous vessels, a detailed explanation of which is contained in the second chapter of this thesis, has grasped considerable academic, industry and government attention, as has the concept of cyber-attacks. It is undeniable that both topics have independently been considered at length. However, given the multidisciplinary characteristic of cyber-attacks, it remains difficult to understand exactly what type of cyber-attacks face autonomous vessels specifically, and the extent of damage such attacks can cause. In addition, a lack of clear understanding of various cyber-threats in the industry means that protection by way of insurance may fall short, or simply not cater for the resulting cyber-attacks that may arise from cyber-threats on autonomous vessels.

As Rolls-Royce has identified as early as 2016, *"Cybersecurity will be critical to the safe and successful operation of remote and autonomous vessels"*[1], following in 2017 with: *"Protecting […] data streams and ship's systems to which they connect from hackers will, of course, be crucial. You don't want troublemakers to divert ships from their route, or worse, make them collide with something"*[2].

Relatedly, the term "cyber security" is at the forefront of insurers minds in light of the introduction of increasingly sophisticated vessel systems. England's National Security Cyber Centre has identified general "cyber security" as relating to: *"… how individuals and organisations reduce the risk of a cyber attack"*[3]. Cyber security in relation to shipping is concerned with data protection of IT systems, hardware and sensors located onboard ships, data leaks from unauthorised access as well as disruption[4]. With the increase in 'state-of-the-art' autonomous vessels, such as the Yara Birkeland in Norway, the first ever zero emission, autonomous container ship[5], perpetrators have shifted their focus to cyber-attacks which can disrupt the safe operation of the vessel at sea, particularly as they can be controlled from ashore. One such example is the world's first uncrewed freight route at sea has been approved in Trondheimsjord[6], that is being remotely controlled.

For all vessels, H&M insurance is pivotal, as it protects a vessel or fleet against physical damage caused by perils at sea, or other perils that are covered under an insurance policy while the vessel is in transit over water[7]. Such insurance transfers the risk of, often considerable, financial loss due to unpredictable events, in exchange for a premium. A shortfall in insurance may result in shipowners facing large losses that have severe implications on a business. One such example

---

[1] Rolls Royce, "Rolls-Royce unveils a vision of the future of remote and autonomous shipping", last modified 12 April 2016, https://www.rolls-royce.com/media/press-releases/2016/pr-12-04-2016-rr-unveils-a-vision-of-future-of-remote-and-autonomus-shipping.aspx.

[2] MFame Team, "Forget Autonomous Cars – Autonomous Ships Are Almost Here", last modified 31 January 2017, https://mfame.guru/forget-autonomous-cars-autonomous-ships-almost/.

[3] National Cyber Security Centre, "What is cyber security?", last accessed 24 May 2023, https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.

[4] Marine Digital, "The importance of cybersecurity in the maritime industry", last accessed 24 May 2023, https://marine-digital.com/article_importance_of_cybersecurity.

[5] Yara International ASA, "The first ever zero emission, autonomous ship", last accessed 24 May 2023, https://www.yara.com/knowledge-grows/game-changer-for-the-environment/.

[6] Maritime Robotics, "World's first uncrewed freight route at sea in the Trondheimsfjord", last modified 2 March 2023, https://www.maritimerobotics.com/post/world-s-first-uncrewed-freight-route-at-sea-in-the-trondheimsfjord.

[7] Howden Insurance, "Marine hull insurance", last accessed 24 May 2023, https://www.howdengroup.com/id-en/cover/marine-hull.

relates to the cyber-attack against Maersk, where malware spread through the company's network and beyond, resulting in damages over USD 10 billion[8]. It is therefore important to examine how cybersecurity in general is viewed by insurers, to what extent shipowners are protected in the event of a cyber-attack and related duties which may impact cover for cyber-related loss.

1.2 Structure, Methodology and Legal Sources

The following chapters of the paper will firstly define what is meant by 'autonomous shipping', before turning to cyber threats posed to autonomous vessels. In order to place the legal analysis into the context of autonomous vessels, it has been necessary to include a section detailing the technical complexities of the systems utilised by such vessels. Such an overview is intended to provide the reader with a basic level of understanding around the different software that may be subject of a cyber-attack. A review of the technical software was carried out with the assistance of research studies and opinions by professionals in the technical sphere.

The description of cyber threats will turn to consider what different risks face traditional, manned vessels and what novel risks arise in autonomous, crewless vessels that may materialise into cyber-attacks. Secondly, the attention will turn to the marine insurance market, specifically H&M insurance in Norway. This position will be compared with the English insurance market, given its prominence in the field, comparing insurance conditions and how cyber-attacks are treated. Thirdly, the paper will turn to the assured duties contained in insurance policies, including duties of disclosure and care, which are relied on by insurers to manage the likelihood of cyber-attacks occurring on autonomous vessels.

As will be discussed, cyber threats and resulting attacks are greater in autonomous vessels due to the novel technology utilised onboard and offshore. A consideration is therefore given to what tools exist in the market to allow insurers to manage cyber-threats in autonomous vessels by reference to assureds duties as well as re-insurance. The paper will conclude by summarising the findings related to cyber threats in autonomous shipping, cover afforded by H&M policies, proposed ways for insurers to adequately cater for such risks and authors' own conclusions.

In order to answer the above research questions, a number of sources will be utilised including the legal framework relevant to H&M insurance policies, the relevant law and precedents.

[8] Industrial CyberSecurity Pulse, "Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk", last modified 30 September 2021, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/.

In respect of the analysis of cyber-attack coverage in H&M policies, a review of the Nordic Marine Insurance Plan of 2013, Version 2023 ("**NP**") and the Institute Time Clauses Hulls 1983 ("**ITCH**"), subject to English law and jurisdiction has been undertaken.

The NP and ITCH are standard contracts utilised by insurers in insurance policies that regulate hull insurance, and are therefore fundamental in this review. The NP is based on an 'all risk' concept and as will be discussed in detail in the following chapters by default provides cyber coverage[9]. Due to the 'all risk' approach of the NP, insurers often deviate from it by excluding certain matters from cover and insert their own wording in the insurance contract. Accordingly, a review will be undertaken into the perils typically excluded by CL380, LMA5402 and LMA5403, commonly known as Institute Cyber Attack Exclusion Clause, Marine Cyber Exclusion Clause and Marine Cyber Endorsement, respectively. The review includes a reference to the Commentary contained in the NP, as well as insurance contracts. The NP and the Commentary are intended to be read alongside each other, with the Commentary assisting readers in understanding how the clauses operate.

Similarly, the ITCH will be evaluated, to understand how the position in England varies from the Nordics, if at all. The ITCH are based on Lloyd's S.G. Forms of policy, as formerly included in the Marine Insurance Act 1905 (First Schedule) ("**MIA**"). The ITCH, as the NP, have been and continue to be, widely used in the respective marine markets. While the NP is the result of an agreement between shipowners and insurers, the ITCH was developed solely by Lloyd's. Furthermore, contrary to the NP's 'all-risks' principle, the ITCH is based on the "named perils" principle, as will be discussed in this thesis.

In relation to the management of cyber-attacks, the focus is on the mandatory requirements that are placed on shipowners, including a review of IMO's Resolution MSC.428(98) *"Maritime Cyber Risk Management in Safety Management Systems"*[10]. Assureds duties, the assured being the party that is entitled to compensation under the insurance contract[11] will be considered as part of this review. Assureds duties play an important part in the overall insurance contract and are regulated by the insurance conditions which are considered in the latter part of this thesis. A comparison will be made between the assureds duties set out in the NP with the English legal system contained in MIA and the Insurance Act 2015 ("**IA**").

---

[9] The Nordic Marine Insurance Plan of 2013, Version 2023, https://www.nordicplan.org/the-plan/.

[10] Resolution MSC.428(98) (adopted on 16 June 2017), "Maritime Cyber Risk Management in Safety Management Systems" https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf.

[11] NP Cl. 1-1 (b) and (c).

1.3 Scope of Study and Limitations

This paper will mainly focus on the Norwegian marine insurance market and Norwegian H&M and war risk policies, comparing the position with the English approach, given its prominence in the marine insurance market. However, the NP which is being reviewed as part of the analysis is applicable across all of the Nordics. The thesis is limited to vessels only.

2 WHAT IS 'AUTONOMOUS SHIPPING'?

2.1 IMO Definition

The International Maritime Organisation's ("**IMO**") Maritime Safety Committee completed a regulatory scoping exercise on Maritime Autonomous Surface Ships[2] ("**MASS**")[12], defining MASS as *"a ship which, to a varying degree, can operate independently of human interaction"*[13]. Unmanned ships have also been defined by scholars as: *"those which are capable of controlled movement on the water in the absence of any on board crew"*[14].

The IMO proposed four degrees of autonomy: (1) board crews with automated processes; (2) remotely controlled ship with seafarers on board; (3) remotely controlled ships without seafarers on board; and (4) fully autonomous ships[15].

Categories (3) and (4) concern crewless vessels which can be remotely controlled from ashore by crew, or by artificial intelligence. Categories (3) and (4) will be the main focus of the thesis, however, to the extent the thesis reviews cyber risks by reference to the location from which various human functions in relation to the performance of the vessel are performed, categories (1) and (2) will also be considered.

2.2 Information Technology Systems and the role of Artificial Intelligence

Autonomous vessels are particularly vulnerable to cyber-attacks due to the information technology systems utilised aboard a vessel, specifically, the operational technology ("**OT**") equipment. Without delving into the complexity of computer systems onboard vessels, it is important

---

[12] International Maritime Organisation, "Autonomous Ships: regulatory scoping exercise completed", last modified 25 May 2021, https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx.

[13] International Maritime Organisation, "IMO takes first steps to address autonomous ships", last modified 25 May 2018, https://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx.

[14] Robert Veal and Henrik Ringbom, "Unmanned ships and the International Regulatory Framework": *Journal of International Maritime Law.* 2017, 23 (2), 1.

[15] International Maritime Organisation, "Autonomous Ships: regulatory scoping exercise completed", https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx.

to understand the basic components that make up an automated ship in order to assess the type of cyber threats that may materialise, as will be discussed in Chapter 3 of this thesis.

2.2.1 Information Technology and Operational Technology

Information technology ("**IT**") on board a vessel is connected to the internet, which assists with the processing of data onboard, as well as streamlining the flow of information between different parties in the maritime industry. OT equipment *"exchanges online communications data with the shore for monitoring the main functions of the ship"*[16] . Simply, OT controls the vessel itself as well as other systems aboard. The distinction between IT and OT systems is around the use of the data; IT systems focus on the *use of data as information*, whereas OT systems *use the data to control or monitor* physical processes[17]. The use of OT systems, together with the integration of IT systems, are collectively known as Cyber Physical Systems that constitute the central part of the digitalisation onboard ships[18].

While many existing, manned vessels are digitalised and make use of, for example, auto-pilot systems utilising sophisticated navigational equipment on board a ship, systems deployed in automated vessels go one step further and use *"...modern IT-enabled operations [that] are allowed to be accessed and controlled by outward-facing information systems, through interfaces that are rarely adequately secure"*[19]. While it can be compared with usual IT systems utilised by businesses worldwide, the OT systems which are utilised by vessels pose unique vulnerabilities to the maritime industry. The Electrical Nautical Chart Systems ("**ECDIS**") is a pivotal example, as the control and navigation of autonomous vessels is based on satellite navigation relying on Electronic Chart Displays.

As explained by G. Kavallieratos and S. Katsikas, remotely operated and autonomous vessels are a type of cyber-enabled ships, which is a cyber physical ecosystem: *"...consisting of the vessel itself, a Shore Control Centre ("**SCC**") that controls and handles the C-ES [Cyber-Enabled Ship, and] communication links between the vessel and the SCC, and other ships in the vicinity"*[20]. With this increasing focus on SCC's, sophisticated communication systems and utilisation of ECDIS, new cyber threats arise as is considered in detail at Chapter 3 of this thesis.

---

[16] Zăgan Remus, Raicu Gabriel, "Understanding of the cyber risk on board ship and ship stability" *Annals of "Dunarea de Jos" University of Galati*, (2019): 81.

[17] International Maritime Organisation, Guidelines on Maritime Cyber Risk Management, 14 June 2021: 2.1.2.

[18] Kavallieratos Georgios, Sokratis Katsikas, Managing Cyber Security Risks of the Cyber-Enabled Ship, *Journal of Marine Science and Engineering*, 8, 768 (2020): 1.

[19] Ibid.

[20] Ibid.

2.2.2 Artificial Intelligence

Autonomous vessels are facilitated by artificial intelligence ("**AI**"). As outlined by J. A. Glomsrud et al *"...one can even consider AI and autonomy as synonymous given the deployment of AI in any transport system entails the transfer of decision making from humans to algorithms"*[21]. AI is already making headway in the maritime industry, and is expected to increase safety and efficiency of future maritime navigation[22] with the capabilities of enabling ships to navigate, dock and make decisions on their own[23]. AI works by utilising sensors, algorithms and machine learning. Sensors and related software equipment will assist with the collection of data related to vessel's surroundings, which is fed into AI algorithms that use machine learning which interprets the information. For example, if a navigation system onboard an autonomous vessel utilises AI, it will be able to utilise data it gathered around it in order to determine the most efficient route for the vessel based on sea conditions and the weather.

3 CYBER AND AUTONOMOUS VESSELS

3.1 Definitions

The term 'cyber security' has been referred to in the introduction of this thesis. It relates to the protection of IT systems, hardware and sensors onboard vessels. However, the concept of 'cyber' must also be fully understood, before the relatively new terms such as 'cyber-threats' and 'cyber-attacks' are considered.

Cyber in general relates to anything that is related to computers, networks and digital technology. It has been highlighted that 'cyber' as a concept has become an *"insurance industry shorthand for a variety of information technology risks, including but not limited to: hardware, software, IT consulting, cloud services, and data processing"*[24]. It appears to be a broad, catch-all term, that is intended to cover a variety of cyber security threats and attacks on vessels.

A cyber security threat can be defined as a harmful act that is intended to harm, steal or disrupt data, such as acts leading to the installation of computer viruses and data breaches[25]. A cyber

---

[21] Glomsrud Jon Arne et al, Trustworthy versus Explainable AI in Autonomous Vessels, in *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC)*, (Helsinki, 2019), 37.

[22] Safety4Sea, A brief introduction to AI and its applications in the maritime industry, last modified 8 February 2023, https://safety4sea.com/cm-a-brief-introduction-to-ai-and-its-applications-in-the-maritime-industry/.

[23] Ibid.

[24] Martinez, P. Leo, Cyber Risks: Three Basic Structural Issues to Resolve, in *InsurTech: a Legal and Regulatory View*, (Springer, 2020): 212.

[25] Prey Project, "What are cyber threats and how to safeguard your data", last modified 21 April 2023, https://prey-project.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them.

security threat is synonymous with 'cyber-threats', which are harmful activities intending to disrupt data and digital life.

In turn, the IMO has defined *'maritime cyber risk'* as a threat to a technology asset due to a potential circumstance or event resulting in shipping-related failures[26]. For example, the term 'cyber risk' can include financial loss, disruption to business operations or damage to reputation of a shipping organisation. This thesis will focus on the cyber threats and cyber-attacks in autonomous shipping.

As referred to above, autonomous ships, like traditional, manned ships, make use of auto-pilot systems and sophisticated navigation equipment. However, to what extent do the cyber threats facing autonomous vessels actually differ to traditional, manned vessels?

In short, greater cyber threats may materialise due to untested, novel, combinations of sophisticated autonomy technology employed by automated vessels[27]. Indeed, these factors were considered during the development of the cover for construction risk in the NP. The revised construction risk sections in the NP include updated definitions and exclusions. Furthermore, new provisions were added, that deal with design errors and omissions, to account for the technology being utilised in the shipping industry.

As a lot of the technologies associated with autonomous vessels have not yet been tested and despite a number of advances, it has not yet been possible to assess the full risks and vulnerabilities associated with autonomous shipping. As such, it is questionable whether marine insurers are able to predict with accuracy, what novel risks may present themselves, and further yet, to provide guidelines to prevent them from arising. Nevertheless, to aid in the discussion and shed some light on the *possible* cyber-threats and how these may vary from traditional, manned vessels, different types of cyber threats are examined below, to provide context for analysis under Nordic and UK marine insurance policies.

3.2 Types of Cyber Threats

3.2.1 Shore Control Centres and Connectivity

The concept of SCC or 'remote operability' is not new. Indeed, underwater remotely operated vehicles have been utilised in areas that are too dangerous for commercial divers, as they can be operated from a nearby shore or boat. Furthermore, the YARA Birkeland, as referred to

[26] IMO Guidelines on Maritime Cyber Risk Management: 1.1.

[27] Tam, Kimberley and Jones, Kevin, "Cyber Risk Assessment for Autonomous Ships", *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* (Glasgow, UK, 2018): 1.

above, is set up to be controlled by three on-shore centres who oversee emergency, operational and conditional monitoring[28].

SCCs permit a human operator to control the vessel remotely, ranging from simple monitoring of the vessel, to full controllability of vessel's systems[29]. To effectively control the vessel's navigation, a SCC will have remote access to vessel's navigation equipment[30] as well as data and communication systems utilised by unmanned vessels. It is these connections that pose the biggest cyber-threats. As commented by V. Bolbot et al: *"Attacks on the shore control centre and the ship control station, targeting at obtaining privileged access, have the highest potential safety implication and thus can be of high interest to terrorists for the specific vessel"*[31].

IT and OT systems (as referred to above in Chapter 2), are frequently connected to the internet, which in and of itself creates risks of unauthorised access and/or malicious attacks to vessels' networks and systems[32]. As SCC are frequently equipped with systems that have a direct access to public networks, they are considered to be the ones that are the easiest to exploit[33]. Indeed, it is considered that GPS in its current form is easily exploitable[34]. A GPS signal related attack usually means that hackers have taken control of a ship i.e. are in control of a GPS signal that controls the navigation of the vessel and are able to manipulate the system to show an incorrect location of the vessel, otherwise known as 'spoofing'. The risks of spoofing already exist in manned vessels at sea today, indeed, a number of incidents have been reported to date. For example, the Yuk Tung vessel used the spoofing technique on its own Automatic Identification System ("**AIS**"), in order to impersonate another vessel, alter its own course to hide their identity and conduct shipments in violation of sanctions[35]. AIS is used to control vessel traffic in seaways and works by tracking the vessel's position and movements via the vessel's GPS systems[36]. As reliance on GPS signal grows in autonomous vessels, specifically where the vessel is controlled from a SCC and there is no crew on board to act promptly, the risks of collision and/or loss of vessels is arguably much greater, as is the risk of a cyber-attack.

---

[28] Ibid: 2.

[29] Ringbom, Henrik and Collin Flexi, Terminology and concepts, in *Autonomous Ships and the Law, 1st ed.* (Taylor and Francis, 2020): 9.

[30] Ibid.

[31] Bolbot, Victor et al, A novel cyber-risk assessment method for ship systems, *Safety Science 131* (2020): 8.

[32] Zăgan R. "Understanding of the cyber risk": 82.

[33] Bolbot, V, "A novel cyber-risk assessment": 8.

[34] Ibid.

[35] United Nations, Security Council, last modified 5 March 2019 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf: 9.

[36] NATO Shipping Centre, "AIS (Automatic Identification System) overview", last modified 2021, https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview.

Similarly, with the increased reliance on ECDIS, potential cyber-attackers may be able to manipulate the vessel's navigation, through the introduction of manipulated nautical charts. While the current, manned vessels make use of auto-pilot and similar technology, they are not controlled from SCC which can pose greater risks when it comes to cyber-attacks.

While not considered in detail in this thesis, it is important to note that a cyber-attack may materialise due to a human operator being subject to a 'phishing' attack. Cyber-attackers usually use 'phishing' in order to deceive humans into either installing malware or deceive humans into releasing confidential information. For example, in the maritime industry, the inadvertent installation of a ransomware by a member of staff may result in a vessel being re-directed at sea. Such malware may not be obvious, nor spotted, until the risk itself materialises particularly where a cyber-attacker can manipulate the malware to be triggered in specific locations.

3.2.2 Autonomous Vessel Software

Aside from traditional sensors and radar systems located on existing, manned vessels, it is envisaged that autonomous vessels will host a new type of sensor system relating to object recognition, alongside traditional radar systems[37]. Object recognition software is important, as autonomous vessels will host a new range of sensors, meaning that the vessel will need to identify the position of nearby objects[38]. Such technology relies on radio detection and ranging, which may be subject to a cyber-attack. As is explained by K. Tam and K. Jones, traditionally radar-based attacks pose low risks to manned vessels due to the presence of crew who gather information from various sources, including visual cues[39]. Autonomous vessels, on the other hand, are more vulnerable to cyber-attacks due to their reliance on radar sensors, and similar software which emit sound that cyber-attackers may exploit[40]. An exploitation of such technologies may pose an increased risk related to cargo management. For example, the mappings of cargo and sensor systems will be reliant on communication channels that are required in autonomous vessels that make an autonomous ship more vulnerable[41]. Sensory data is used by human crew when making decisions relating to the operation of the ship, however, an autonomous vessel will be solely dependent on, for example, satellite data and AIS that can be easily hacked[42].

The above technological advances in autonomous vessels present significant cyber vulnerabilities. As autonomous ships become more reliant on technology and AI systems, *"…the attack-*

[37] Tam, Kimberley, "Cyber Risk Assessment": 2.
[38] Ibid: 5.
[39] Ibid.
[40] Ibid.
[41] Ibid: 3.
[42] Ibid.

surface of an autonomous ships is significantly more than traditional ships."[43]. This means that arguably, a cyber-hackers' task is easier due to the interaction between systems and reliance of data that can be accessed remotely and subsequently tampered with.

In summary, the risks which are faced by autonomous vessels vary greatly to those of manned, traditional vessels at sea due to the following factors:

1. Vulnerability to remote attacks. As has been outlined above, autonomous vessels heavily rely on sensors, GPS and control systems which can be manipulated by cyber-attackers. Manned vessels, on the other hand, retain manual controls which are not so easily accessible to cyber-attackers.

2. Dependence on technology. Manned vessels continue to rely on skilled, experienced crew members who are positions on the bridge of the ships and maintain control over the systems onboard the vessels. Autonomous vessels, on the other hand, rely on technologies to operate, which makes them much more susceptible to cyber-attacks.

3. Limited physical access. Traditionally, in the event of a cyber-attacks and/or other attacks to a vessel at sea, only crew had access to critical systems onboard the vessels. In autonomous vessels such critical control systems can be accessed remotely, making them more vulnerable to cyber-attacks.

4. Complexity of systems. Due to the utilisation of AI, as has been explained above, cyber-attacks can now create systems which manipulate the algorithms and compromise vessel's systems.

As such, the various cyber-attacks on autonomous vessels are much more complex requiring sophisticated cyber-security measures in order to mitigate such risks, as will be discussed below. In the next section, examples of possible cyber-attacks on autonomous vessels are explored.

3.3 Cyber Attack Examples

Having outlined how autonomous vessels operate by reference to various systems and how cyber risks differ to the usual risks associated with traditional vessels by reference to specific software systems and onshore centres, specific examples of possible cyber-attacks are explored below.

[43] Ibid: 2.

In order to analyse the potential risks in autonomous vessels, one needs to consider the motivations of cyber-attackers. For example, a cyber-attack based on terrorism will vary significantly in gravity to potential cyber-attacks initiated by, for example, competitors in the maritime industry. The former may take over a vessel in order to transform it into a weapon or an asset to be used for war purposes, whereas the latter may focus on accessing data for competition purposes, hacking into some of the shore based centres with no direct impact on the vessel at sea[44]. Competitors may also seek to disrupt operations of an autonomous vessel, by tampering with the automated cargo management systems and diverting the cargo during loading. This would include manipulation of GPS systems and propulsion systems utilised onboard the vessels (a mechanism that drives the vessel through the water). The propulsion system is critical and if hacked, can lead to a number of serious implications as it directly affects the vessel's speed, manoeuvrability and performance.

In relation to criminals who are motivated by monetary rewards, they may steal and/or modify communications data for smuggling of prohibited goods, or target goods in transit, at sea, or at ports. This could include the installation of malware on the vessel's systems which would enable an attacker to steal sensitive information from the vessel's database. Furthermore, the use of cyber-attacks on communication systems utilised by autonomous vessels, as described above, may enable criminals to steal cargo, or even the ship itself. It may also become possible for cyber-attackers to take control of the SCC's in order to take control over 100 vessels, all at once. The extent to which this would be possible depends on whether each SCC and vessel companies utilise the same electronic systems. While such an example may seem far removed from reality, it will be by no means impossible.

Another possibility is an attack by a group of activists who are becoming a lot more advanced in their quest to disrupt certain activities i.e. to make a statement regarding the maritime industry and/or to target the cargo onboard a vessel. As no human crew is present onboard the vessel, there is no real risk to life which may encourage activists to engage in cyber-attacks on autonomous vessels[45].

In parallel, it is also important to recognise that, for example, an attack by a terrorist organisation seeking to weaponise a vessel is unlikely. The most likely threat is likely to come from criminals who are aware of the potential financial gain resulting from a cyber-attack. Furthermore, it is likely that the most common form of cyber-attack is the installation of malicious malware on an information system, which, once installed, enables the hacker to control and/or

[44] Ibid: 4.

[45] Ibid: 2.

shut down the systems[46]. It could be argued that some of the examples above present risks which are present today, particularly as many vessels already possess autonomous systems, such as AIS. However, the difference lies in the fact that an autonomous vessel will heavily rely on advances technologies while at sea with little to no human presence on board. This means that the possibility to manually take over the operation of the vessel may not be as immediate. Of course, SCCs are being built in such a way so as to be alerted of any problems but it is difficult to envisage such systems being as effective as crew onboard a vessel.

The above examples serve as examples of the type of cyber-risks that are unique to autonomous vessels at sea. While the use of systems and advanced technologies is seen as increasing safety and efficiency, it is also increasing the likelihood of cyber-attacks arising due to data and communication systems utilised by such systems, as has been explored above. With this in mind, it is important to understand how, if at all, and the extent to which, the marine insurance market responds in the event of a cyber-attack, and extent to which shipowners are protected in such eventualities.

4 MARINE INSURANCE MARKET

4.1 The Norwegian Marine Insurance Framework

In Norway, the marine insurance framework is governed by the Insurance Contract Act 1989, the NP, the Norwegian Cargo Clauses 2004, as well as the Gard and Skuld P&I Conditions 2011. The NP is the focal point of this thesis, as it provides most of the relevant insurances that a shipowner may wish to purchase, including H&M and War Risk Insurance.

Cl. 1-1 of the NP sets out definitions of the parties to the insurance contract, as follows:

(a) The insurer: *"the party who under the terms of the contract has undertaken to grant insurance"*;

(b) The person effecting the insurance: *"the party who has entered into the insurance contract with the insurer"*; and

(c) The assured: *"the party who is entitled under the insurance contract to compensation or the sum insured"*[47].

[46] MacFarlane, Rory, "Cyber-risk in shipping and its management", in *Ship Operations, New Risks, Liabilities and Technologies in the Maritime Sector*, (Routledge, UK, 2021): 71.

The main distinction concerns the person effecting the insurance, with whom the insurer has an insurance contract, and the assured. The assured is the person who is entitled under such an insurance contract to compensation from the insurer. In relation to H&M insurance policies, as will be discussed below, this distinction is important as it could be the bareboat charterer who effects the insurance, but the shipowner who would be entitled to claim for damage under the insurance policy, as the assured[48]. This thesis will refer to the assured, as the person who can claim compensation in the event of damage or loss of the vessel.

Separately, another important player in the marine insurance market is the re-insurer. As will be explained below, due to the potentially large exposures related to damage or loss of a vessel, the insurer will take out a re-insurance policy, which re-insures the risk that is undertaken by the insurer under the insurance contract with the assured.

4.2 Types of Insurances

The marine insurance market is wide and covers a range of different economic risks. Insofar as vessels are concerned, a shipowner would typically consider the following insurances:

1. H&M Insurance, a type of property insurance covering physical damage to, and loss of, the vessel itself and its equipment resulting from for example, collision or grounding.

2. Loss of Hire Insurance relating to shipowners' loss of income following damage to the insured vessel. The loss of time must be due to damage that is in principle covered under the shipowners' H&M policy[49].

3. Marine Cargo Insurance, insuring the economic interest in the cargo catering specifically to the marine cargo carried by the vessel.

4. Protection and Indemnity Insurance ("**P&I**"), which forms part of the P&I club cover (a mutual insurance group providing risk pooling, information and representation to its

[48] NP Commentary Cl.1.1.

[49] GARD, "Loss of Hire Insurance – Back to Basics", last modified 14 September 2016, https://www.gard.no/web/updates/content/21853295/loss-of-hire-insurance-back-to-basics#:~:text=The%20loss%20of%20hire%20insurers,policy%20the%20claim%20falls%20under.

members), covering, amongst other things the vessel owners' liability arising from injury to persons onboard, as well as damage to other ships following a collision, pollution and fines.

5. War Insurance, insuring the economic interest in the vessel against war and war-related perils. Such war insurance is intended to fill a gap in insurance, as standard property and P&I insurances do not respond to loss and liabilities due to war and terrorism.

6. Defence Insurance otherwise known as "FD&D" insurance, insuring economic interests relating to legal costs in pursuing or defending claims relating to the insured vessel.

In addition to the above marine insurances, cyber insurance is available in the insurance market, but not specifically within the marine insurance sphere. Cyber insurance is not usually seen as the 'standard' insurance taken by shipowners, with cyber-risks being generally accepted risks in the industry. This is particularly due to the design of the traditional vessels that make up most of the vessels at sea which, while make use of GPS and electronic charts, rely on human crew and general on-board management of the vessel.

The focus of this thesis is on H&M insurance, and the extent to which cyber risks are covered under standard conditions. As part of this analysis, a review of how cyber exclusion clauses typically included in H&M policies will be undertaken. As will be explored below, one of the reasons for the introduction of cyber exclusion clauses relates to the attempted elimination of what has been termed as "silent cyber". "Silent cyber" relates to cyber risk that is not expressly covered or excluded in an insurance policy, which has the result of coverage uncertainty for the assureds, who did not know whether they were, or were not covered for cyber risk[50]. Silent cyber relates cyber specific losses which arise from insurance policies, such as H&M, that were not designed to account for cyber risks which exist in today's society. It is due to this issue, that this thesis intends to clarify how the conditions in H&M policies treat cyber risk.

For a complete review of cyber risk coverage in the maritime insurance market, war risk insurance, forming part of H&M insurance and referred to in NP Cl. 2-9, will be evaluated.

[50] WTW "Silent Cyber: What you need to know", last modified 1 February 2021, https://www.wtwco.com/en-GB/Insights/2021/01/silent-cyber-what-you-need-to-know.

5 Hull and Machinery Insurance

The type of H&M policies underwritten by insurers differs from country to country as different policy wordings are used by maritime underwriters. This section focuses on the Nordic insurance contracts which are regulated by the NP. Further, a comparison is made to an English position, given its prominence in the maritime insurance industry.

5.1 H&M Insurance Conditions: Nordics

Nordic marine insurance contracts are based on the NP, an agreed document which is deeply rooted in the Norwegian marine insurance market. The NP dates back to 1871, and is now updated by the Standing Revision Committee every 4 years[51]. Some of the earlier years of the NP contained provisions related to cargo as well as P&I insurances. These were later removed in 1967 and 1996, respectively and were instead dealt with by the Norwegian Conditions relating to Insurance for the Carriage of Goods and by P&I clubs. The NP is an Agreed Document between shipowners and insurers which comprehensively sets out rules related to insurance contracts, covering, amongst others, rules relating to H&M and war insurance. The NP is maintained and published by CEFOR, which is the Nordic Association of Marine Insurers, in collaboration with the Danish Shipowners' Association, the Norwegian Shipowners' Association, the Swedish Shipowners' Association and the Finnish Shipowners' Association. Part One (Chapters 1-9) of the NP deal with rules common to all types of insurance and Part Two (Chapters 10-13) of the NP deal with hull insurance; the focus of this thesis[52]. It is common for Norwegian H&M insurers to base their insurance policies on the NP.

5.1.1 Scope of H&M Cover

Scope of cover in insurance generally refers to the extent of cover provided by an insurance contract. An insurance contract will set out the risks which it covers, as well as limits of cover and exclusions that may apply. This scope of cover varies from policy to policy and is dependent on the terms utilised.

H&M insurance policies as based on the NP provide coverage under the "all risks" concept, meaning that all risks are covered, unless specifically excluded. The "all risks" concept is important as it provides cover for new perils, or the perils which were not thought about at the time of writing of the policy.

---

[51] Wihelmsen, Trine-Lise and Bull, Hans Jacob, Handbook on Hull Insurance, (2nd ed. 2017): 65.

[52] GARD, "the Nordic Marine Insurance Plan of 2013, Version 2023", last modified 20 October 2022, https://www.gard.no/web/articles?documentId=34367309.

The risks which the assured is insured against i.e. the perils that are covered by a H&M policy, can include, for example, unexpected weather, failure of equipment or human error. For an assured to be able to claim under a H&M policy, a peril, of the type insured under the policy, must be established before an insurer provides compensation and accepts liability under an insurance contract[53]. As a H&M policy is an 'all-risks' policy, an insurer will accept liability unless the loss arose out of a peril that is specifically excluded, as will be addressed below. In this regard, causation must be present. Cl. 2-11 of the NP confirms that the insurer will only be liable *"when the interest insured is struck by an insured peril during the insurance period"*[54]. A usual H&M policy will be for a limited time, usually a year, and in order to trigger insurers liability the Commentary to the NP confirms that there is a requirement of a causal connection between the peril that is insured under the policy, and the loss that was suffered by the assured (the insured interest[55]), which occurred during the policy year.

By way of example, in order for H&M insurance to provide coverage for a cyber-attack, several conditions must be met. Firstly, the attack must fall within the purview of an insured peril that is not excluded from coverage. Secondly, there must be an occurrence of an insured event, which results in loss of the vessel. Thirdly, the loss incurred must have caused damage to the assured, such as a total loss. Finally, the loss must have occurred within the policy period. These conditions serve as the fundamental criteria for assessing the coverage of cyber risks under H&M policies.

5.1.2 Hull Interest Insurance

At this juncture, a distinction must be made in respect of ordinary H&M Insurance and Hull Interest Insurance. Ordinary H&M insurance covers the market value of the vessel insured under the policy and under such insurance any extra compensation in excess of market value is not provided[56]. Hull Interest insurance therefore exists to provide shipowners with cover for the additional excess of the vessel's market value. This includes cover up to the mortgage value of a vessel as well as the additional costs of replacing a vessel, where it is a total loss[57]. Only H&M insurance is being considered in this thesis.

---

[53] MasterThesis, "Coverage of Cyber Risks in the Norwegian Insurance Market", University of Oslo, 2022: 8-10.

[54] NP Cl. 2-11.

[55] NP Commentary Cl. 2-11.

[56] The Swedish Club, "Increased Value Insurance/Hull Interest Insurance", last modified June 2015, https://www.swedishclub.com/media_upload/files/Hull%20Interest%20InsuranceJ.pdf.

[57] Ibid.

5.1.3 Perils insured

As has been outlined, the biggest risks in relation to potential cyber-attacks arise due to the technologies utilised by autonomous vessels, including communication equipment, programs and data that is exchanged, together with the use of SCCs. To review whether cyber-attacks on such technologies fall under cover in H&M policies, NP Cl. 2-8 will be reviewed, as it details the insured marine perils.

Cl. 2-8 covers the perils covered by an insurance against marine perils. Cl. 2-8 of the NP states: *"An insurance against marine perils covers all perils to which the interest may be exposed, with the exception of..."*[58]. As has been stated above, the NP covers all risks, other than those which are excluded. The exclusions are therefore important, as they comprise of risk which insurers are not willing to expose themselves to. The exclusions include, amongst others:

1. Perils covered by war insurance as per Cl. 2-9; and
2. Standard exclusions, including Radioactive Contamination, Chemical, Biological, Biochemical and Electromagnetic Weapons exclusion clause ("**RACE**").

Cl. 2-8(e) relating to the RACE exclusion includes a reference to "electromagnetic weapon" which, as has been confirmed in the Commentary to the NP, means *"sophisticated mechanisms designed to destroy computer software, and not to methods for detonating or attaching explosives"*[59]. A reference to *"sophisticated mechanisms designed to destroy computer software"* could include cyber-attacks on a vessel, as cyber-attacks are usually carried out using advanced technologies which intend to either destroy, or take over, computer software. However, a cyber-attack may result in other events such as stealing of data information, as has been discussed above, and therefore not fall within the definition. The Commentary to the NP further refers to the Cyber Attack Clause, Cl. 380, relating to an exclusion for the use of computer technology for harmful purposes[60]. Ultimately, this exclusion was not directly incorporated into the NP, but is often included in insurance contracts, as will be considered in detail below[61].

On the face of it, one must therefore conclude that apart from the reference to Cl. 2-8(e), cyber-risks related to autonomous vessels are covered, as no specific cyber-exclusion exists in the NP. The extent to which a cyber-attack constitutes a war peril in accordance with Cl. 2-9 is considered below.

---

[58] NP. 2-8.

[59] NP Commentary Cl. 2-8(e).

[60] Ibid.

[61] Ibid.

6 Marine Cyber Exclusion in the Nordics and England: Cl. 380 and LMA5402

As has been discussed, the NP is based on an "all risks" concept, and while on the face of it, the NP does provide cover for cyber-attacks, most marine property wordings contain an exclusion for losses that result from such attacks. Insurers can also deviate from the standard language contained in insurance contracts and exclude risks related to cyber-attacks by way of an additional clause inserted into the insurance contract. As noted above, the H&M insurance market is heavily dependent on re-insurance mainly due to the potentially vast sums involved in the event of a vessel collision or related accidents. Indeed, should one of the potential scenarios detailed above relating to possible cyber-attacks materialise, it can amount to total loss of a vessel. Due to potentially large exposures, insurers and re-insurers sought to manage their risks and began to exclude cyber risks from cover. In the Nordics, this exclusion is often referred to as Cl. 380 (the Institute Cyber Attack Exclusion Clause).

As with the NP, marine policies in England (including H&M, war risks and cargo policies), began to exclude losses related to cyber-attacks by way of wording akin to Cl. 380, known in England as LMA5402. A Lloyd's of London market bulletin dated 4 July 2019 required that as of 1 January 2020 all policies needed to clarify whether cover for cyber-attacks is provided or not[62], resulting in the introduction of LMA5402. LMA5402 contains wording published by the Lloyd's Market Association, and is similar to the Cl. 380 exclusion. As matters stand, insurers now include Cl. 380 / LMA5402 exclusions as standard. In England, the Prudential Regulation Authority requested that all insurers expressly state whether cyber risk is covered, resulting in LMA5402. An example of Cl. 380 and LMA5402 wording is set out below.

> *"...in no case shall this insurance cover loss damage liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any electronic system."*[63]

Such an exclusion is usual in the marine property insurance market and is often not disputed or questioned by the assured (shipowners). The result is that cyber coverage will need to be purchased separately, at an additional cost.

---

[62] Lloyd's Market Bulletin, Ref Y5258 "Providing clarity for Lloyd's customers on coverage for cyber exposures", last modified on 4 July 2019 https://assets.lloyds.com/assets/y5258-providing-clarity-for-lloyd-s-customers-on-coverage-for-cyber-exposures/1/Y5258%20-%20Providing%20clarity%20for%20Lloyd's%20customers%20on%20coverage%20for%20cyber%20exposures.pdf.

[63] Norwegian Hull Club, "Cyber Attack Exclusion Buy-Back", last accessed on 25 May 2023 https://www.norclub.com/products-and-services/cyber-attack-exclusion-buy-back.

The Cl. 380 exclusion is clear that cover in respect of physical damage that is caused by a malicious cyber-attack is excluded from a H&M policy. In order to interpret the wording, one can turn to the English case of *"The Atlantic B"*[64], which confirms that each such clause, in this case an exclusion clause in a war and strikes risks policy, should be construed in the context of each policy[65]. This is the traditional starting point for interpretation of contracts generally, and will now be used in the context of Cl. 380 and LMA5402. In addition, the commercial purpose of the clause needs be considered, and whether it is intended to exclude **all** losses which arise from cyber-attacks.

Undoubtedly, the drafting of the Cl. 380/LMA5402 clause is very broad and is intended to be a 'catch all' clause, particularly by the use of causation triggers, such as: "directly or indirectly". A causation trigger such as this one refers to language which is used in contractual clauses to establish a causal relationship between an event, and the consequence. The use of the wording indicated that an insured peril may have caused, directly or indirectly, damage or loss to the assured. There is no room for doubt in the Cl. 380/LMA5402 exclusion that losses which are "directly or indirectly" linked to a computer, or a software programme, are excluded. Indeed, using *The Atlantic B*[66] case, one can see that this aligns with the context of the exclusion i.e. to exclude all losses relating to cyber-attacks. This can be therefore be seen as a draconian exclusion, particularly given the increasing frequency of cyber-attacks in the maritime industry.

The broadness of the language used in the clause can also be seen in relation to AI software, which has been discussed in this thesis. The wording: *"computer software programme... and any other electronic system"* appear to encompass AI software, as well as any attack on a hardware as the source of loss. This is significant as many cyber-attacks are likely to target computer software and all other electronic systems utilised onboard an autonomous vessel.

However, while it contains broad language, Cl. 380/LMA5402 was introduced in order to respond to the increasing risk of cyber-attacks on vessels which have the potential to incur huge losses. Indeed, cyber-attacks have the potential to cost companies billions, such as the Maersk example included in the introduction of this thesis. The introduction of Cl. 380/LMA5402 could also be seen as a signal to the assureds (usually shipowners) to introduce robust cybersecurity measures in order to prevent cyber-attacks from materialising in the first place, as is explored below.

---

[64] [2018] UKSC 26.

[65] Soyer Baris, "Cyber-risk insurance – developing a new cover in the market", in *Ship Operations, New Risks, Liabilities and Technologies in the Maritime Sector* (Routledge, UK, 2021): 121.

[66] [2018] UKSC 26.

Questions have been raised around the extent to which insurers could continue to rely on Cl 380/LMA5402 exclusion where the shipowner suffered damage as a result of a cyber-attack by a third party. B. Sayer uses the following example to demonstrate the draconian effects of Cl. 380/LMA5402: *"…an amateur hacker circulated malware randomly, which led the ECDIS of the insured vessel to malfunctioning resulting in her grounding"* [67]. Would insurers in this instance be able to rely on the CL. 380/LMA5402 exclusion? Pursuant to the *The Atlantic B*[68] case discussed above, it is clear that Cl. 380/LMA5402 is a standalone exclusion which is intended to put any type of restrictions on who could cause loss, and to whom it was intended at. This has potentially draconian effects. Taking B. Sayer's example of a vessel grounding due to malfunctioning of the ECDIS as a result of a cyber-attack, a shipowner would not be able to claim on the policy, even though grounding is an ordinarily insured peril under H&M policies[69]. However, while one can look to the English common law system for assistance and interpretation of policy wordings, case law in the marine insurance industry relating to cyber exclusions is scarce.

Furthermore, cyber insurance does not fall part of the 'general' insurances available in the market, and as such, does not fall within the usual, 'standard' cover offered to the assureds. The position of cyber insurance is akin to the political risk cover in the NP. Specifically, the Commentary to the NP notes, in respect of political risk (used for comparison purposes), that:

> *"The standard cover provided by the Plan is not intended to provide the kind of "political risk" cover that would more fully protect owners of vessels trading to countries that have a more or less dysfunctional political system. Solutions for such vessels are available in the market and it is a matter for the assured to decide what level of more specific cover they deem appropriate. It is not natural to spread this risk over all assureds that do not trade in these areas"*[70] (emphasis added).

Similarly to political risk cover, it is up to the assureds to decide whether they require cyber risk protection and the extent of such coverage. In this regard, some insurers have started to offer services which address the Cl. 380 exclusion. For example, one insurer provides an opportunity for Cl. 380 buy-back in exchange for additional premium in order to secure cover for

[67] Soyer Baris, "Cyber Risk Insurance": 121.
[68] [2018] UKSC 26.
[69] Soyer Baris, "Cyber Risk Insurance": 122.
[70] NP Commentary Cl. 2-8.

cyber-attacks[71]. Such buy-back is bought under the war policy, regulated by NP Cl. 2-9. A war policy can be purchased for an additional premium, and will be discussed below.

In today's market, there are a number of cyber protection products in the insurance market. In addition to the buy-back, if a shipowner is utilising technology onboard an autonomous vessel which is particularly prone to cyber-attacks, they do have the possibilities to take out extra cyber-risk cover. Such cover is, however, likely to be costly, mainly due to the unknown risks which are being undertaken by insurers. Cyber risks can be difficult to predict, and as has been mentioned, a single attack can result in a total loss of a vessel. As such, it is likely that shipowners will have to pay higher premiums i.e. pay more for insurance coverage that provides protection in the event of a cyber-attack. In essence, this is a risk transfer mechanism where shipowners are expected to pay more for insurers to assume the risk of a cyber incident occurring. Due to the nature of cyber-attacks, the fact that insurers are likely to charge higher premiums for a cyber-risk policy is not surprising. A market for cyber related insurance in shipping is considered towards the end of this thesis.

As matters currently stand, it is understood that for the time being, cyber risk is not seen as a necessity in the industry and with the Cl. 380 exclusions many shipowners will find themselves without cover in the event of a potentially costly cyber-attack.

With the above in mind, a recent article published by Lloyd's List quoted a marine cyber insurer stating that: *"We are not dealing with the same degree of cyber vulnerability in 2023"*, and that when it comes to purchase of cyber-insurance, *"the biggest impediment… is that people don't trust it to pay out when it needs to"*[72]. It makes note that companies offering cyber insurance fail to take into account the improvements being made by shipowners to ensure that shipping is cyber-secure[73], something which should be reflected in the policy premiums and wordings. Shipowners' own management of risk is considered in Chapter 9 below.

6.1 LMA5403

In order to combat the potentially draconian effects of LMA5402, LMA5403 (the Marine Cyber Endorsement) was introduced by Lloyd's on 11 November 2019 in order to provide clarity in

[71] https://www.norclub.com/products-and-services/cyber-attack-exclusion-buy-back.

[72] Lloyd's List, "Lloyd's exclusion clauses do not meet shipping's needs, says marine cyber insurer", last accessed 17 May 2023.

[73] Ibid.

the insurance market i.e. eliminating 'silent cyber', as has been discussed above, and making clear the limit, or the extent, of cyber cover[74].

In England, Lloyd's developed the LMA5403 wording which provides cover for non-malicious cyber acts only, excluding losses, damage and liability of expenses arising from malicious acts[75]. LMA5403 however, maintains an exclusion relating to malicious cyber loss, as is discussed below. Example wording of LMA5403:

> *"... in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus, computer process or any other electronic system...*
>
> *Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software programme, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm.*
>
> *Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile..."*

The LMA5403 excludes cover for any "malicious" cyber loss but in turn provides affirmative cover for non-malicious acts that would be afforded cover 'but for' the cyber element. The clause therefore does vary from the other exclusions as it covers cyber accidents that were inflicted *"not as a means for inflicting harm"*[76]. However, as has been assessed above in relation to cyber-attack scenarios, most of the cyber-attacks are likely to be carried out with a malicious intent i.e. stealing of data or taking control of a vessel. Furthermore, the LMA5403 exclusion removed the need for direct causation as the endorsement refers to "any computer" as contributor to the loss[77].

---

[74] Astaara Group, "LMA 5403 A Lost Opportunity?", last modified July 2020 https://astaaragroup.com/wp-content/uploads/2020/07/LMA-5403-A-Lost-Opportunity.pdf.

[75] Liberty Specialty Market, "Cyber Cargo – addressing the coverage gap", last accessed 25 May 2023 https://www.libertyspecialtymarkets.com/static/2020-09/LSM_Cyber_Cargo_FS.pdf.

[76] Master Thesis, "Coverage of Cyber Risks in the Norwegian Insurance Market", University of Oslo, 2022: 33.

[77] Howden, "Marine cyber risk and insurance", last modified 6 November 2020 https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden.

Nevertheless, despite the fact that LMA5403 does provide wider coverage than usual insurance contracts that contain the LMA5402 or Cl. 380 wording, it arguably does not go far enough to protect shipowners with 'common' cyber-attacks, such as phishing. A phishing attack deceives humans into installing malware of deceiving humans into releasing confidential information. Such an attack would be seen as 'malicious', and therefore not covered by LMA 5403.

As the endorsement only provides affirmative cover for non-malicious acts, shipowners should continue to consider whether to take out vessel-specific cyber insurance to protect them in the event of a cyber-attack[78]. As matters stand, LMA5403 can be considered as falling short of providing assureds with adequate cover in the event of such an attack.

7 Insurance of Objects: Clause 10-1 and Cl. 18-2

Another issue which needs to be addressed is the extent to which objects onboard a vessel are insured under a typical H&M policy. A review is therefore undertaken to address whether H&M coverage is provided in respect of damage to vessels stemming from cyber-attacks on software. To analyse the position, NP Cl. 10-1 and Cl. 18-2 are considered insofar as they relate to software aboard a vessel, together with an exclusion relating to blueprints, plans and specifications which are relevant to this review.

Generally, hull insurance pursuant to the NP provides cover for a vessel comprising of hull and machinery. Cl. 10-1 of the NP details the 'objects insured' under the NP. It confirms that the insurance covers:

a. the vessel,
b. equipment on board and spare parts for the vessel and its equipment, provided that the equipment or spare parts belong to the assured or have been borrowed, leased or purchased with a vendor's lien or similar encumbrance,
c. bunkers and lubricating oil on board[79]*.*

Specifically, Cl. 10-1 confirms that equipment on board is insured. The term 'equipment' is discussed in the next paragraph. The requirement of equipment to be located "on board" poses problems in instances where cyber-attacks are carried out on SCCs. Pursuant to the NP, cyber-attacks on for example, SCCs are not covered under a H&M policy as these policies only re-

[78] Ibid.
[79] NP Cl. 10-1.

spond to physical losses triggered by the covered elements above. These limitations are important in circumstances where many of the cyber-attacks are likely to occur on SCCs due to their management and control of autonomous vessels at sea. It is therefore important to make this distinction at the outset, as any such cyber-attacks would only be covered under cyber risk insurance as opposed to under H&M or P&I policies.

Cl. 10-1(b) is clear that insurance coverage is provided for "equipment on board". Looking at the natural wording of "equipment on board" one can conclude that it refers to any software installed on the vessel, that is used for navigational or operational purposes. For example, it can include software controlling navigation and communication systems. The Commentary to the NP provides further assistance, confirming what is meant by the term "equipment":

"…collective term for loose objects that accompany the ***vessel*** *in its trade, but which cannot be deemed to be part of it, e.g. radio and radar equipment,* ***digital, navigation and communication equipment,*** *search lights, loose shifting beams, furniture and other fixtures and fittings. The prerequisite for covering equipment and spare parts under the* ***vessel's*** *hull insurance is nevertheless that they are normally on board, cf. the term "on board", which indicates that the object in question shall be on board for an indefinite or prolonged period of time."*[80]

The terms bolded in the above extract from the NP Commentary highlight amendments made in the 2023 NP. It stresses that the term "equipment" includes more than radio and radar like digital equipment. This is a welcomed amendment, given the increased reliance on digital communication equipment utilised in autonomous vessels.

However, despite this Commentary, it is unclear whether H&M insurance provides cover for damage to vessels that stemmed from cyber-attacks on technological software. For example, autonomous vessels utilise AI, as has been discussed above. AI is programmed in such a way that the more data is processed from each voyage undertaken by the vessel, the more it learns and the more advanced in becomes. This results in each individual vessel utilising unique AI experiences, which cannot be directly replicated in other vessels[81]. The question which therefore arises in the first instance is whether AI software is covered under the NP.

The definition of "equipment" in the NP Commentary presumes the presence of something physical, by using words such as *"…and other fixtures and fittings",* as well as *"communication*

[80] NP Commentary Cl. 10-1.

[81] Camilla Sogaaard Hudson, "Legal Challenges in Unmanned Shipping", Copenhagen Business School, 17 May 2021: 25.

equipment"[82]. However, as has been discussed in the context of AI software, it is unclear to what extent "equipment" includes programs, data and related information.

By way of an example, ECDIS, the vessel's navigation system, may be seen as integrated into the hardware of the vessel and therefore falling within the NP definition. However, it has been discussed that AI is a software which is unique to each vessel, given its abilities to assimilate new information and adapt accordingly. If one looks at the original purpose of H&M insurance, which is to restore the vessel to its original state, it is arguably impossible for insurers to fulfil this duty when it comes to AI software. While on the reading of the NP and the Commentary, it has been stated that to the extent software forms part of the hardware it is covered under the NP[83], it remains unclear to what extent insurers could re-instate the assured under the H&M policy in the event of a cyber-attack on AI software, due to its unique features i.e. the knowledge the AI software assimilated during voyages. Furthermore, AI software is not a "physical" object and without direct reference to software and programs, it is difficult to conclude with certainty that it would be covered under a H&M policy. It is possible to find guidance in Cl. 18-2, sub-clause 2(c) which provides an exclusion in respect of *"…blueprint, plans, specifications…",* things that are specific to each vessel. Arguably, AI software may fall under this category in the future as it is part of a vessel which cannot simply be restored to its original form. Currently, insurers abilities to provide effective cover for such software may be practically impossible, and even if it was offered, could be restricted by re-insurers due to potentially large exposures associated with AI software. As matters stand, no such exclusion exists in the NP.

It conclusion, AI software itself is covered under the NP due to the definition of "equipment" which has been addressed above, but the extent to which the knowledge accumulated by AI software is covered, and indeed, whether it is possible for it to be covered, remains to be seen.

8 H&M Insurance Conditions in England and the War Risk Exclusion

In this chapter, a comparison will be made between the NP and the Institute Time Clauses Hulls 1983 ("**ITCH**"), which are subject to English law and jurisdiction, insofar as it relates to cyber coverage. As England, in particular London, is considered as a leader for the marine insurance market, it is important to understand how it caters for cyber risks in its H&M policies, as based on ITCH.

[82] NP Commentary Cl. 10-1.

[83] Wilhelmsen, Trine-Lise and Bull, Hans Jacob, "Hull insurance of autonomous ships according to Nordic Law. What are the challenges?", in *Autonomous Ships and the Law* (Routledge, 2021): 178.

Due to the 'all-perils' principle adopted by the NP, a cyber-attack is, in principle, covered under the NP (unless excluded by use of Cl. 380 or LMA1504). Under the ITCH, cover is provided for 'named perils' in the Policy. This raises the question of how, and if at all, do the ITCH provide cover for cyber-attacks, as compared with the NP?

The ITCH wording does not mention cyber risks, and similarly to the NP, the ITCH cover physical loss or damage to the insured vessel. The named perils in the ITCH (Cl. 6 and 7) are not exhaustive, but make clear that for the policy to be triggered the perils which are insured against must at least be: *"consequent on or incidental to the navigation of the sea"* as prescribed in s. 3 (2)[84]. Furthermore, ITCH's concluding words: *"and other perils, either of the like kind or which may be designated by the policy"* confirm that the Policy is restricted to perils related to the navigation of the sea[85]. Notably, the wording "navigation of the sea" does not include a reference to navigation by use of electronic charts and remote control. It can be presumed that at the time the clause was drafted only manual charts were used and there was no need to reflect modern language covering electronic charts. Insurers can, as has been mentioned, include their own wording in insurance contracts and are now likely to refer to the use of electronic charts by way of a separate clause. However, despite this analysis, there remains no mention of cyber-attacks and as such one must conclude that due to the "named perils" approach, cyber threats are not covered.

The position, however, is arguably clearer under the ITCH, due to its "named perils" approach, which omits any reference to cyber-risks. Whereas with the NP, one is left to assume that cyber-risks are covered, as they are not specifically excluded, due to the "all perils" principle.

8.1 The War Risk Exclusion: Nordics and UK

8.1.1 War Risk Insurance: Nordics

War H&M coverage under the NP is based on the "named perils" principle such that only the perils specified in the NP are covered, contrary to NP 2-8 which is based on the "all risk" principle, as has been discussed above. It was concluded in this thesis that unless cyber-risk was specifically excluded under Cl. 2-8 of the NP, it was covered. However, one of the exclusions referred to Cl. 2-9 which are the perils covered by an insurance against war perils. This chapter will therefore assess to what extent, if at all, cyber risks are included in the war insurance, as laid out in Cl. 2-9.

[84] Song, Meixian, "Moving forward by looking back. Insuring autonomous vessels under English hull and machinery cover and law" in *Autonomous Ships and the Law* (Routledge, 2021): 225.

[85] Ibid.

Cl. 2-9 of the NP regulates insurance against war risk, covering the following "named perils":

a. *war or war-like conditions, including civil war or the use of arms or other implements of war in the course of military exercises in peacetime or in guarding against infringements of neutrality,*
b. *capture at sea, confiscation, expropriation and other similar interventions by a foreign State power, provided any such intervention is made for the furtherance of an overriding national or supranational political objective[…]*
c. *riots, sabotage, acts of terrorism or other social, religious or politically motivated use of violence or threats of the use of violence, strikes or lockouts,*
d. *piracy and mutiny,*
e. *measures taken by a State power to avert or limit damage, provided that the risk of such damage is caused by a peril referred to in sub-clause 1 (a) - (d)*[86]

The insurance does not cover the following:

f. *involvency […]*
g. *perils covered by the RACE II Clause […]*
h. *requisition by State power.* [87]

It is clear from this exhaustive list, that cyber-attack is not included and without the Cl. 380 buy-back, as has been discussed above, no cover for cyber-attacks is provided. Nevertheless, the named perils under Cl. 2.9 that relate to 'war', 'capture at sea', 'sabotage' or 'acts of terrorism', may arise through cyber-attacks resulting in a cyber-attack being a peril or forming part of the losses that are covered under insurance policies The examples of possible cyber-attacks which were explored above include examples of potential cyber-attacks due to war and acts of terrorism. One such example may relate to a terrorist group taking control of an autonomous vessel in order to cause a collision with another vessel, resulting in vast damage to the vessel facing the attack[88]. Such a situation is likely to be afforded cover under the war insurance as the act of terrorism is a covered peril under the policy, making the cyber-attack part of the peril. The wording used in Cl. 2-9 therefore makes it is possible to envisage how a cyber-attack could be covered.

[86] NP Cl. 2-9.
[87] Ibid.
[88] Master Thesis, "Coverage of Cyber Risks in the Norwegian Insurance Market", University of Oslo, 2022: 26.

8.1.2 War Risk Insurance: England

As referred to above, the ITCH covers named perils listed in Clause 6 and 7. While Piracy is included as a marine peril, it is usually excluded from insurance policies and included in the war risk policy. Clause 23.1 to 23.3 sets out war perils that are excluded, which includes violent theft and piracy. However, most of the excluded perils are commonly transferred to the assured's war policy, by way of an exclusion in the H&M policy, known as JH2005/046, and an extension relating to the war policy, being JH2005/002[89].

The perils which are excluded under Cl. 23.1 – 23.3 are covered by NP Cl. 2-9, as referred to above. There is therefore little difference between the operation of H&M policies in the England and Nordics.

9 Management of Cyber-Attacks

Given the increasing risk of cyber-attacks on autonomous vessels it is important to identify how shipowners, together with insurers, can manage the risk of cyber-attacks from materialising. This chapter will firstly focus on what mandatory measures are put in place on the shipowners for the prevention of cyber-attacks by the IMO. Furthermore, this chapter will explore the efforts undertaken by insurers to assist the assureds (shipowners) with the management of cyber-risks, as well as various duties placed on them as assureds by reference to the Nordic and English law. Lastly, shipowners own efforts will be explored, in order to assess what they can do themselves in order to prevent cyber-attacks.

9.1 Insurers' Protection

Cyber-attacks in shipping undoubtedly pose new challenges for insurers. As has been explored above, the damage which cyber-attacks can cause is yet unknown but can amount to a total loss of the vessel. As such, exclusion clauses Cl. 380 and LMA5402 which have been discussed at length above, have been established to protect insurers from potentially large exposures.

However, in addition to such exclusions, insurers in the Nordics are protected by way of 'assureds duties' that are imposed on shipowners at the time of entering into an insurance contract, and in the contract itself, by reference to the NP. In the UK, in addition to duties imposed by

[89] CEFOR, "Institute Time Clauses (Hulls) (ITCH) vs Nordic Plan", accessed 5 April 2023 https://cefor.no/globalassets/documents/clauses/comparison/comparison-itch-vs-nordic-plan.pdf page 34.

ITCH, insurers are afforded protection by way of 'warranties' and duties that are found in Sections 33-41 of the Marine Insurance Act 1906 ("**MIA**"). These are explored in turn below, with an effort to make a direct comparison between the two jurisdictions.

9.1.1 Assureds duties: NP

The NP imposes a number of duties on the assureds, with which the assured must comply with before and throughout the duration of the insurance contract.

Duty of Disclosure

Firstly, the duty of disclosure in Cl. 3-1 of the NP states that:

> *"The person effecting the insurance shall, at the time the contract is concluded, make full and correct disclosure of all circumstances that are material to the insurer when deciding whether and on what conditions it is prepared to accept the insurance.*
>
> *If the person effecting the insurance subsequently becomes aware that it has given incorrect or incomplete information regarding the risk, it shall without undue delay notify the insurer."*

This clause confirms that the assured has an obligation to disclose all circumstances that are 'material' to the insurer in its assessment of the risk being insured, before it accepts the risk. The reference to 'material' relates to information which could influence insurers' decision to accept, or reject, a particular risk. It also assists insurers with determining the terms on which a risk will be placed. The fact that the assured is looking to insure an autonomous vessel with a remote crew based at a SCC is likely to be a 'material' factor which should be disclosed. The Commentary to the NP confirms that the NP's approach is around the active duty to disclose information and *"the person effecting the insurance is usually a professional and will, accordingly, have knowledge about what kind of information the insurer requires".*[90] This is particularly important in respect of factors that may increase the risk of loss, or damage, to the vessel and will therefore form part of insurers' assessment of the risk.

It must be noted that the general condition in Cl. 3-14 of the NP provides that a vessel must be classed in a classification society which has been approved by an insurer. It has been commented that the duty contained in Cl. 3-1 of the NP should therefore be read in tandem with Cl.

[90] NP Commentary Cl. 3-1.

3-14 of the NP and presumed that a vessel which has been approved by a classification society falls within the generally accepted standards[91].

A classification society has the task of verifying, amongst other things, the vessel's strength, reliability and functions of systems in order to maintain essential services on board[92]. Once a vessel complies with classification rules, the shipowner may apply for a certificate of classification which attests that the vessel is in compliance with the classification society rules[93]. However, it has been noted by the International Association of Classification Societies that classification societies are not: *"guarantors of safety of life or property at sea or the seaworthiness of a vessel because the Classification Society has no control over how a vessel is manned, operated and maintained between the periodical surveys which it conducts"*[94]. This is an important distinction as it highlights that insurers, despite reviewing a classification certificate of a particular vessel, should still carry out their own analysis of risks involved in autonomous and crewless vessels. In any circumstance, the insurer is likely to know, once it obtains the particulars of the vessel, that the vessel to be insured in autonomous and crewless, meaning that the insurer is unlikely to invoke a breach of duty disclosure. In the event that an insurer chooses to invoke a breach of duty disclosure, it is important to take note of NP Cl. 3-5 which states that:

> *"The insurer may not plead that incorrect or incomplete information has been given if, at the time when the information should have been given,* ***it*** *knew or ought to have known of the matter".*

NP 3-5 confirms that where the insurer 'knew or ought to have known of the matter', it cannot argue that the person effecting insurance failed to provide all required information. The Commentary to the NP confirms that NP Cl. 3-5 imposes a duty on the insurer to show due diligence with respect to the information received[95] and where the person effecting insurance *"...gives certain information about which the insurer might wish to have greater detail, then he must request it".*

Due to the requirements set out in NP Cl. 3-14, insurers are provided with the required information about the vessel by virtue of the vessel's classification. As such, even if the assured does not disclose all factors relevant to the manning and operating of the vessel, insurers will often

---

[91] Wilhelmsen, Trine-Lise and Bull, Hans Jacob, "Hull insurance of autonomous ships according to Nordic Law": 186.

[92] International Association of Classification Societies, "Classification societies – what, why and how?", last accessed 26 May 2023, https://iacs.org.uk/media/8871/classification-what-why-how.pdf.

[93] Ibid.

[94] Ibid.

[95] NP Commentary Cl. 3-5.

be aware of the specific particulars of the vessel and where they are not aware they should request further information.

Of course, NP Cl. 3-1 is not made redundant by the operation of NP Cl. 3-14. For example, if the shipowner is aware of specific, perhaps novel, technologies that it seeks to utilise onboard a vessel and such technology is prone to cyber-attacks or is easily hacked into it should be disclosed to insurers at time of effecting the insurance. Such facts are likely to be classed as *"…material to the insurer when deciding whether and on what conditions **it** is prepared to accept the insurance.*"[96].

Safety Regulations

Another notable rule, relevant for the purposes of this thesis is NP Cl. 3-22 concerning safety regulations:

> *"A safety regulation is a rule concerning measures for the prevention of loss, issued by public authorities, stipulated in the insurance contract, prescribed by the insurer pursuant to the insurance contract, or issued by the classification society*."

Cl. 3-22 stipulates that the assured must comply with safety regulations. Any breach of a safety regulation can mean that the insurer is not liable for the loss should there be a causal link between the breach of safety regulation and the casualty, and the breach is culpable[97]. The assured has to abide by measures which are issued by public authorities or those issued by the classification society. Taking firstly the requirements issued by 'public authorities', the NP Commentary confirms that public authorities are made up of *"public authorities in all states providing the rule is binding for the assured and consequently a duty the assured must adhere to"*, which includes the Flag State and its national laws[98]. In addition to the flag states, the NP Commentary states that the assured *"…has to abide by the regulations it is bound by, due to the location of its vessel"*[99].

Notably, according to the NP the International Safety Management that has been adopted by the IMO classifies as a safety regulation with which the assured has to comply:

---

[96] NP Cl. 3-1.

[97] Sandell, Peter and Roos, Ninna, "Risk Management, Marine Insurance and Charterparties – Formulating the Research needs for autonomous vessels in maritime universities", *University of Applied Sciences, Rauma, Suojantie 2 26101*, Finland [no page numbers available].

[98] NP Commentary Cl 3-22.

[99] Ibid.

"When establishing the Safety Management System that is necessary to fulfil the assured's obligation to comply with the International Safety Management Code as adopted by IMO…"[100].

The IMO has a strong standing in the sphere of maritime cyber-security and any recommendations and guidance issued by the IMO, while not binding itself, is highly regarded in the industry. Firstly, the IMO is referred to in the United Nations Convention on the Law of the Sea ("**UNCLOS**"), which is binding[101] on shipowners and imposes a duty on shipowners to follow guidelines that were established by *"competent international organisations"*[102]. Secondly, the IMO refers to the International Security Management Code ("**ISM Code**") with which shipowners must comply. The ISM Code sets out the international standards for the safe management and operation of ships and for pollution prevention[103].

The IMO, responding to the increasing risk of cyber-attacks occurring, in its 98th meeting, adopted a resolution (MSC 428 (98)) (the "**IMO Resolution**") on maritime cyber risk management in safety management systems *"…having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities"*[104]. The outcome of the IMO Resolution is the requirement for companies to implement approved safety management systems that take into account cyber risk management in accordance with the IMO Resolution and requirements of the ISM Code[105]. The IMO confirmed that companies after 1 January 2021 and no later than the first annual verification of their Document of Compliance have to be able to show that cyber-security is an integral part of their safety management systems[106]. The Document of Compliance is a certificate that is issued to a shipping company, once it compliance with the ISM Code.

Following the IMO Resolution, the IMO published "Guidelines on maritime cyber risk management" (the "**Cyber Risk Management Guidelines**"). The Cyber Risk Management Guidelines were implemented due to the significant weaknesses which were identified in the technol-

---

[100] NP Cl. 3-22.

[101] Hopcraft, Rory and Martin, M. Keith, "Effective maritime cybersecurity regulation – the case for a cyber code" *Journal of the Indian Ocean Region 354 (2018) 14(3)*: 356 .

[102] UNCLOS, Art. 217.

[103] The International Safety Management Code, https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx.

[104] IMO Guidelines on Maritime Cyber Risk Management: 1.

[105] DNV, "Cyber security to be covered in SMS from 1 January 2021 – are you prepared?", last modified 2 June 2020 https://www.dnv.com/news/cyber-security-to-be-covered-in-sms-from-1-january-2021-are-you-prepared--176620.

[106] Ibid.

ogies utilised by vessels at sea, including GPS, AIS and ECDIS, all of which have been addressed in this thesis[107]. IMO confirmed that the goal of maritime cyber risk management is to: *"support safe and secure shipping, which is operationally resilient to cyber risks"*[108]. The Cyber Risk Management Guidelines focused on action that can be taken to support effective cyber risk management, including: (i) identifying systems that if disrupted, could pose a risk; (ii) implementation of risk control processes; (iii) development of systems to detect a cyber incident in a timely manner; (iv) set up a plan for restoration of systems which were halted because of a cyber-attack; (v) recovery and restoration of systems[109].

The IMO Resolution and the Cyber Risk Management Guidelines came at a time when autonomous shipping has started to become a reality, and indeed with that, an increase in cyber-threats. Given the weaknesses in systems used by vessels worldwide and the fact that they can exploited by cyber-attackers for their own gain, such guidelines serve as an important starting point in the prevention of cyber-attacks. However, it could be argued that the Cyber Risk Management Guidelines are just that, a starting point. Cyber-security is such a large topic amongst those in the maritime industry, impacting a number of complex systems which arguably require more than guidelines to effectively prevent cyber-attacks from occurring.

Nevertheless, the communication from IMO confirms that cyber-security is not something which shipowners can simply ignore. It forces shipowners to think about cyber-security as a real risk, which is something that many have not considered before.

Furthermore and related to shipowners' requirement to comply with safety protocols, NP Cl. 2-12 states:

> *"The assured has the burden of proving that **it** has suffered a loss of the kind covered by the insurance and of proving the extent of the loss. The insurer has the burden of proving that the loss has been caused by a peril that is not covered by the insurance, unless other provisions of the Plan provide to the contrary."*[110]

The above Clause relating to burden of proof confirms that insurers liability will not trigger under an insurance policy covering a cyber risk, where the shipowner did not incorporate and/or follow cyber related safety protocols. This corresponds to the "all risk" principle under the NP

[107] Zhu, Ling and Xing, Richard "A pioneering study of third-party liability insurance for unmanned/autonomous commercial ships", *Journal of Business Law, J.B.L 2019*: 446.

[108] IMO Guidelines on Maritime Cyber Risk Management: 3.2.

[109] Ibid: 3.5

[110] NP Cl. 2-11

which confirms that any casualty is covered, unless excluded, and is hereby located in NP Chapter 3 resulting in insurers having the burden of proof.

While the loss suffered by the shipowners would have to arise out of the failure to follow cyber security guidelines, this provision remains significant as shipowners may take extra caution in implementing, and complying with, the cyber-security guidelines. This discussion is relevant when considering the duties placed on the assured by insurers.

Despite the fact that the IMO is not binding on shipowners, it nevertheless remains relevant for shipowners due to references in UNCLOS and reference to the ISM Code. Furthermore, it has been commented by Norwegian academics that while the IMO is not directly binding, it is implemented in the Nordic legislation through the Nordic Ship Safety Acts, such as the Norwegian Ship Safety Act at Section 6[111]. The NP Commentary states that *"…a class-related requirement will always have the status of safety regulation, as will requirements primarily aimed at preventing oil spills; e.g. marine pollution rules."*[112].

The result of the Cl. 3-22 requirement is that the assured will not be able to claim under its insurance policy if a loss to the autonomous vessel arose out of a breach of the safety regulations. These provisions exist to provide insurers with baseline protection i.e. a shipowner cannot simply take out an insurance policy and carry on with its business in a manner which breaches internationally accepted standards for safety. It serves as an important safeguard for insurers, encouraging the assureds to maintain high standards of safety and maintenance in order to reduce losses at sea, as well as preventable accidents. It has also been commented that classification societies standards for the software that is being utilised on board will also be crucial for insurers' risk assessment and will form part of important sources of safety regulations[113].

Pursuant to Cl. 3-22, a safety regulation can also be "…*stipulated in the insurance contract"*[114]. Insurers are therefore free to set out additional requirements in the insurance contract itself. For example, given the advances in technology in autonomous vessels and the existence of SCC instead of an onboard crew, insurers may consider the existing regulations to be insufficient and wish to cater specifically for the increased risks in autonomous vessels. For example, it may result in a requirement relating to mandatory training of staff based in SCC relating to cyber-risks and remote crisis management.

---

[111] Wilhelmsen, Trine-Lise and Bull, Hans Jacob, "Hull insurance of autonomous ships according to Nordic Law": 187.

[112] NP Commentary Cl. 3-22.

113 Sandell, Peter "Risk Management, Marine Insurance and Charterparties".

[114] NP Cl. 3-22.

Insurer Guidance

While not specifically a binding assured duty contained in the NP, insurers themselves have started to issue guidance, case studies and training for the assured to prevent cyber-attacks onboard vessels. Insurers are more than aware of the potentially vast risks that cyber-attacks pose to vessels and have therefore sought to ensure that shipowners adequately protect themselves.

In response to the growing cyber concerns, insurers may now require safety and cyber-security measures to be implemented before a policy for an autonomous vessel is issued. The measures can include regular cyber risk assessment, network security protocols and crew training programs based in SCC. Various recommendations have been issued in response to the IMO Resolution, which, as has been detailed above, requires shipowners to incorporate cyber risk into ships' management systems.

By way of an example, Gard has issued recommendations relating to cyber risks, intended to protect *"...the confidentiality, integrity and accessibility of both IT and OT systems through measures covering processes, technology and most importantly people"*[115].

In addition to prevention measures, insurers may also stipulate that they require any cyber-related accidents to be reported promptly, to mitigate further damages and losses.

9.1.2 Assured's Duties: England

By way of comparison to the Nordic position, the UK marine insurance system is based on the **MIA**, and **IA**, which has been heavily influenced by case law. Like the NP, MIA seeks to provide protection to insurers, by imposing various guarantees on the assureds. The MIA does this by way of 'warranties', set out in Sections 33-41 of the MIA. Warranties relate to statements and/or promises made by the assured to an insurer, that certain conditions will be complied with throughout the life of an insurance policy. These are fundamental in English insurance contracts and a breach of a warranty may result in the insured being released from all liability under the policy, regardless of whether the breach by the assured resulted in loss or not.

In addition to warranties, there are a number of duties which are imposed on the assureds, similar to those contained in the NP, such as the fair presentation of risk duty, explained below. Some of the assureds duties contained in the MIA are similar to those contained in the NP,

[115] Gard, "Cyber security", last modified 12 January 2021, https://www.gard.no/web/topics/article/21025160/cyber-security.

whereas others set out duties which are not present in the NP. Below is a summary of some of the assureds duties which are intended to serve as an example comparison to the position in the Nordic insurance market. The below is not intended to be a comprehensive review of the complex duties by which the assureds are bound in the English insurance market, but it is merely set out for comparison purposes.

Fair Presentation of the Risk

The duty of disclosure in NP Cl. 3-1 is akin to the requirement of 'duty of fair presentation of the risk' set out in Section 14 of the **IA**[116]. Section 14 requires the assured to disclose relevant material facts to the insurer. This includes every material circumstances that the assured knows or ought to know, or to provide sufficient information to put a prudent insurers on notice that it should make further inquiries[117]. As mentioned above, due to the increase in cyber-threats it is vital for shipowners to disclose all information relevant to its cyber prevention measures and related management systems.

Seaworthiness

The concept of seaworthiness is an implied warranty at the commencement of a voyage[118]. MIA has a general rule which states that a vessel is seaworthy when it is reasonably fit to encounter the ordinary perils of the seas[119]. Under the English legal system, shipowners have a duty to comply with international guidelines, together with a duty to ensure that the vessel is seaworthy. In comparison to the NP, there is no concept of 'safety regulations' under the English system, which is similar to the one described above. Furthermore, since 2007, under the NP, there is no longer a requirement to ensure that a vessel is made seaworthy by the shipowner[120]. The requirement of seaworthiness under the NP was abolished in 2007 as it was considered that the rules concerning safety regulations were similar to the 'seaworthiness' concept[121].

Under English law, however, an assured has a duty to exercise due diligence to ensure that their vessel complies with the requirement of seaworthiness. For example, in the English case of

[116] Insurance Act 2015, s.14.
[117] Ibid.
[118] MIA s.39(1).
[119] MIA s.39(4).
[120] Sandell, Peter "Risk Management, Marine Insurance and Charterparties".
[121] Ibid.

Papera v Hyundai[122], it was ruled that crew training and competence was essential to the seaworthiness of a vessel[123]. It has been discussed that training of crew is an important safety aspect when it comes to cyber-attacks, as humans continue to be the 'weakest links' when it comes to cyber safety. Applying this principle to autonomous vessels, should shipowners fail to train operators of the SCC, the vessel, subject to presence of causation, could be rendered to be unseaworthy.

Privity

Furthermore, the concept of 'privity' is important when talking of seaworthiness. 'Privity' is important in shipping where time charters are utilised, as it provides protection to the insurer by placing the liability on the shipowner in the event a vessel is unseaworthy at the commencement of its voyage, as set out in Section 39(5) of MIA:

> *"In a time policy there is no implied warranty that the ship shall be seaworthy at any stage of the adventure, but where, with the privity of the assured, the ship is sent to sea in an unseaworthy state, the insurer is not liable for any loss attributable to unseaworthiness."*

The case of *The Gloria*[124] confirms that if the shipowner deliberately fails to examine the vessel as it does not want to become alert to potential problems, then the shipowner will be privy to the vessel commencing its journey in an unworthy state[125]. Paragraph 58 of The Gloria is clear in this regard:

> *"I think that if it were shown that an owner had reason to believe that his ship was in fact unseaworthy, and deliberately refrained from an examination which would have turned his belief into knowledge, he might properly be held privy to the unseaworthiness of his ship. But the mere omission to take precautions against the possibility of the ship being unseaworthy cannot, I think, make the owner privy to any unseaworthiness which such precaution might have disclosed."*

---

[122] Papera Traders Co Ltd v Hyundai Merchant Marine Co Ltd ("The Eurasian Dream") (No.1) [2002] EWHC 118 (Comm): [150].

[123] Jessica Ann Andreassen, "Protecting shipowners' interests: an analysis of cyber risk regulation in public international law and marine insurance contracts, and how legal reform can mitigate against future risk", University of Southampton, 2022: 32.

[124] The Gloria (1935) 54 LILR 35: [58].

[125] Jessica Ann Andreassen, "Protecting shipowners' interests": 29.

The Gloria judgment has since been affirmed in *The Star Sea*[126] judgment. These are important considerations when reviewing autonomous vessels and cyber risks, as it demonstrates that shipowner duties may go beyond what has previously been classed as sufficient. For example, shipowners may not have traditionally placed much value on training of crew regarding cyber security. However, such shortcomings may prove costly to shipowners should a cyber-attack materialise as insurers under English law may have the possibility to utilise the concept of 'seaworthiness' to exclude its liability. The same can be applied in respect of the 'safety regulations' requirement under NP Cl. 3-22.

Arguably, in the context of autonomous vessels and cyber risk management, the concept of seaworthiness is more difficult to understand and comply with. Under English law, the existing case law detailing what it means for a vessel to be unseaworthy relates to manned vessels only, lacking case law specific to autonomous vessels. As such, should a dispute arise regarding the seaworthiness of an autonomous vessel that has not been previously considered, it would take some time for the Courts to develop new laws and guidance[127].

In this instance, the system employed under the NP relating to the safety regulations can be seen as more beneficial for both, the assured and insurers, as it provides more certainty, particularly where shipowners have good maintenance systems and clearly follow the safety guidance. The concept of unseaworthiness however, raises a number of uncertainties even if safety regulations are followed. As such, it can be concluded by way of comparison that the NP rules will be easier to adjust to autonomous vessels than the system of common law rules of law found in English law[128]. Nevertheless, both of the concepts exist to ensure that the shipowner secures its vessel in order to prevent any accidents while at sea and comply with the industry standards.

9.1.3 Premium

A temporary solution for insurers, insofar as it relates to insuring cyber risks and the sophisticated technology in autonomous vessels, would be to impose higher premiums due to the unknown risks. However, this solution is not a sustainable, long term solution for insurers or shipowners. The scope of cover and subjective duties of the assureds, of the type explained above, as well as their applicability to autonomous vessels and the risk of cyber-attacks remains uncertain. Currently, the management of such risks will, and is, being dealt with on an individual,

[126] Manifest Shipping Company Limited v Uni-Polaris Shipping Company Limited and Others ("The Star Sea") [2001] UKHL 1: [36].

[127] Sandell, Peter "Risk Management, Marine Insurance and Charterparties".

[128] Ibid.

contractual basis and ultimately the cost of insurance will depend on a variety of factors including levels of risk as well as safety and security measures in place.

Relatedly, the extent to which insurers are prepared to offer protection for unknown cyber risks is also limited by their own re-insurance programmes, as is detailed below.

9.1.4 Re-insurance

Re-insurance involves an insurer transferring some, or all, of its risk to another insurer (the re-insurer). By way of a practical example, a H&M insurer may wish to apportion some of the risk with another insurer, the re-insurance, in the event of damage of the vessel it had insured. As H&M insurance is often for large risks covering the whole vessel, it is the case that the hull risk insurance will be dependent on re-insurance[129]. It is for this reason that re-insurers themselves will want to control the type of risks covered by insurers, who have the direct contract with the shipowner.

A notable example of re-insurance influence is the RACE II Clause (as has been discussed above) and the Cl. 380/LMA5402 exclusion. While these clauses do not directly feature in the NP, they are often inserted in insurance policies as a special clause[130].

Insurers are therefore not able to simply provide cover for autonomous, crewless vessels as they see fit. They are bound by the requirements imposed on them by re-insurers and before deciding to accept potentially large risks they will want to ensure that re-insurers are prepared to cover the direct insurer in the event of a high loss under the insurance contract.

10 Cyber Insurance for Shipowners: A New Market?

As has been discussed in this thesis, gaps in H&M insurance exist, particularly when it comes to cyber-risks and the Cl. 380/LMA 5402 exclusion. This section of the thesis intends to explore the extent to which there is a need for separate cyber coverage in respect of autonomous vessels and to what extent it is available and/or accessible to the assureds.

Cyber-attacks are an on-going issue in the industry. Indeed, every day a number of cyber-attacks are attempted in the shipping industry. It is thus not a question of if, but when, a cyber-attack will occur. Due to the increasing reliance on technology and the Cl. 380 exclusion, shipowners

[129] Wilhelmsen, Trine-Lise and Bull, Hans Jacob, "Hull insurance of autonomous ships according to Nordic Law": 179.

[130] Ibid: 180.

should be more aware and seriously consider the uptake of the cyber-risk insurance add on or take out separate cyber-insurance policies. For example, AXA XL provides cyber cover in relation to third party liability, including data breach security and privacy liability as well as media internet communications and first party losses, including business interruption, loss of electronic assets and data restoration[131].

Further to the IMO Resolution, it is undisputable that cyber-risk assessment is now part of general risk assessment for purposes of insurance. The IMO Resolution, together with the assureds' duties which have been discussed above, make it clear that cyber issues are an integral part of the risk posed to vessels. A real consideration should therefore be given by shipowners on whether to invest in cyber insurance, particularly in respect of autonomous vessels that utilise advanced technologies. Of course, marine cyber insurance is not compulsory, unlike, for example pollution damage, and remains optional despite the fact that a cyber-attack could result in damage to the vessel at sea. Any such insurance would therefore require an extra push from the maritime market to make it an attractive product for shipowners.

However, as has been discussed, insurers main concern is around the potential exposures related to a cyber-attack. Furthermore, due to limited data related to cyber-attacks, it is difficult for insurers to quantify the potential risks. This factor makes it difficult to insurers to analyse the rate of the premium in respect of cyber risks and may limit reinsurers capacity and/or appetite to take such risks[132].

From the shipowners' perspective, the cyber insurance market may be confusing. Not only do insurers, as standard, include the Cl. 380/LMA5402 cyber exclusion in H&M policies creating gaps in cover but the cyber policies which do exist in the market are specific to different types of losses[133]. The various cyber insurance policies which exist provide products relating to either business interruption or cover for loss of data, but rarely the type of comprehensive cover sought after by shipowners. The general cyber insurance market therefore lacks the expertise and the knowledge that is necessary to cater for shipowners and the type of technologies they employ, as well as the way its businesses function at sea.

In response, insurers have started to cater cyber insurance that is specific to the maritime market. For example, Willis Tower Watson has began to offer 'CyNav', which is a cyber insurance

---

[131] AXAXL, "Cyber Insurance", last accessed 25 May 2023, https://axaxl.com/insurance/products/cyber-insurance-international.

[132] Soyer, B, "Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems" in Mukherjee, P.K., Mejia, M.Q., Xu, J. (eds) *Maritime Law in Motion. WMU Studies in Maritime Affairs, Vol. 8, Springer 2020*: 631.

[133] Ibid.

solution for shipowners catering for the increased reliance on technology for all aspects of vessel's operation and shore side activities[134]. CyNav offers cover for loss of income due to business interruption, crisis management expenses, hull and machinery damage, loss of hire due to hull and machinery damage and due to vessel detainment. Such cyber cover is important in an insurance market where H&M policies include the Cl. 380 cyber exclusion and typical cyber policies provide no cover for financial losses when normal business operations are interrupted, as a consequence of property damage caused by a cyber-attack[135].

Even if such products exist, shipowners may not be willing to spend the extra costs on cyber-cover, where they are already paying high premiums for 'mandatory' insurances, such as P&I and H&M. Indeed, it has been reported that cyber insurance prices have surged in recent years with insurers passing the costs of ransomware claims onto the shipowners[136]. Such increases will make cyber policies less attractive to shipowners and coupled with a lack of understanding about the potential reach of cyber-attacks, are likely to result in shipowners opting to take risks they would not otherwise have. Ultimately, until cyber policies become more attractive and shipowners realise their importance they are unlikely to incur the extra costs.

11 Conclusion

The purpose of this thesis was to explore cyber risks in autonomous vessels, coverage of the same in the marine hull insurance market in Nordics and England, ending with a review of safety measurements. As has been discussed, technology in autonomous vessels has become more advanced and as shipowners move towards the use of shore based crews, the more real the prospect of cyber-attacks becomes. Indeed, due to the advances in technology and the increasing sophistication of cyber-hackers, shipowners need to be aware of increasing cyber-risks associated with autonomous vessels, which are arguably easier to exploit than traditional, manned vessels.

The insurance market in the Nordics and the UK currently makes use of the industry standard cyber exclusion clauses. The result is that cyber risks are rarely covered in standard insurance

[134] Willis Tower Watson, "CyNav: Navigating shipowners' cyber security risks", last accessed 24 April 2023, https://www.wtwco.com/en-US/solutions/products/cynav-navigating-your-cyber-security-risks.

[135] Seatrade Maritime News, "New customised cyber insurance product for shipowners", last modified 28 April 2020, https://www.seatrade-maritime.com/finance-insurance/new-customised-cyber-insurance-product-shipowners.

[136] Financial Times, "Lloyd's of London defends cyber insurance exclusion for state backed attacks", last accessed 25 April 2023, https://www.ft.com/content/e865a3d1-5652-41aa-990a-bb5ad57288c6.

policies taken out by the assureds. While insurance cover is fact specific, and depends on circumstances, the exclusions currently utilised exclude a broad range of cyber-attacks and the consequential losses from policies.

It can therefore be concluded that while insuring of an autonomous vessel under H&M policies does not pose many problems, the lack of cyber cover fails to acknowledge the increasing threat of cyber-attacks. While H&M policy is seen as property insurance and therefore excludes cover for non-physical objects, cyber-attacks can nevertheless result in physical damage to the vessel.

It has been shown that cyber security has become an important part of shipowners operation of the vessel, particularly in light of mandatory regulations and safety requirements with which shipowners' must comply, such as the IMO Resolution. While cyber cover is scarce in the market, shipowners can take the matter in their own hands and ensure that certain programs and procedures are adhered to in order to prevent cyber risks. Insurers in tandem have also spent significant time in ensuring that shipowners have access to basic cyber training tools and remain protected, to a certain degree, by the imposition of assureds duties and warranties in insurance contracts.

In conclusion, while steps are being taken by the insurance market and shipowners to prepare for the potential losses caused by cyber-attacks, more is needed by way of guidance to assist operators of autonomous vessels. The insurance market needs to keep up with the technological advances and the increase in autonomous vessels in order to ensure adequate cover is provided in the event of a cyber-attack.

BIBLIOGRAPHY

Legal Sources

The Nordic Marine Insurance Plan of 2013, Version 2023, CEFOR https://www.nordicplan.org/the-plan/

Commentary to the Nordic Marine Insurance Plan of 2013, Version 2023, CEFOR https://www.nordicplan.org/commentary/.

Institute Cyber Attack Exclusion Clause, Cl. 380.

Marine Cyber Exclusion Clause, Lloyd's Market Association, LMA5402.

Marine Cyber Endorsement, Lloyd's Market Association, LMA5403.

International Maritime Organisation, Guidelines on Maritime Cyber Risk Management, MSC-FAL. 1/Circ.3 Annex, *Guidelines on Maritime Cyber Risk Management* (July 5, 2017), https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.

Resolution MSC.428(98) (adopted on 16 June 2017), "Maritime Cyber Risk Management in Safety Management Systems" https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

International Maritime Organisation, "Autonomous Ships: regulatory scoping exercise completed", last modified 25 May 2021, https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx

International Maritime Organisation, "IMO takes first steps to address autonomous ships", last modified 25 May 2018, https://www.imo.org/en/MediaCentre/PressBriefings/Pages/08-MSC-99-MASS-scoping.aspx

United Nations, Security Council, 5 March 2019 https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2019_171.pdf.

Lloyd's Market Bulletin, Ref Y5258 "Providing clarity for Lloyd's customers on coverage for cyber exposures", last modified on 4 July 2019 https://assets.lloyds.com/assets/y5258-

providing-clarity-for-lloyd-s-customers-on-coverage-for-cyber-exposures/1/Y5258%20-%20Providing%20clarity%20for%20Lloyd's%20customers%20on%20coverage%20for%20cyber%20exposures.pdf

CEFOR, "Institute Time Clauses (Hulls) (ITCH) vs Nordic Plan", accessed 5 April 2023 https://cefor.no/globalassets/documents/clauses/comparison/comparison-itch-vs-nordic-plan.pdf page 34.

UNCLOS, Article 217.

The International Safety Management Code, https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx.

Insurance Act 2015, Section 14.

Marine Insurance Act 1905 (First Schedule), Section 39.

Papera Traders Co Ltd v Hyundai Merchant Marine Co Ltd ("The Eurasian Dream") (No.1) [2002] EWHC 118 (Comm).

The Gloria (1935) 54 LILR 35.

Manifest Shipping Company Limited v Uni-Polaris Shipping Company Limited and Others ("The Star Sea") [2001] UKHL 1.

Journal Articles

Robert Veal and Henrik Ringbom, "Unmanned ships and the International Regulatory Framework": *Journal of International Maritime Law.* 2017, 23 (2).

Zăgan Remus, Raicu Gabriel, "Understanding of the cyber risk on board ship and ship stability" *Annals of "Dunarea de Jos" University of Galati*, (2019).

Kavallieratos Georgios, Sokratis Katsikas, Managing Cyber Security Risks of the Cyber-Enabled Ship, *Journal of Marine Science and Engineering*, 8, 768 (2020).

Glomsrud Jon Arne et al, Trustworthy versus Explainable AI in Autonomous Vessels, in *Proceedings of the International Seminar on Safety and Security of Autonomous Vessels (ISSAV) and European STAMP Workshop and Conference (ESWC)*, (Helsinki, 2019).

Martinez, P. Leo, Cyber Risks: Three Basic Structural Issues to Resolve, in *InsurTech: a Legal and Regulatory View*, (Springer, 2020).

Tam, Kimberley and Jones, Kevin, "Cyber Risk Assessment for Autonomous Ships", *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security),* (Glasgow, UK, 2018).

Ringbom, Henrik and Collin Flexi, Terminology and concepts, in *Autonomous Ships and the Law, 1st ed.* (Taylor and Francis, 2020).

Bolbot, Victor et al, A novel cyber-risk assessment method for ship systems, Safety Science 131 (2020).

MacFarlane, Rory, Cyber-risk in shipping and its management, in *Ship Operations, New Risks, Liabilities and Technologies in the Maritime Sector*, (Routledge, UK, 2021).

Soyer Baris, "Cyber-risk insurance – developing a new cover in the market", in *Ship Operations, New Risks, Liabilities and Technologies in the Maritime Sector* (Routledge, UK, 2021).

Wilhelmsen, Trine-Lise and Bull, Hans Jacob, "Hull insurance of autonomous ships according to Nordic Law. What are the challenges?", in *Autonomous Ships and the Law* (Routledge, 2021).

Song, Meixian, "Moving forward by looking back. Insuring autonomous vessels under English hull and machinery cover and law" in *Autonomous Ships and the Law* (Routledge, 2021).

Sandell, Peter and Roos, Ninna, "Risk Management, Marine Insurance and Charterparties – Formulating the Research needs for autonomous vessels in maritime universities", *University of Applied Sciences, Rauma, Suojantie 2 26101*, Finland.

Hopcraft, Rory and Martin, M. Keith 'Effective maritime cybersecurity regulation – the case for a cyber code' *Journal of the Indian Ocean Region 354 (2018) 14(3)*.

Zhu, Ling and Xing, Richard "A pioneering study of third-party liability insurance for unmanned/autonomous commercial ships", *Journal of Business Law, J.B.L 2019*.

Soyer, B, "Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems" in Mukherjee, P.K., Mejia, M.Q., Xu, J. (eds) *Maritime Law in Motion*. *WMU Studies in Maritime Affairs, Vol. 8, Springer 2020*.

Books

Pierpaolo Marano, Kyriaki Noussia, *InsurTech: a Legal and Regulatory View*, (Springer, 2020).

Henrik Ringbom, Erik Røsæg, Trond Solvang, *Autonomous Ships and the Law, 1st ed,* IMLI Studies in International Maritime Law (Taylor and Francis, 2020).

Baris Soyer, Andrew Tettenborn, *Ship Operations, New Risks, Liabilities and Technologies in the Maritime Sector*, (Routledge, UK, 2021).

Wihelmsen, Trine-Lise and Bull, Hans Jacob, Handbook on Hull Insurance, (2nd ed. 2017).

Master's Thesis

Unknown, "Coverage of Cyber Risks in the Norwegian Insurance Market", University of Oslo, 2022.

Camilla Sogaaard Hudson, "Legal Challenges in Unmanned Shipping", Copenhagen Business School, 17 May 2021.

Jessica Ann Andreassen, "Protecting shipowners' interests: an analysis of cyber risk regulation in public international law and marine insurance contracts, and how legal reform can mitigate against future risk", University of Southampton, 2022.

Electronic Sources

Rolls Royce, "Rolls-Royce unveils a vision of the future of remote and autonomous shipping", last modified 12 April 2016, https://www.rolls-royce.com/media/press-releases/2016/pr-12-04-2016-rr-unveils-a-vision-of-future-of-remote-and-autonomus-shipping.aspx.

MFame Team, "Forget Autonomous Cars – Autonomous Ships Are Almost Here", last modified 31 January 2017, https://mfame.guru/forget-autonomous-cars-autonomous-ships-almost/.

National Cyber Security Centre, "What is cyber security?", last accessed 24 May 2023, https://www.ncsc.gov.uk/section/about-ncsc/what-is-cyber-security.

Marine Digital, “The importance of cybersecurity in the maritime industry”, last accessed 24 May 2023, https://marine-digital.com/article_importance_of_cybersecurity.

Yara International ASA, “The first ever zero emission, autonomous ship”, last accessed 24 May 2023, https://www.yara.com/knowledge-grows/game-changer-for-the-environment/.

Maritime Robotics, “World’s first uncrewed freight route at sea in the Trondheimsfjord”, last modified 2 March 2023, https://www.maritimerobotics.com/post/world-s-first-uncrewed-freight-route-at-sea-in-the-trondheimsfjord.

Howden, “Marine hull insurance”, last accessed 24 May 2023, https://www.howden-group.com/id-en/cover/marine-hull.

Industrial CyberSecurity Pulse, “Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk”, last modified 30 September 2021, https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/.

Safety4Sea, A brief introduction to AI and its applications in the maritime industry, last modified 8 February 2023, https://safety4sea.com/cm-a-brief-introduction-to-ai-and-its-applications-in-the-maritime-industry/.

Prey Project, “What are cyber threats and how to safeguard your data”, last modified 21 April 2023, https://preyproject.com/blog/what-are-cyber-threats-how-they-affect-you-what-to-do-about-them.

NATO Shipping Centre, “AIS (Automatic Identification System) overview”, last modified 2021, https://shipping.nato.int/nsc/operations/news/2021/ais-automatic-identification-system-overview.

GARD, “Loss of Hire Insurance – Back to Basics”, 14 September 2016, https://www.gard.no/web/updates/content/21853295/loss-of-hire-insurance-back-to-basics#:~:text=The%20loss%20of%20hire%20insurers,policy%20the%20claim%20falls%20under.

WTW “Silent Cyber: What you need to know”, 1 February 2021, https://www.wtwco.com/en-GB/Insights/2021/01/silent-cyber-what-you-need-to-know.

GARD, “the Nordic Marine Insurance Plan of 2013, Version 2023”, 20 October 2022, https://www.gard.no/web/articles?documentId=34367309.

The Swedish Club, “Increased Value Insurance/Hull Interest Insurance”, June 2015, https://www.swedishclub.com/media_upload/files/Hull%20Interest%20InsuranceJ.pdf.

Norwegian Hull Club, “Cyber Attack Exclusion Buy-Back”, last accessed on 25 May 2023 https://www.norclub.com/products-and-services/cyber-attack-exclusion-buy-back.

Lloyd’s List, “Lloyd’s exclusion clauses do not meet shipping’s needs, says marine cyber insurer”, 17 May 2023.

Astaara Group, “LMA 5403 A Lost Opportunity?”, last modified July 2020 https://astaaragroup.com/wp-content/uploads/2020/07/LMA-5403-A-Lost-Opportunity.pdf.

Liberty Specialty Market, “Cyber Cargo – addressing the coverage gap”, last accessed 25 May 2023 https://www.libertyspecialtymarkets.com/static/2020-09/LSM_Cyber_Cargo_FS.pdf.

Howden, “Marine cyber risk and insurance”, last modified 6 November 2020 https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden.

International Association of Classification Societies, “Classification societies – what, why and how?”, last accessed 26 May 2023, https://iacs.org.uk/media/8871/classification-what-why-how.pdf.

DNV, “Cyber security to be covered in SMS from 1 January 2021 – are you prepared?”, last modified 2 June 2020 https://www.dnv.com/news/cyber-security-to-be-covered-in-sms-from-1-january-2021-are-you-prepared--176620.

Gard, “Cyber security”, last modified 12 January 2021, https://www.gard.no/web/topics/article/21025160/cyber-security.

AXAXL, “Cyber Insurance”, last accessed 25 May 2023, https://axaxl.com/insurance/products/cyber-insurance-international.

Willis Tower Watson, “CyNav: Navigating shipowners’ cyber security risks”, last accessed 24 April 2023, https://www.wtwco.com/en-US/solutions/products/cynav-navigating-your-cyber-security-risks.

Seatrade Maritime News, “New customised cyber insurance product for shipowners”, last modified 28 April 2020, https://www.seatrade-maritime.com/finance-insurance/new-customised-cyber-insurance-product-shipowners.

Financial Times, “Lloyd’s of London defends cyber insurance exclusion for state backed attacks”, last accessed 25 April 2023, https://www.ft.com/content/e865a3d1-5652-41aa-990a-bb5ad57288c6.