UiO : Faculty of Law
University of Oslo

Coverage of Cyber Risks in the Norwegian Maritime Insurance Market

An analysis of cyber vulnerabilities in vessels, insurance coverage for cyber incidents under standard conditions, and the impact of cyber exclusion clauses

Candidate number: 607

Submission deadline: December 1, 2022

Number of words: 17,818

Table of contents

1 Introduction

In the past few years, the topic of "cyber" has been gaining traction in the maritime industry. This is due both to the uncertainty of the cyber risks in the industry, and to the increase in cyber-related incidents affecting the sector; it has been reported that the number of cyber-attacks in the maritime industry increased as much as 400% from July 2019 to July 2020.[1] This number only includes reported incidents,[2] and it is estimated that the actual number is much higher as incidents have not been disclosed or have been misclassified as machine or human error.[3]

While the number and impact of cyber incidents has drastically increased in the past years, the maritime industry is repeatedly evaluated as being unprepared to deal with cyber risks. Indeed, some evaluate the maritime industry as being "roughly 20 years behind equivalent sectors in terms of cybersecurity."[4] This is alarming, as vessels are "making increasing use of cyber-dependent systems for a wide range of business and operational functions."[5] Cyber-dependent technologies are used for navigation, communication, environmental control, safety, temperature regulation and monitoring of cargo, emergency systems, and many other operational and safety critical functions onboard vessels.[6]

Cyber risks becoming increasingly relevant to the maritime industry, as evaluations of cyber vulnerabilities are moving from focusing on privacy and personal information "into an area which is more about physical damage and bodily injury[.]"[7] It is suggested that accidents or attacks on the cyber-system of these vessels can cause injury to the vessel, its cargo, people, and the marine environment, along with business disruptions.[8] Because of the wide scope of

---

[1] Julian Clark, *The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels,* SHIPPING LAWS AND REGULATIONS 2021, ICLG (Aug. 6, 2021), https://iclg.com/practice-areas/shipping-laws-and-regulations/1-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels (last visited June 1, 2022).

[2] *Id.*

[3] Kimberly Tam & Kevin Jones, *Maritime Cybersecurity Policy: the Scope and Impact of Evolving Technology on International Shipping*, J. CYBER POL'Y 2 (2018).

[4] *Id.*

[5] Andrew E. Tucci, *Cyber Risks in the Marine Transportation System*, *in* CYBER-PHYSICAL SECURITY: PROTECTING CRITICAL INFRASTRUCTURE AT THE STATE AND LOCAL LEVEL 114 (Robert M. Clark & Simon Hakim ed. 2017).

[6] *Id.* at 114-116.

[7] Judy Greenwald, *Marine Sector Struggles with Cyber Risks; Navigation Systems Vulnerable to Attack*, 48 BUS. INS. (2014).

[8] Tucci, *supra* note 5, at 115; DEAN ARMSTRONG, THOMAS STEWARD & SHYAM THEKERAR, CYBER RISKS AND INSURANCE: THE LEGAL PRINCIPLES 134 (2021).

damage to economic interests, it is important to do a comprehensive evaluation of how cyber security and vulnerabilities fit into the marine insurance market.

1.1 Research Question: To What Extent Are Cyber Risks Covered In The Current Norwegian Maritime Insurance Market?

This thesis will answer the question**: to what extent are cyber risks covered in the current Norwegian maritime insurance market?** To do this, some sub questions must first be answered:

1. What is the legal framework for Norwegian maritime insurance contracts?
2. What are the cyber risks vessels are exposed to?
3. Are the cyber risks covered under standard conditions?
4. How do Cyber Exclusion Clauses impact the coverage?

These questions will be answered in order, followed by a discussion on other potential solutions to dealing with cyber risks that fall outside the Norwegian maritime insurance market coverage. The scope of the thesis will be limited to vessels only, and any insurances or cyber risks associated with onshore business of the shipowner and managers or ports will not be evaluated.

1.2 Methodology

To answer these questions, different methodologies will be used. For analysis of the legal framework and how cyber risks are covered under this framework, the methodology used will be legal doctrinal analysis. The research will be conducted by locating the relevant law, mainly in Chapter 2, and then interpreting and analyzing it, in Chapters 2 and 4.[9]

Because this thesis also makes suggestions for action by various actors on considerations such as fairness, economic efficiency, and technical limitations, it is not possible to maintain a strict legal doctrinal analysis through the entirety of the thesis. Questions related to what *ought* to be done, such as Chapter 5 and sub-chapter 4.5, will therefore be conducted using a more interdisciplinary sociolegal methodology.[10] In addition to all the sources listed, many opinions and suggestions are based on the input of professionals working in the industry, from cyber security experts to insurance providers to shipowners. No structured interviews have been

[9] Rónán Kennedy, *Doctrinal Analysis: The Real 'Law in Action', in* LEGAL RESEARCH METHODS: PRINCIPLES AND PRACTICALITIES 21, 31 (Laura Cahillane & Jennifer Schweppe eds. 2016).

[10] MICHAEL SALTER & JULIE MASON, WRITING LAW DISSERTATIONS 129-131 (2007).

conducted, but the input from the industry have been incorporated as appropriate and their questions and concerns have shaped many parts of this thesis.

To evaluate the cyber risks vessels are exposed to, an extensive literary analysis has been conducted in Chapter 3. Efforts have been done to ensure that the literature relied on is peer reviewed or from otherwise credible sources, and that it generally contains a level of detail that is useful for practitioners in the field of cyber security and security of vessels.

2 Legal Framework And Sources

2.1 Introduction and Legal Sources

This section outlines the legal sources and framework used to evaluate the coverage of cyber risks in the current Norwegian maritime insurance market. This section will focus on the black-letter law by evaluating current acts and agreed documents that are incorporated into insurance contracts. The sources evaluated are the Insurance Contract Act, the Nordic Marine Insurance Plan, and the Norwegian Cargo Insurance Clauses (CICG). In addition, textbooks and handbooks have been consulted to understand the meaning of the texts. The books used are the Handbook on Hull Insurance and Norwegian Cargo Insurance, both by Trine-Lise Wilhelmsen and Hans Jacob Bull; and Scandinavian Maritime Law: the Norwegian Perspective by Thor Falkanger, Hans Jacob Bull and Lasse Brautaset. In Chapter 4, the terms of Skuld and Gard's insurance conditions are also evaluated, along with Gard Handbook on P&I Insurance by Edgar Gold.

While this thesis focuses on the "Norwegian" maritime insurance market, the maritime insurance market is by nature international. The P&I conditions evaluated in Chapter 4 are international, and the Nordic Maritime Insurance Plan is common to the Nordic countries; only the cargo clauses evaluated are uniquely Norwegian. As such, much of what this thesis will examine is relevant in other markets and jurisdictions. Still, since only Norwegian cargo terms and Norwegian insurance providers are evaluated, this thesis will still narrow its scope and language to focus on cyber coverage in the Norwegian marine insurance market.

2.2 The Insurance Contract Act

Insurance in Norway is generally regulated by the Insurance Contract Act (ICA).[11] While previous versions had specific exceptions for insurance for ships subject to registration and goods in international transit,[12] the July 2022 revision states that insurance contracts can deviate from the ICA if they are for "large risks."[13] "Large risks" are regulated in Chapter one of the Regulation to the ICA,[14] referring to the Financial Undertakings Regulation[15] § 2-12,

[11] Lov of Forsikringsavtaler (Insurance Contract Act [ICA] 1989:69) (Nor.); LOV-1989-06-16-69.

[12] Previously § 1-3 second paragraph (c) & (e) (ICA 1989:69).

[13] "Store risikoer" in Norwegian. As of this writing, no English version has been published for the July 2022 update. § 1-3 second paragraph, § 1A-2 second paragraph, §2-3 second paragraph (FOR 2022:323).

[14] Forskrift om forsikringsavtaler (forsikringsavtaleforskriften [FOR] 2022:323) (Nor.); FOR-2022-03-04-323.

[15] Forskrift om finansforetak og finanskonsern (finansforetaksforskriften [FOR] 2016:1502) (Nor.); FOR-2016-12-09-1502.

defining different insurance classes that fall under the definition of "large risks." These are further grouped together in § 2-13, which establishes the group for "marine and transport insurance."[16] The section also creates an exclusion for liability insurance.

Because of the exceptions for large risks, the ICA is not the starting point for marine insurance contracts.[17] Instead, insurers are generally free to use their own terms in the insurance contracts. Many of these terms, called conditions, are based on agreed documents or standardized terms, which will be evaluated in turn below.

2.3 Insuring a Vessel

Marine insurance is taken out by the person effecting the insurance[18] to protect the assured's[19] economic interest in the "insurable interest." Insurable interest encompasses more than just an object; "[t]he concept of insurable interest emphasizes that the object of insurance is not the thing as such – [as the ship under a hull insurance] – but the economic interest in the ship."[20] The concept "explains the fact that several economic interests in the same object can be insured, i.e. the objective value, the earnings, the need to avoid expenses, etc[.]"[21]All insurance contracts must relate to an interest to be valid.[22]

The different types of insurances cover different economic interests. In relation to a vessel, the following insurances are common:

- Hull and machinery (H&M), insuring the economic interest in the physical vessel and its equipment, along with some liability for striking and collision;
- War insurance, insuring the economic interest in the vessel against war and war-related perils;
- Cargo insurance, insuring the economic interest in the cargo;
- Protection & Indemnity (P&I), protecting the liabilities as it related to the operation of the vessel;

---

[16] § 2-13 (FOR 2022:323).

[17] Still, the conditions used for marine insurance are often modified to take the ICA into account, THOR FALKANGER, HANS JACOB BULL & LASSE BRAUTASET, SCANDINAVIAN MARITIME LAW: THE NORWEGIAN PERSPECTIVE 619 (4th ed. 2017).

[18] *See infra* Chapter 2.6.1.

[19] *See infra* Chapter 2.6.1.

[20] TRINE-LISE WILHELMSEN & HANS JACOB BULL, HANDBOOK ON HULL INSURANCE 65 (2nd ed. 2017) [hereinafter HANDBOOK ON HULL INSURANCE].

[21] *Id.*

[22] *See* Cl. 2-1 The Nordic Marine Insurance Plan of 2013, Version 2023, https://nordicplan.org/the-plan/ [hereinafter NP].

- Loss of Hire (LOH), protecting the loss of revenue while a ship is out of service due to damage covered under the hull insurance;
- Defence cover, protecting the economic interest as it relates to the cost of legal counsel in relation to the operation of the vessel.

Due to time and word constraints, only hull and machinery (both marine and war), cargo, and P&I insurance will be covered in this thesis.

2.4 The Nordic Marine Insurance Plan

Many Norwegian marine insurance contracts are based on the Nordic Marine Insurance Plan 2013, commonly called the Nordic Plan or simply the Plan.[23] The Nordic Plan is an agreed document[24] with a long history in the Nordic insurance market, and covers rules on hull insurance, war insurance, loss of hire insurance, as well as some specific insurances not discussed in this thesis.

The current Nordic Plan is based on the Norwegian Marine Insurance Plan 1996 Version 2010, and the history of the Norwegian Marine Insurance Plan dates back to 1871 with its first publication.[25] When standardizing the Nordic conditions, the Norwegian Plan was used as the baseline for the Nordic Marine Insurance Plan 2013.[26] Previous versions of the Norwegian plan have included terms for both cargo and P&I, but cargo insurance was removed from the plan in 1964, and were first published as the Cargo Insurance Plan in 1967.[27] New cargo conditions were based on the 1967 Cargo Insurance Plan, and the conditions for cargo insurance used today are found in the Norwegian Conditions relating to Insurance for the Carriage of Goods (CICG) published in 1995, and updated in 2004.[28] Similarly, P&I insurance was removed from the Norwegian plan in 1996, because the P&I clubs "are connected in an international network that to a great extent operates with common insurance conditions."[29] It was therefore not natural for the P&I clubs to tie their conditions to the Nordic Plan, and they remain separate from the Plan.[30]

---

[23] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 26.

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*; TRINE-LISE WILHELMSEN & HANS JACOB BULL, NORWEGIAN CARGO INSURANCE 14 (2012) [hereinafter NORWEGIAN CARGO INSURANCE].

[28] *Id.*

[29] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 29.

[30] *Id.*

The Nordic Plan is regularly updated by the Standing Revision Committee, now every four years,[31] and is maintained and published by Cefor, the Nordic Association of Marine Insurers, in collaboration with Danish Shipping, The Finnish Shipowners' Association, The Norwegian Shipowners' Association, and The Swedish Shipowners' Association.[32] The Plan comprehensively deals with issues related to all parts of the insurance contract, including premiums, duties of the insurer and the person effecting the insurance, total loss, and the settlement of claims. The current version as of this writing is based on the 2013 plan, Version 2023, which was published for use on October 3rd, 2022.[33]

Norwegian hull and machinery and war insurers base their insurance contracts on the Nordic Plan. Hull and machinery and war policies are first party property insurance, and encompass most of the vessel and its equipment, with a few limitations. Under the Plan, these limits relate to fishing equipment, items used for securing or carrying cargo, and items intended for consumption or that is lost during normal use of the vessel, with the exception of bunker and lubricating oil, which is covered.[34]

2.5 The Norwegian Conditions relating to Insurance for the Carriage of Goods

As mentioned above, cargo insurance is no longer regulated by the Nordic Plan, but rather by the Norwegian Conditions relating to Insurance for the Carriage of Goods (CICG).

Neither the Nordic Plan nor the CICG are in themselves binding but becomes binding on the parties to the insurance contract by being incorporated into standard maritime insurance policies.[35] The standard method of incorporation is to refer to the Plan or the CICG in the insurance contract.[36] The supplementary Commentary of both the Plan and the CICG are given significant weight for the interpretation of the conditions by Norwegian courts, and will also be used in this thesis for clarification.[37]

---

[31] *Id.* at 30.

[32] *See* Nordic Plan Agreement of 2010, with Addendum 2019, https://cefor.no/globalassets/documents/clauses/nordic-plan/agreement-nordic-plan-03-11-2010---amended-09-12-2016-with-addendum-1-21-08-2019.pdf; *The Nordic Marine Insurance Plan of 2013, Version 2023*, CEFOR, https://cefor.no/clauses/nordic-plan/ (last visited Oct. 13, 2022).

[33] CEFOR, *supra* note 32.

[34] NP Cl. 10-1 & 10-3.

[35] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 29-30; NORWEGIAN CARGO INSURANCE, *supra* note 27, at 14.

[36] *Id.*

[37] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 27; NORWEGIAN CARGO INSURANCE, *supra* note 27, at 15.

2.6 Marine Insurance Framework

2.6.1 Person Effecting Insurance, Assured, And Insured

In Nordic insurance law, there is a distinction between the person effecting the insurance, meaning the person that enters into the insurance contract with the insurer, and the assured, meaning the beneficiary under the contract.[38] The distinction exists because the person effecting the insurance is not always the one that has an economic interest in the objects insured under the contract; the assured is the person that "holds a position with a right to compensation[.]"[39] While these parties are often the same, usually the shipowner, this is not always the case; for instance, the person effecting the insurance might be the bareboat charterer, while the shipowner is the assured.[40] There is also a distinction between the duties of the person effecting the insurance (such as the duty to pay premiums, NP Cl. 6-1), and the duties on the assured, such as duties related to safety regulations in NP Ch. 3, discussed further in Chapter 4.6.

Due to the use of a variety of sources that do not make this distinction, the term "insured" is something used in this thesis. Where appropriate, the term has been substituted with the person effecting insurance or the assured, but where this is not possible, the term "insured" has been kept to encompass both.

2.6.2 Scope Of Cover: Perils, Casualty, Losses Covered, Causation

To determine what, when, why, and how an insurer is liable under an insurance contract, we have to start by examining the scope of cover. The term "scope of cover" refers to the nature of the cover available to the assured.[41] Scope of cover addresses several issues, the first one being what risks are insured against, in other words defining the perils that are covered under the marine insurance.[42] "A number of perils may pose a risk to the ship: heavy weather, ice, problems with cargo, performance of the captain or crew, failure of equipment on board. . . Some of these perils, but not necessarily all of them, may be covered by insurance."[43] The peril therefore needs to be identified in order to establish liability under an insurance contract.

---

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

[39] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 45.

[40] Cl. 1-1, Commentary to the Nordic Marine Insurance Plan of 2013, Version 2023, https://nordicplan.org/commentary/.

[41] FALKANGER, BULL & BRAUTASET, *supra* note 17, at 626.

[42] *Id.*; HANDBOOK ON HULL INSURANCE, *supra* note 20, at 78.

[43] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 78.

The Plan covers perils under two distinct principles: the "all risks principle" and the "named risks principle."[44] Under the Plan, hull and machinery (H&M) coverage operates under the all risks principle, meaning that all risks, unless specifically excluded, are covered by the insurance policy.[45] In contrast, war risk coverage under the Nordic Plan follows the named perils principle, meaning that only those perils that are named specifically in the Plan will be covered by the policy.[46] Both principles will be discussed in detail in the relation to the NP and the CICG in Chapter 4.

The second issue scope of cover addresses is how to define the casualty, also called insured event or incidence of loss. The casualty is the event the covered peril must *materialize through* to trigger the insurer's liability.[47] Per the language of the Plan, the casualty is the point in time "when the interest insured is struck by an insured peril."[48]

The third issue is defining what type of loss is covered by the insurance contract.[49] Under the Nordic Plan, the starting point is that "[t]he insurer is liable for loss incurred when the interest insured is struck by an insured peril during the insurance period."[50] The losses covered will therefore be the loss to the interest insured caused by a qualifying event.

Lastly, the fourth issue scope of cover addresses is establishing causation. Causation requires that a connection is required between the peril insured against and the casualty (insured event), and between the casualty and the loss for which the insurer is liable.[51] As a starting point, the peril must be a necessary condition for the casualty. This is the minimum requirement, and the causation must be legally qualified in some additional way for the insurer to be liable for the loss.[52] There are generally two methods for to solve this problem: the principle of adequate causation or proximity,[53] and the principle of combination of causes/apportionment.[54] The Nordic Plan and the CICG base their regulation of causation on the principle of

---

[44] *Id.* at 79; FALKANGER, BULL & BRAUTASET, *supra* note 17, at 627.

[45] NP Cl. 2-8; HANDBOOK ON HULL INSURANCE, *supra* note 20, at 79.

[46] *Id.*

[47] *Id.* at 78, 129.

[48] *Id.* at 130.

[49] *Id.* at 78.

[50] NP Cl. 2-11 sub-clause 1.

[51] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 78; NORWEGIAN CARGO INSURANCE, *supra* note 27, at 83.

[52] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 116.

[53] FALKANGER, BULL & BRAUTASET, *supra* note 17, at 629.

[54] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 116.

combination of causes[55] and is, as a starting point, based on NP Cl. 2-13 and CICG § 20 first paragraph.[56] This means that liability shall be apportioned amongst the perils according to the influence which of them had on the loss rather than placing the liability on the cause closest (most proximate) to the loss.[57]

The terms and concepts defined above can be difficult to differentiate because they are so closely linked. For a visual representation see Figure 1 below, where the different concepts are placed in the boxes and the arrows represent causation. Thus, for the insurer to be liable for any damage or loss, the whole chain illustrated below must be present; a peril insured against must cause an insured event which causes damage or loss to an insured interest, all within the insurance period. If a peril and casualty occur but does not cause any damage or loss, the insurer is not liable.[58] Similarly, it is not sufficient to trigger liability "that a peril is established; the peril must in fact materialize into an even that causes damage[.]"[59]

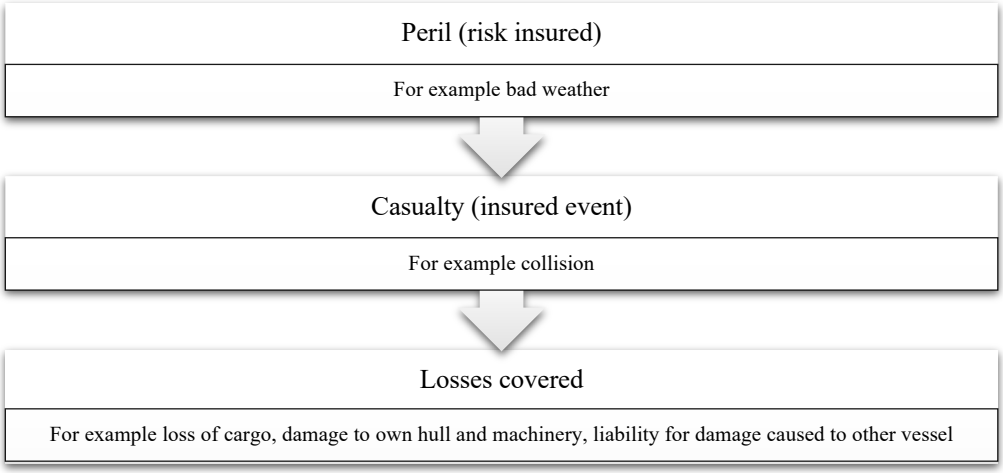

Figure 1 – *Scope of cover illustration*

With this legal framework in mind, we will now evaluate the specific cyber risks related to vessels, before we place the risks in the above framework in Chapter 4.

---

[55] *Id.* at 128; § 20 first paragraph of Conditions relating to Insurance for the Carriage of Goods of 1995, Version 2004 [CICG], https://cefor.no/globalassets/documents/clauses/norwegian-cargo-clauses/cefor-cargo-clauses-261-2004-eng.pdf.

[56] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 116.

[57] A notable exception to the combination of causes principle under the Plan related to Cl. 2-14, which states that if the loss has been caused by both marine perils (Cl. 2-8) and war perils (Cl. 2-9), "the whole loss shall be deemed to have been caused by the class of perils which was the dominant cause." The CICG also has an exception to the general rule in cases related to chemical, biological, biochemical, or electromagnetic weapons, CICG §20 second paragraph.

[58] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 131.

[59] *Id.* at 129.

3 Risk Analysis Of Maritime Cyber Incidents

3.1 Introduction

3.1.1 Research Question: What Are The Insurable Risks (Perils) Stemming From Cyber Incidents In The Maritime Sector?

While it is agreed that cyber security poses a substantial risk in the maritime sector, there is little comprehensive literature evaluating what the practical risks related to cyber-incidents are for vessels. This section will therefore evaluate the existing literature and answer the question: **what are the insurable risks (perils) stemming from cyber incidents in the maritime sector?**

In this risk analysis section, I will first limit the scope and put forth some definitions that applies to the remainder of the thesis. I will then look at the vulnerabilities presented in the literature related to maritime cyber security. Next, I will look at the cyber vulnerabilities of the individual components of a vessel and what insured perils and casualties might arise from this, before concluding with a summary of the findings.

3.1.2 Methodology

This section is a literature review of the market and vulnerabilities as they exist today. There is a lack of detailed information about the intersection of cyber risks and vessel operations; many in the shipping sector are worried about cyber risks, and many cyber security experts are worried about vessels, but there are few who have sufficient knowledge in both areas to create comprehensive descriptions of the ways in which components of the vessel are at risk for cyber incidents. As such, much of the existing literature talks about "cyber risks to the operational system" or "vulnerabilities in the steering of a vessel," without explaining or evaluating exactly what a potential malicious actor could do if accessing the vessel's cyber structure.[60] Such broad statements should be view with skepticism, and the thesis therefore relies on the conclusions of the articles and studies that have looked more in-depth at these issues.

3.1.3 Definitions

It is necessary to define some terms before diving further into this risk analysis.

The term "cyber system" will be used to talk about the computers, computer software, computer systems and networks, electronic systems, and computer code, and any use thereof,

[60] MASS SOLDAL LUND ET AL., INTEGRITY OF INTEGRATED NAVIGATION SYSTEMS (2018).

as usually defined in cyber exclusion clauses which will be evaluated in depth in Chapter 4. While the term might be imprecise from a technical standpoint, the term is intentionally used broadly in this thesis to match the way the word is used in the marine insurance market.

Furthermore, the term "cyber-attacks" is used to refer to unauthorized access to and manipulation of electronic hardware, software, and information as a means for inflicting harm. This definition does therefore not distinguish between cyber-crime, cyber-warfare, cyber-terrorism, or the like. Furthermore, the term will not make distinctions between targeted and untargeted attacks. While targeted attacks will be aimed at the specific vessel in question, untargeted attacks are attempts at infiltrate cyber systems that are conducted broadly, with the hope that the attack will infiltrate something, whether that is a personal computer, an office space, or a vessel.[61] Because both targeted and untargeted attacks are conducted intentionally and with an intent to cause harm,[62] we will not make further distinctions between the two types.

Cyber events that are not cyber-attacks, such as wrongful use, software errors, and the like, will be referred to as "cyber accidents." This thesis will use the term "cyber incidents" to include both malicious cyber-attacks and cyber accidents.

Lastly, the IMO defines "maritime cyber risk" as "a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety[,] or security failures as a consequence of information or systems being corrupted, lost[,] or compromised."[63] To avoid confusion with the term "risk" as it related to perils, the phrase "maritime cyber vulnerability" will be used instead. The word "cyber security" will be used to describe the identification off, and measures taken to limit these vulnerabilities and thus protect the cyber systems of vessels.

3.2 Cyber Vulnerabilities on Vessels

There is not one definite reason why the maritime sector is so vulnerable to cyber incidents; rather, a myriad of reasons work in concert to create and maintain these vulnerabilities. First, there is a lack of understanding and expertise surrounding the IT and OT systems of each vessel. For instance, "[i]n many shipping companies, the IT department located at headquarters tends to be in charge of land-based IT systems, whereas the vessel-based IT systems fall under

[61] M. Bob Kao, *Cybersecurity in the Shipping Industry and English Marine Insurance Law*, 45 TUL. MAR. L.J. 467, 474 (2021).

[62] Evaluated further in Ch. 4.5.

[63] Int'l Maritime Org. [IMO] 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.

the purview of the marine technical department – who often have very limited IT background knowledge."[64] The individual devices and equipment onboard a vessel are also often maintained and supported by the provider of that piece of equipment, meaning that there is also a lack of understanding of the vulnerabilities when these devices connect to each other. A further weakness on vessels is that their digitalized equipment is a patchwork of technology built to last for decades, much of which is outdated, lack continued updates, and was never intended to be connected to the Internet.[65]

To clarify the actual vulnerabilities of a vessel, we will now look at its individual components to see whether and how they are vulnerable to cyber incidents.

3.2.1 Operational Technology

Ships today are operated by both Information Technology (IT) and OT systems.[66] The more familiar IT-systems store and process data information, such as personal data of people onboard the vessel, certificates and compliance documents, and policies and procedures.[67] OT-systems, on the other hand, control the vessel, its movements, and industrial systems onboard, "such as thruster direction and force, rudder angle, cargo handling, ballast water handling, power distribution[,] and navigational aiding system."[68] In the words of the IMO, IT systems "may be thought of as focusing on the use of data as information," while OT systems "may be thought of as focusing on the use of data to *control or monitor physical processes*"(emphasis added).[69] While all businesses can have vulnerable IT-systems, the vulnerabilities and consequences of interruption in the OT-systems of a vessel are unique to the maritime industry.

Cybersecurity of a vessel therefore includes not just the traditional concerns of the IT system, but also the OT-systems, which requires receiving the correct information at the right time in relation to speed, position, weather, location of other vessels, etc.[70] While OT and IT systems have been separated in the past, they are increasingly connected to each other and to the internet, making the systems more vulnerable to a cyber incident.[71] Many of these systems

---

[64] Lars Jensen, *Challenges in Maritime Cyber-Resilience*, 5 TECH. INNOVATION MGMT. REV. 35, 36 (2015).

[65] Kao, *supra* note 61, at 476; Oliver Daum, *Cyber Security in the Maritime Sector*, 50 J. MAR. L. & COM. 1, 6 (2019); Greenwald, *supra* note 7.

[66] E. Erstad, R. Ostnes & M.S. Lund, *An Operational Approach to Maritime Cyber Resilience*, 15 INT'L J. ON MARINE NAVIGATION AND SAFETY OF SEA TRANSP. 27, 29 (2021).

[67] *Id.*

[68] *Id.*

[69] IMO, *supra* note 63, at 2.1.2.

[70] *Id.*

[71] Erstad, Ostnes & Lund, *supra* note 66, at 29.

were never intended to be connected to the internet, and have inadequate or no protection against cyber threats.[72]

Now, however, they are connected to the integrated bridge system (IBS), which "acts as the main command and control of a vessel as it interconnects various digital devices used for navigation in open seas and is also connected to other on-board systems of a vessel e.g., navigation and control, propulsion and machinery management system, cargo management system and safety management system, core infrastructure systems, administrative and crew welfare systems, etc."[73] The IBS of vessels increasingly do have internet access,[74] which leaves "not only an IBS but also all the on-board systems vulnerable to cyber-attacks."[75] Some bridge operations have been shut down with ransomware demands, and Electronic Chart Display and Information Systems (ECDIS) security flaws have been targeted.[76] Furthermore, attempts at infiltration has shown that "ECDIS flaws could allow an attacker to access and modify files and charts on board or on shore. The result of modified chart data would be unreliable and potentially dangerously misleading navigation information. That could lead to a mishap resulting in environmental and financial damage."[77]

Despite this, it does not appear from the literature that the full OT systems are vulnerable to cyber-attacks. The threat appears to be related to the interruption of the access of information and control of the OT systems for shorter periods of time. While limiting the access to information such as wind and current readings can be important, it is not so threatening as someone with malicious intent remotely taking control over the ship. If someone were able to control parts of the OT of the vessel, the most critical functions still have manual means of control. The crew can therefore limit most potential damage if they are aware that a cyber-attack is taking place.

3.2.2 Cargo Management

While many systems and monitors related to the cargo of a vessel are digitalized, there has been little literary discussion of any threats to these systems. Cargo is only mentioned in

---

[72] Greenwald, *supra* note 7.

[73] Malik Shahzad Kaleem Awan & Mohammed A. Al Ghamdi, *Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)*, 7 J. MAR. SCI. & ENGINEERING 1, 2 (2019).

[74] *Id.*

[75] *Id.*

[76] Phil McGillivary, *Why Maritime Cyberseucirty is an Ocean Policy Priority and How it Can Be Addressed*, 52 MAR. TECH. SOC'Y J. 44, 44 (2018).

[77] JOSEPH DIRENZO, DANA A. GOWARD & FRED S. ROBERTS, THE LITTLE-KNOWN CHALLENGE OF MARITIME CYBER SECURITY (2015).

general terms,[78] and a detailed risk analysis of cargo management specifically is therefore not possible. Cargo systems are considered a part of OT systems, and the general analysis above therefore also applies to cargo systems.

3.2.3 GPS and Navigation

The biggest threats in the cyber maritime space are related to issues of navigation and collision avoidance. When people say that hackers can "take control of a ship," what they often mean is that hackers can control of Global Positioning System (GPS) signals related to the navigation of the vessel.[79] While it is misleading to say that GPS interference is taking control of a ship, which conjures up an image of someone taking over the capacity to physically stir the ship, GPS interference is still something that can have serious consequences for a vessel as it can affect bridge navigation, GPS-based timing, and communications equipment.[80]

3.2.4 Spoofing and Jamming

Intentionally manipulating the GPS signal of a vessel is called *spoofing*.[81] Spoofing is manipulation of the GPS navigation system, where "the user is presented with incorrect position data[.]"[82] This can both affect the ship itself, as the location on the electronic charts systems appears different than the actual geographical location of the vessel, and affect other ships, as they believe the vessel is in another location than it actually is. Spoofing can also go undetected by the master and crew; whereas loss of GPS signals will usually set off alarms or stop the operation of the vessel, systems are unable to detect when it is receiving wrongful GPS signals.[83]

Numerous incidents of spoofing have been reported. The Centre for Advanced Defense Studies published a report in 2019 on spoofing in Russia, the Crimea, and Syria, where they identified 9,833 instances of spoofing affecting 1,311 vessels between February 2016 and 2019.[84] Furthermore, multiple research teams have intentionally conducted spoofing attacks on vessels in operation.[85] The autopilot for one of these vessels corrected for the spoofing, which

---

[78] *See e.g.* Tucci, *supra* note 5, at 114-115; Daum, *supra* note 65, at 5; Erstad, Ostnes & Lund, *supra* note 66, at 29.

[79] *See e.g.* Logan Kugler, *Why GPS Spoofing is a Threat to Companies, Countires*, 60 COMM. ACM 18, 18 (2017).

[80] NORMA CYBER, ANNUAL THREAT ASSESSMENT 2022, 8 (2022)

[81] Daum, *supra* note 65, at 8.

[82] *Id.* at 9.

[83] *Id.* at 8.

[84] ARMSTRONG ET AL., *supra* note 8, at 135.

[85] Erstad, Ostnes & Lund, *supra* note 66, at 30; *see also* Kao, *supra* note 61, at 478.

resulted in a "'controlled' grounding of the vessel."[86] Some people now fear that such GPS hijacking can take place in sensitive areas like the Suez Canal, where the grounding of the ship Ever Given in March 2021 demonstrated just how vulnerable that area is to minor changes in navigation.[87] A cyber defense firm has also demonstrated that it is possible to alter a vessel's position during such critical times when they hacked into a vessel's systems during night-time passage through a narrow canal.[88] If the vessel had been operational during this planned infiltration, "it would have most certainly run aground."[89]

There appears to have been large changes in the ability to carry out spoofing attacks in the last ten years. At the time one of the research teams spoofed a vessel, they noted that received information about the systems and the vessel that a normal hacker would not have easy access to, and emphasized that there is a "need for both proximity and persistent presence . . . for this attack to work. It can't be done remotely."[90] The equipment used for the spoofing attacks were "a laptop and a homemade receiver costing less than USD 3,000."[91]

Since then, the price is estimated to have dropped below $1,000,[92] and as can be seen from the reported numbers above, there have been thousands of instances of spoofing attacks. With the right motivation, persistence, and physical access, a spoofing attack is therefore not outside the realm of feasible economic and practical considerations. Still, spoofing is reported as being primarily conducted by nation state actors.[93] Spoofing attacks could cause great damage in connection with the use of auto pilot on a vessel if the master and crew are relying solely or too heavily on those systems. The inability to navigate safely without GPS signals could lead to grounding and collision, which could have great impact on hull and machinery, cargo, liability towards others, personal injury, or environmental pollution. Effectively countering spoofing technology is thus named as one of, if not the *most* pressing cyber vulnerabilities for vessels.[94]

---

[86] Odd Sveinung Hareide et al., *Enhancing Navigator Competence by Demonstrating Maritime Cyber Security*, J. NAVIGATION 1, 11 (2018).

[87] Lloyd's Register, *Can a lack of cyber security send cargo ships off course?*, LR (July 27, 2021), https://www.lr.org/en/insights/articles/can-a-lack-of-cyber-security-send-cargo-ships-off-course/.

[88] Vincent Wee, *Naval Dome exposes vessel vulnerabilities to cyber attack*, SEATRADE MARITIME NEWS (Dec. 22, 2017), https://www.seatrade-maritime.com/asia/naval-dome-exposes-vessel-vulnerabilities-cyber-attack.

[89] *Id.* While the defense firm claims to also have eliminated radar target and disrupted the valves and pumps of the ballast system, they have not provided detailed information on how they got access to the systems and whether this was possible due to the cooperation of the vessel's owner and crew. Because the test and subsequent publication was done to market their own services, these findings will not be considered further in this section.

[90] DIRENZO ET AL., *supra* note 77.

[91] Daum, *supra* note 65, at 8.

[92] Some estimate that the pricetag has even dropped to below $1,000, Kugler, *supra* note 79, at 19.

[93] NORMA CYBER, *supra* note 80, at 8.

[94] Daum, *supra* note 65, at 18.

Jamming is similarly related to GPS signals, but entails the denial of reception.[95] This means that the vessel would lose all access to GPS signals, which will severely impact navigation. In this case, alarms are likely to alert the crew of the lack of signals.[96] Jamming can lead to major problems in situations where there is low staff, which will likely be the case in more modern and digitalized ships, or "during a highly complex maneuver requiring high concentration, such as docking under very low visibility."[97]

Jamming is a less sophisticated method than spoofing, and jamming devices are relatively small and inexpensive.[98] Jamming can be "particularly effective on ships, as they are often very far from other signal sources, making those signals very weak and easy to jam theoretically and in practice."[99] It could theoretically be possible for attackers to deploy land-based jamming on ships, which could be highly effective on equipment such as wireless-only automooring systems that use radio-based remote controls and do not have any wired alternative.[100] However, there is thus far no citable evidence for ocean-based instances of spoofing.[101] At ports, jamming has been used frequently for events such as cargo theft by organized crime.[102]

3.2.5 AIS

Another issue related to GPS is the disturbance of Automatic Identification System (AIS) signals. AIS shows the ship's geographical position and other characteristics, such as cargo loaded,[103] speed, type of vessel, and destination,[104] and is required by the IMO to be installed on vessels larger than 300 gross tonnage engaged in international voyage, vessels larger than 500 gross tonnage not engaged in international voyage, and all passenger vessels.[105] This means that the shipowners, insurers, and anyone else can see where the vessel is through open-source data.[106] The availability of this information is a potential weakness that could be exploited by for instance pirates tracking the location of a ship with especially interesting

---

[95] DIRENZO ET AL., *supra* note 77.

[96] Tam & Jones, *supra* note 3, at 12.

[97] DIRENZO ET AL., *supra* note 77.

[98] Tam & Jones, *supra* note 3, at 9.

[99] *Id.*

[100] *Id.* at 10.

[101] *Id.*

[102] DIRENZO ET AL., *supra* note 77.

[103] Hristos Karahalios, *Appraisal of a Ship's Cybersecurity efficiency: the case of piracy*, 13 J. TRANSP. Security 179, 182-183 (2020).

[104] DIRENZO ET AL., *supra* note 77.

[105] SOLAS regulation V/19.2.4, Carriage Requirements for Shipborne Navigational Systems and Equipment, as amended by Resolution A.1106(29).

[106] Numerous websites display AIS signals and information, including https://www.marinetraffic.com, https://www.vesselfinder.com, and https://www.myshiptracking.com.

cargo.[107] All AIS signals are automatically assumed to be genuine, and "[t]here is no built-in security or verification system that provides a level of backup."[108] These signals are not encrypted nor authenticated, and thus can be used for spoofing, hijacking, or jamming.[109] Some assess that the "GPS signal of AIS could be interrupted with low-cost jammers available at a price of $20."[110]

In practice, a study evaluating the reported incidents of AIS manipulation has found that AIS has been deliberately exploited to hide the real identity of a vessel, carry illegal concealed cargo, and avoid attacks from pirates.[111] The interferences of AIS signals is mainly done to conduct information warfare, but that it can also have serious legal and financial implications if the AIS signals "move" a vessel into sanctioned areas.[112]

3.2.6 Computer Virus

One of the most common fears related to cyber vulnerabilities is the introduction of a computer virus into an IT system. A computer virus is defined as "[a] computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk."[113] A computer virus is thus a very specific type of cyber-attack, but the consequences can be quite broad. A virus could impact the IBS, OT, or IT systems of a vessel, and lead to the removal or destruction of data, such as personnel data or electronic maps and navigational software. A research group has demonstrated the an ECDIS could be attacked by penetrating the system and read, download, replace, and delate any file stored on the machine hosting the system.[114] Data is especially important for vessels like cruise ships, that hold large amounts of personal data with regard to passengers, such as details concerning bank accounts and credit cards.[115] A virus might also come in the form of a ransomware

[107] Ships are now often allowed to turn off their AIS when traveling through high piracy areas for exactly this reason. Tam & Jones, *supra* note 3, at 15.

[108] DIRENZO ET AL., *supra* note 77.

[109] Karahalois, *supra* note 103, at 182-183.

[110] *Id.* at 182, citing DIRENZO ET AL., *supra* note 77.

[111] Awan & Ghamdi, *supra* note 73, at 12.

[112] NORMA CYBER, *supra* note 80, at 11.

[113] *Glossary: Virus*, COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/glossary/term/virus (last visited Nov. 24, 2022).

[114] Kao, *supra* note 61, at 480.

[115] Barış Soyer, *Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems, in* MARITIME LAW IN MOTION 629 (Proshanto K. Mukherjee et al. ed., 2020).

attack, where the computer system and data stored therein becomes inaccessible to the owner until a ransom is paid.[116]

Depending on their connectivity, a cyber-attack on a vessel could also infiltrate the land-based business of the assured.[117] This would normally not happen in a traditional maritime casualty; only the vessel and everything on board would be at risk. Now, however, connections between the vessels computer systems and that of the onshore business can cause significant disruptions if one of them is affected, as it would necessarily affect the other one. This can lead to major business disruptions and large financial losses.

3.3 Conclusion

There are many new perils arising from cyber vulnerabilities for vessels. In broad strokes, the cyber risks vessels are exposed to can be described as cyber-attacks and cyber accidents. A few examples from each category are presented in the table below.

Cyber-attack on vessel	**Cyber accident on vessel**
Computer virus	User error/human error
GPS interference: spoofing, jamming, AIS interference	Software issues, bugs, outdated version, etc.
Efforts targeting the OT system	Incompatibility of hardware and software as connected

Table 1 – *Perils from cyber incidents*

It is important to note that the cyber element giving rise to liability of the insurer does not always come in the form of a peril, but sometimes in the form of the casualty or the causation linking the peril with the loss suffered. This will be examined at the beginning of the next chapter.

[116] *Ransomware*, INTERNET CRIME COMPLAINT CENTER, https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf (last visited Nov. 24, 2022).

[117] Soyer, *supra* note 115, at 630.

4 Coverage Of Cyber Risks In The Norwegian Maritime Insurance Market

We will now return to a doctrinal analysis. First, we will place the cyber risks examined in Chapter 3 in the insurance framework outlined in Chapter 2. We will then look at standard coverage in the Norwegian maritime insurance market for hull and machinery, war risk, and cargo, and then look at the exclusion clauses frequently used in them all. Next, we will look at the concrete terms of coverage for two Intentional Clubs offering P&I insurance. We will then examine the issues related to identifying the malicious actor and the obligations of the insured, before concluding with an overview of the current coverage.

4.1 Placing Cyber within the Legal Framework

Cyber risks have not been explained in terms of Norwegian insurance concepts before. We therefore have to bridge the gap between cyber risks and marine insurance. Cyber coverage is typically examined by evaluating "scope" and "trigger."[118] These terms are not used in the Norwegian marine insurance market; what is referred to as "scope" encompasses what has explained as the "losses covered" above, while the "trigger" is the "peril" or "risk insured."[119] Cyber coverage is therefore typically examined by looking at losses covered and perils. To fully understand cyber coverage in the marine insurance market, we therefore have to fill in the understanding of causation and casualty.

The concept of causation should not be different for cyber incidents compared to more traditional perils. At the bare minimum, causation requires that there is a connection between the peril and the casualty, and the casualty and the losses covered. Determining the causation of a loss is a fact-specific endeavor, rather than legal or theoretical, and will thus be tied to the specific incident in question.

The concept of casualty or insured event in relation to cyber incidents and marine insurance is not expressed in the literature on the topic. As mentioned earlier, the casualty is the event the covered peril must materialize through to trigger the insurer's liability. This means two things for cyber incidents. First, if a covered peril materializes through the use of cyber systems or equipment, the casualty is the cyber incident. This could for instance be if state actors use computer viruses to infiltrate the computer system of a ship. Second, if the cyber element leads to a casualty, the cyber element is the peril. This could happen when the wrong

[118] Kirsty Middleton & Maria Kazamia, *Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns, in* THE "DEMATERIALIZED" INSURANCE 185, 194 (Pierpaolo Marano et. al. ed., 2016).
[119] *Id.* at 194-195.

use of software or a malfunction of the computerized system for instance leads to errors in temperature regulation for cargo.

Cyber elements can also be part of the losses covered. Here, a distinction has to be made between damage to the cyber equipment itself, and any consequential damage to the vessel and other equipment following a cyber incident. Much of the cyber equipment is covered as part of the equipment outlined in Cl. 10-1. Indeed, the Commentary to Cl. 10-1 was amended in the latest version to clarify that "equipment" also includes "digital, navigation[,] and communication equipment."[120] If the shipowner fails to maintain the computer equipment and the equipment is damaged following a cyber incident, the insurer is not liable for the damage to that equipment itself.[121] While it is not yet clear what will qualify as inadequate maintenance of computer systems on vessels, failure to update software and patch known and serious vulnerabilities might fall into this category. Whether consequential damages to the vessel and other equipment following a cyber incident is covered depends on whether the damage is caused by insured events and risks insured.

The losses caused by maritime cyber incidents generally fall into one of three categories: business disruption; theft of information, finance, and cargo; and damage to reputation, goods, and environment.[122] Vessels and equipment must necessarily fall within the third category as a "goods," as they are also at risk of damage or loss. These will all result in losses to the shipowner.

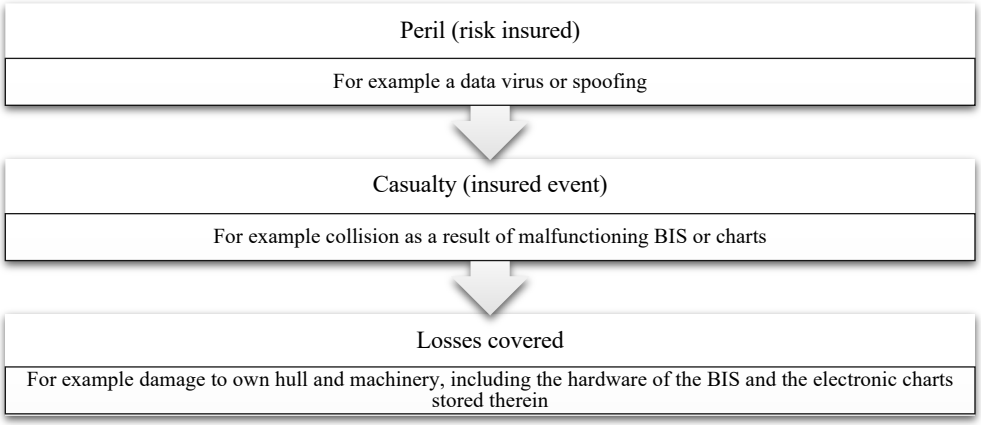

Figure 2 – *Placing cyber in the scope of cover illustration*

[120] Commentary to the NP, Ch. 10-13.

[121] NP Cl. 12-13; *see also* Trine-Lise Wilhelmsen & Hans Jacob Bull, *Hull Insurance of Autonomous Ships According to Nordic Law: What Are the Challenges? in* AUTONOMOUS SHIPS AND THE LAW 175, 185 (Henrik Ringbom, Eris Røsæg & Trond Solvang eds., 2021) [hereinafter *Hull Insurance of Autonomous Ships*].

[122] Tam & Jones, *supra* note 3, at 3.

Marine insurances covers losses from all three categories: business disruption which results in loss of income falls under loss of hire insurance; theft of cargo and perhaps finance, but not information, will fall under cargo or war insurance, depending on the actor; and damage to goods and environment will be losses covered under H&M marine or war insurances, cargo insurance, and P&I insurance.

The below table places some of the unique cyber elements of vessels in the terms of perils and casualties. The table is by no means exhaustive and is merely an attempt to organize all the above concepts and technologies.

PERIL	AFFECTED SYSTEM	CASUALTY / INSURED EVENT
Spoofing Jamming	GPS signal, confusing autopilot or crew correcting route wrongly, interference with communications	Collision, grounding, delay Interrupting wireless systems like mooring
Interference with OT system	Interrupt lines of communication Interfere with maneuvering	Collision, grounding, delay Interrupting wireless systems like mooring unable to receive or provide aid in case of emergency
Data virus	Steal, delete, or encrypt data Data and personnel/cargo information	Can most notably lead to one of the other perils
AIS interference	Use of AIS	Cargo theft, pirate attack, foreign state interference
	Manipulation of AIS	Collision, delay, sanctions
Accidents (wrong use, software error, lack of compatibility, etc.)	Any	Collision, grounding, delay

Table 2 – *Examples of cyber perils in the scope of cover analysis*

4.2 Standard Insurance Clauses

4.2.1 Research Question: Are The Cyber Risks Covered Under Standard Conditions?

4.2.2 Hull & Machinery and War Insurance

The Plan covers perils under two distinct principles: the "all risks principle" and the "named risks principle."[123] Under the Plan, marine hull and machinery (H&M) coverage operates under the "all risks principle." Marine H&M coverage is lain out in NP Cl. 2-8 as follows:

> An insurance against marine perils covers all perils to which the interest may be exposed, with the exception of:
> a. perils covered by an insurance against war perils in accordance with Cl. 2-9,
> b. capture at sea, confiscation, expropriation and other similar interventions by own State power . . .
> c. requisition by State power,
> d. insolvency or lack of liquidity of the assured . . .
> e. perils covered by the RACE II Clause [related to nuclear and radioactive fuel, waste, and weapons, and chemical, biological, bio-chemical, or electromagnetic weapons].[124]

The use of all risks principle for marine H&M is significant for distribution of risks for new perils.[125] Under this principle, the risk of covering new perils, or perils not thought about when the conditions were written, will fall on the insurer.[126] Although cyber incidents have most certainly been thought about during the most recent revision of the Plan in 2022, the peril is likely still considered "new" as there has been no changes to confirm or deny coverage in the Plan. As cyber risks are not mentioned in any of the exclusions, they are covered for marine perils based on the Plan.

In contrast, war H&M coverage under the Nordic Plan follows the named perils principle, meaning that only those perils that are named specifically in the Plan will be covered by the policy.[127] Clause 2-9 lays it out as such:

---

[123] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 79; FALKANGER, BULL & BRAUTASET, *supra* note 17, at 627.

[124] NP Cl. 2-8.

[125] HANDBOOK ON HULL INSURANCE, *supra* note 20, at 80.

[126] *Id.*

[127] *Id.* at 79.

An insurance against war perils covers:

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 subclause 1 (a) - (d).

The insurance does not cover:

a. insolvency or lack of liquidity of the assured . . .
b. perils covered by the RACE II Clause [related to nuclear and radioactive fuel, waste, and weapons, and chemical, biological, bio-chemical, or electromagnetic weapons],
c. requisition by State power.[128]

At first glance, it does not appear that any cyber incidents are covered under the war insurer, as they are not listed in the named perils. However, cyber incidents might manifest themselves through covered perils, which would make the insurer liable for covered losses.[129] As mentioned above, cyber incidents can a peril, a casualty, or part of the losses covered. For instance, if a terrorist group launched a cyber-attack on a vessel which caused it to collide with another vessel, leading to severe damage to the hull of the vessel suffering the attack, the losses would be covered under the war insurance. In this example, the act of terrorism is the peril, and the act is the cyber-attack; thus, the cyber-attack is a part of the peril. If, however, pirates used a cyber-attack to temporarily prevent a vessel from moving, and then physically attacked the ship, leading to a loss of cargo and personal injury to the crew, the pirates are the insured peril, but the cyber-attack might not be. In this case, the cyber-attack is the tool used, and might instead be the casualty. In both scenarios, the peril is covered, and the losses are covered; the

[128] NP Cl. 2-9.

[129] *Hull Insurance of Autonomous Ships*, *supra* note 121, at 184.

cyber incident fits in somewhere between the two. Exactly what the cyber incident is categorized as will therefore differ, and must be a fact-specific endeavor that is done on a case by case basis.

All perils from Cl. 2-9 (b) through (e) involve some intentional act. This means that any cyber accident would have to fall under Cl. 2-9 (a) to be covered under war insurance; while traditional acts of war fall under letter (a), so does "all such measures that are regularly taken by powers at war," such as extinguishing lighthouses, orders to sail without navigation lights, etc.[130] While it is difficult to imagine how cyber accidents can be the result of war in a way that triggers the liability of a war insurer, this is not excluded as a possibility. For instance, war or war-like conditions could cause the Internet to be shut down in certain places or at certain times, leading to errors of the cyber systems on a vessel. If this leads to a covered loss, and the assured is able to meet its burden in proving that the loss was suffered due to war or war-like conditions, the war insurer could still be liable for the loss.

Beyond Cl. 2-9 sub-clause 1 (a), Cl. 2-9, sub-clause 1, letter (c) seems relevant for coverage of cyber incidents. Letter (c) states that an insurance against war perils covers "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[.]"[131] We will here evaluate sabotage as an example of how cyber would fit in. According to the Commentary, sabotage means "wilful (sic) destruction which does not form part of the conduct of war, but which is connected with, for example labour (sic) conflicts."[132] The sabotage does not have to be aimed at the object insured; the fact that the action involves recoverable damage to the assured's property is sufficient.[133] The action must be in the furtherance of a specific political, social, or similar goal, see ND 1990.140 NV PETER WESSEL.[134] Destruction by the vessel's own crew as an act of vengeance or protest against the owner is considered vandalism of property, covered under the insurance for marine perils,[135] and thus falls outside the coverage of sub-clause 1, letter (c). While the Commentary does not include any discussion related to this point and cyber, it can be assumed that the use of cyber elements like a cyber-attack to carry out this vandalism will also be covered the marine insurer to the extent it leads to losses covered. In a case where for instance an environmental group launches a cyber-attack on a vessel used to transport oil to bring media attention to the climate impact of oil and the shipping industry, the elements for sabotage are

[130] Commentary to the NP, Cl. 2-9.
[131] NP Cl. 2-9 (c).
[132] Commentary to the NP, Cl. 2-9.
[133] *Id.*
[134] *Id.*
[135] *Id.*

met and a war insurer will cover any insured losses that were caused by this. Sabotage is thus the peril insured, while the cyber-attack is the means with which the peril materializes through to trigger the insurer's liability; and the casualty could be delays, damage to consumable cargo, etc.

Similarly, Clause 2-9, sub-clause 1, letter (b) might link cyber elements with coverage: the war insurance covers "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." Sub-clause 1, letter (b) "deals only with restrictions on the owner's rights in the object insured. Actions leading to an infliction of physical damage fall within the scope of general war perils set forth in sub-clause 1 (a)[.]"[136] For a cyber incident to be covered under letter (b), it must somehow restrict the owner's right in the vessel. It could be argued that a cyber-attack that inhibits the movement, communication, or navigation of a vessel could fall under the "other similar interventions" language of this clause, making it covered under the policy. To receive cover for physical damage to the ship and machinery, the peril would have to fit under the general language of letter (a).

It could be practically challenging to determine that the attack was made "by a foreign State power" and that it was "made for the furtherance of an overriding national or supranational political objective." The burden is on the assured to prove that they have suffered a loss covered by the insurance.[137] The assured is therefore left with the challenge of trying to prove the source and the intent of the attacker. In large-scale incidents, the assured might be aided by police or other government or private organizations to solve this, as other parties might also have an interest in determining the source of an attack. Where determining the source is not possible, the assured have not met their burden of proof to trigger liability of the war risk insurer. The marine insurer under the Plan should therefore cover the losses provided that there is damage to an insured object.

The above examination shows that cyber incidents are generally covered under Cl. 2-8 and can be covered under Cl. 2-9, as long as they otherwise qualify as a war peril.

4.2.3 Cargo Insurance

Cargo insurance under the CICG is, as a starting point, a casualty insurance that does not cover liability to third parties.[138] The losses covered is outlined in §6:

---

[136] *Id.*

[137] NP Cl. 2-12, sub-clause 1 and 2.

[138] *See* CICG §6.

> This insurance covers the following losses:
> 1. Total loss, cf. § 35.
> 2. Shortage, cf. § 36.
> 3. Damage, cf. § 37.
>
> [Second paragraph stating other charges the insurance covers.]
>
> Unless otherwise specially agreed, the Insurer shall not be liable for:
> 1. General capital loss, including loss of time, loss due to economic fluctuations, loss of market, operating loss and similar losses.
> 2. Liability to third parties incurred by the Assured.
>
> [Fourth paragraph about general average conditions.]

It is §6 paragraph three that defines the interest covered in the negative, by stating that general capital loss and liability to third parties is not covered. The insured interest is therefore in the economic value of the cargo, and the insurer will only be liable for the loss of or damage to the cargo as a result of a cyber incident.

Under the CICG, there are different categories of coverage the assured can choose between, called A, B, and C-Clauses. Under the most extensive coverage, A-Clauses in §3, the "insurance covers all risks of loss or damage to which the insured goods are exposed" with the exception of exclusions in clauses §§ 17, 18, and 19.[139] This is an all risk coverage, similar to the marine perils under Cl. 2-8 of the Plan.

C-Clauses in §5 cover transport accidents, defined as follows:

> Subject to the exclusions specified in §§ 17, 18 and 19, C-Clauses insurance covers the following risks to which the insured goods are exposed:
> 1. The carrying vessel having collided, struck any object, sunk, capsized, or suffered a similar serious accident.
> [2 and 3 are related to land and air transportation]
> 4. Fire, lightning or explosion.
> 5. Earthquake, volcanic eruption, landslide, snowslide or similar natural disasters.[140]

[139] CICG §3.

[140] CICG §5.

The B-Clauses cover what is referred to as extended transport accidents, as outlined in §4. This clause includes all the terms of the C-Clauses in addition to the following four:

> 6. The goods being jettisoned or washed overboard.
> 7. Sea, lake or river water entering into warehouse or place of storage.
> 8. Loading or unloading of the insured goods, resulting in the total loss of entire packages.
> 9. Loading, unloading or shifting of the insured goods in a port of distress, and theft or precipitation while the goods are stored in a port of distress.[141]

Similarly to marine H&M cover under the Nordic Plan, cargo insurance under A-Clauses will cover all cyber incidents unless they relate to the specific exclusions. While cyber incidents are not listed as a named peril in the C-Clauses, some of the named perils, like collision and striking, might have manifested itself through a cyber incident, in which case they would be covered under the C-Clauses. The same is true for B-Clauses.

Exclusions are listed in Clauses §§ 17 to 19, and include perils related to war and war like conditions, including state interference, along with storing the cargo on deck and perils related to the nature of the goods, such as natural loss in volume and issues of condensation. Most of these are not relevant for cyber incidents, with the exception of §18 no. 3.

CICG §18 no. 3 excludes loss and damage caused by "protest actions, riots, strikes, lockout, sabotage, acts of terrorism or similar occurrences, unless a special agreement regarding cover has been concluded." Of these, sabotage is especially interesting in a cyber context. Similar to the term sabotage under war insurance, "[t]he terms primarily cover the wilful destruction of objects, perpetrated for a political, social or similar purpose . . . The acts do not necessarily have to target the insured object directly."[142] Causation is also required for this exclusion to apply; the Commentary states that "[t]here must be a certain functional connection between the loss [to or of the cargo] and the action taking place."[143]

There is no further explanation of what qualifies as a political, social, or similar purpose, but from the context it likely refers to incidents beyond just personal motivation. Thus, incidents where the intent and origin of a cyber-attack or unknown, or where the source is known but the person or persons are only acting out of personal interest, the exclusion will not be triggered,

---

[141] CICG §4.

[142] Commentary to the CICG, at 33.

[143] *Id.*

and the insurer would still be liable for losses covered. Cyber security experts are frequently concerned with interference by disgruntled employees and continue to list humans as the number one reason for cyber incidents,[144] so this exception might be something we will see litigated in the future.

While both the terms of the Nordic Plan and of the CICG provide broad coverage of cyber incidents, many H&M and cargo insurers include Cyber Exclusion Clauses in their insurance contracts, which limits the losses covered in relation to cyber incidents.[145] We will now examine some of these exclusion clauses in detail to understand how they change the scope of cover for H&M and cargo insurance.

4.3 Cyber Exclusion Clauses

4.3.1 Research Question: How Do Cyber Exclusion Clauses Impact the Coverage?

While cyber coverage is included in coverage according to the language of the Plan and the CICG, insurance providers can deviate from that language in their own contracts of insurance. As such, insurance providers frequently subject their policies to Cyber Exclusion Clauses (CEC). This means that their insurance contracts exclude cyber incidents that would otherwise be covered. Some of these insurers offer to reinstate the cyber coverage, commonly referred to as Buy-Back.[146] This means that the cyber coverage will come at an additional cost and that the insurer construct the terms separately from the Plan or CICG. Many insurers use CECs to limit their own liability, as many reinsurers have incorporated CECs into their reinsurance contracts.[147] Because insurance providers are unable to reinsurance their liability for cyber risks, many chose to exclude cyber coverage from their own insurance contracts with shipowners.

---

[144] Daum, *supra* note 65, at 6-7; Iosif Progoulakis, Paul Rohmeyer & Nikitas Nikitakos, *Cyber Physical Systems Security for Maritime Assets*, 9 J. Mar. Sci. & Engineering 1, 11 (2021).

[145] JOHN DUNT, MARINE CARGO INSURANCE 252-253 (Second ed. 2016). In fact, as a response to this, Willis Tower Watson, in collaboration with Falvey Cargo Underwriting, launched the first cyber coverage for cargo in 2022. *WTW Partners with Falvey Cargo Underwriting for Affirmative Cargo Cyber Coverage Solution,* WTW (Feb. 16, 2022), https://www.wtwco.com/en-US/News/2022/02/wtw-partners-with-falvey-cargo-underwriting-for-affirmative-cargo-cyber-coverage-solution (last visited Nov. 9, 2022).

[146] As of this writing, only the Norwegian Hull Club had information about buy-back on their website, https://www.norclub.com/products-and-services/cyber-attack-exclusion-buy-back (last visited October 14, 2022).

[147] Preben B. Helverschou & Susanne Kjær Bygholm, *Norway: The Future of Cyber Cover in the Nordic Marine Insurance Markey*, MONDAYQ (Jan. 26, 2021), https://www.mondaq.com/reinsurance/201029500/the-future-of-cyber-cover-in-the-nordic-marine-insurance-market; *Hull Insurance of Autonomous Ships*, *supra* note 121, at 180.

The first widely used clause was the Institute Cyber Attack Exclusion Clause, commonly called CL.380, from 2003. While the clause was widely used with regards to insurance for vessels, it is not unique to the marine industry. The language of CL.380 reads as follows:

> 1.1 Subject only to clause 1.2 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 other electronic system.
>
> 2.1 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, Clause 1.1 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.

This clause has been phased out in recent years as it has been criticized for being ambiguous.[148] First, the language is not very precise because it does not account for how cyber accidents, being cyber incidents *not* done "as a means for inflicting harm," are to be treated.

Furthermore, the language is so broad that most modern casualties including an intent to cause harm could likely be excluded. This is because most actions done to a vessel today include some computer element. The clause excludes losses *directly* or *indirectly* linked to "any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system." There is no limit put on the word "indirectly," which leaves the term wide open for interpretation and litigation. Many other exclusions mirror this language exactly, as will be seen below. All these exclusion clauses thus face similar issues.

The language of CL.380 is incredibly broad, especially considering the addition of "any computer" and "any other electronic system." This language means that the exclusion can apply to cases where the *hardware* is the source of loss, rather than the computer system itself. A common example stems from cargo insurance: if a truck driver is robbed while transporting insured cargo and the robbers are successful in stealing the cargo because they hit the driver over the head with a laptop, a cargo insurance contract with the CL.380 exclusion would not

[148] *Id.*

cover the loss of the cargo as the laptop, a computer per the terms of the clause, was used "as a means for inflicting harm."[149]

Another example is in the instance of document fraud to conduct cargo theft. If someone creates a false bill of lading using a copying machine,[150] correction fluid, and a typewriter, there would be cover for the cargo, while a false bill of lading created using a computer system would somehow exclude cover under the same terms.[151] This makes the exclusion not just broad, but also arbitrary: the perils and losses are the same in both instances, but the mere inclusion of a computer element means the losses in the latter situation are excluded. This demonstrates how the broad language is inappropriate in such a digitalized world, as the arbitrary inclusion of a computer in the chain of causation will leave a loss uncovered which would otherwise be covered under the contract.

As a response to the above issues with CL.380, actors in the marine insurance market created two new draft clauses, the Marine Cyber Exclusion Clause, called LMA5402, and the Marine Cyber Endorsement, called LMA5403.

The language of LMA5402 reads as follows:

> This clause shall be paramount and shall override anything in this insurance inconsistent therewith.
>
> 1 In no case shall this insurance cover any loss, damage, liability or expense directly or indirectly caused by, contributed to by or arising from:
>
> 1.1 the failure, error or malfunction of any computer, computer system, computer software programme, code, or process or any other electronic system, or
>
> 1.2 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 other electronic system.

This clause has failed to limit the exclusions seen in CL.380. First of all, LMA5402 is paramount, meaning that the exclusion shall override any other language suggesting the

[149] Kao, *supra* note 61, at 486, *citing* Soyer, *supra* note 115, at 638.
[150] Assuming that a copying machine does not fall within the definition of "electronic system" in the exclusion.
[151] Chris Chatfield, *Cyber Exclusion Clauses - Are They Fit for Purpose?*, KENNEDYS LAW (June 19, 2018), https://kennedyslaw.com/thought-leadership/article/cyber-exclusion-clauses-are-they-fit-for-purpose/.

inclusion of the cyber incidents listed in the clause.[152] Secondly, this clause maintains all of the same exclusions as seen in CL.380 1.1. In fact, the language is identical. Third, LMA5402 expands the exclusion to include cyber accidents as well, as seen in the language of second paragraph 1.1, which includes failure, error, or malfunction. And fourth, LMA5402 does not include language similar to that of CL.380 2.1, which reinstates coverage under war risk insurances for cyber incidents relating to weapons and missiles. Thus, while LMA5402 in some ways is clearer than CL.380, it excludes more incidents than CL.380.

Because of the broad language of both the above clauses, many insurers are now starting to use the standard clause LMA5403, which excludes malicious cyber loss while affirming cover for cyber accidents that would otherwise be covered under the policy if not for the cyber element.[153] The draft clause reads as follows:

> 1. Subject only to paragraph 3 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, computer process or any other electronic system.
> 2. 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.
> 3. 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. (emphasis added)[154]

---

[152] LMA5402 First paragraph, found at LMA5402 - Marine Cyber Exclusion, LLOYD'S MARKET ASSOCIATION (2019), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx.

[153] *Marine Cyber Risk and Insurance*, HOWDEN GROUP (Nov. 6, 2020), https://www.howdengroup.com/ae-en/marine-cyber-risk-and-insurance-howden (last visited Nov. 6, 2022).

[154] LMA5403 - Marine Cyber Endorsement, LLOYD'S MARKET ASSOCIATION (2019), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx.

Similar to CL.380 and LMA5402, LMA5403 excludes coverage for cyber incidents "as a means for inflicting harm." It differs from the other clauses significantly, however, by explicitly stating that cyber accidents, being cyber incidents "not as a means for inflicting harm," are still covered under the insurance contract. As an example, this means that a H&M insurance with LMA5403 clause would still cover the losses if a software update in the bridge system caused a malfunction of the navigational charts, leading the vessel to ground and sustain elaborate damage to the hull. As seen above, CL.380 remained silent with regards to cyber accident, while LMA5402 explicitly excludes coverage for cyber accidents. Insurance contracts with LMA5403 as the cyber exclusion clause will therefore have wider coverage of claims than a contract with CL.380 or LMA5402.

4.3.2 Coverage for Contracts with Cyber Exclusion Clauses

The inclusion of a CEC in a contract of insurance based on the Nordic Plan or the CICG will limit the coverage for cyber incidents significantly. The language of the CECs does not refer to perils or casualties, but rather to the losses covered. It is not the peril or the casualty themselves that are excluded, but the losses arising from them. This means that cyber incidents materializing both as perils, such as a spoofing attack, and as casualties, for example someone using a cyber system as a means of sabotage, will exclude liability for the insurer. Most H&M marine and cargo insurance contracts today include a cyber exclusion clause, often one of the three examined above.

The approach to CECs is not so uniform when it comes to war insurance providers in Norway. One large provider of both H&M and war policies, Norwegian Hull Club, excludes cyber-attacks from its standard contracts[155] but offers a Cyber-Attack Exclusion Buy-Back.[156] The other large provider, Den Norske Krigsforsikring for Skib (DNK), has chosen not to limit cyber coverage. In fact, DNK provides a slightly extended cyber coverage in its insurance contract by offering a limited cover for damages caused by marine cyber risks, normally covered under Cl. 2-8, to the extent that these risks are excluded from the marine cover.[157] The clause states:

---

[155] While the contract terms are not public, it can be interfered that only attacks are excluded because (1) of the nature of war risk, which generally requires intentional acts for a peril to fall under its coverage, and (2) the name of the Buy-Back is called "cyber-attack exclusion buy-back," indicating that only cyber-attacks were excluded in the first place.

[156] *See* Cyber-Attack Exclusion Buy-Back, NORWEGIAN HULL CLUB, https://www.norclub.com/products-and-services/cyber-attack-exclusion-buy-back (last visited October 14, 2022).

[157] *Hull Insurance of Autonomous Ships*, *supra* note 121, at 183, referencing Den norske krigsforsikring for skib – The Norwegian Shipowners' Mutual War Risks Insurance Association, Conditions of 1 January 2019, Cl. 15.1.

15 Additional Limited Cover for Marine Cyber Attacks ("ALC Marine Cyber Attack")

15.1 Perils covered

This ALC Marine Cyber Attack covers total loss (including hull interest/freight interest) and physical damage directly caused by or contributed to 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 computer process or any other electronic system.

This ALC Marine Cyber Attack covers against marine perils cf. the Plan Cl. 2-8. Cover against Cyber Attacks caused by war perils cf. the Plan Cl. 2-9, is available under the Associations regular war risk insurance.

15.2. Losses covered under this ALC Marine Cyber Attack

This ALC Marine Cyber Attack covers total loss (including hull interest/freight interest) and physical damage only, cf. the Plan Chapter 10-12 and the Plan Cl. 15-2 (a), always subject to Cl. 15.1 above.

This ALC Marine Cyber Attack does not cover the insured member's loss to the extent it is recoverable under any other insurance.[158]

The above language is limited to total loss and physical damage to the ship and does not include limited liability imposed on the assured as the result of striking or collision as normally covered under H&M insurances.[159] The intent of this is to eliminate problems associated with finding the source of a cyber-attack, by covering cyber-attacks regardless of the source if no other insurance covers it. The clause also confirms that cyber incidents are covered under the Nordic Plan, by referring to the perils in Cl. 2-8 and 2-9. Coverage for cyber incidents under war insurance will therefore be according to the Nordic Plan, either automatically through DNK or by purchasing the Buy-Back from Norwegian Hull Club.

[158] Cl. 15, Conditions of 1 January 2022, Den Norske Krigsforsikring For Skib.

[159] *See* NP Cl. 13-1.

The below table summarizes the findings from Chapter 4 thus far.

Risk/casualty	Marine H&M & cargo*	War **	CL.380	LMA5402	LMA5403
Computer virus	Covered	Covered	Not covered	Not covered	Not covered
GPS jamming or spoofing	Covered	Covered	Not covered	Not covered	Not covered
AIS interference	Covered	Covered	Not covered	Not covered	Not covered
OT interference	Covered	Covered	Not covered	Not covered	Not covered
Cyber accident (software error, wrong updates, user error, etc.)	Covered	Generally not covered	Unclear	Not covered	Covered
* Based on the A-Clauses ** Depends on the source of the attack, as evaluated above					

Table 3 – *Coverage under standard clauses and CECs*

4.4 Protection and Indemnity

We will now look at cyber risks under protection and indemnity (P&I) insurance. In contrast to H&M and cargo insurance, which are first party property insurances, P&I insurance covers legal liabilities that arise by means of contracts, in tort, or under other statutory obligations of the assured.[160]Any limitation of cyber incidents under P&I insurances would be significant, as the scope of the coverage is broad.

Terms for P&I coverage are not included in the Nordic Plan. We will therefore base our analysis on the terms of the individual P&I insurance terms. The terms of the different P&I insurers are generally quite similar. This is because the 13 insurers who are a part of the International Group of P&I Clubs generally cooperate to get the same reinsurance contract, and they are connected through the Pooling Agreement and the International Group Agreement,[161] which are essential to spread large financial risks across the Clubs.[162] To make sure the terms of the individual insurers align with their shared reinsurance contract, they thus generally cooperate on the language of the terms offered to shipowners.

[160] EDGAR GOLD, GARD HANDBOOK ON P&I INSURANCE 115 (5th ed. 2002)[hereinafter GARD HANDBOOK].

[161] *Id.* at 105.

[162] *Id.* at 71.

P&I clubs cover risks under the named perils principle, meaning that "only those liabilities and losses that are identified in P&I club rules are covered."[163] The principal types of liabilities and losses covered by P&I insurance are:

i. Liability arising from carriage of cargo.
ii. Pollution liability.
iii. Liability for death of or injury to crew members, passengers and others, such as stevedores, on board ships.
iv. Damage to fixed and floating objects and other property.
v. Such part of the liability for collision damage that is not covered under the ship's hull policy.
vi. The excess liability arising out of a collision, including that which is in excess of the limit of the hull policy.
vii. Wreck removal.[164]

To examine the cyber coverage under P&I insurance, will limit this exploration to the terms contained in the general policy terms of the two Norwegian P&I providers that are members of the International Group, namely Gard and Skuld.

In Skuld's fixed terms for shipowner, clause 25.1.18 states that "[t]he Insurance shall not cover the *Assured* for any liabilities, losses, expenses or costs which arise out of or in respect of . . . *Chemical, Bio-Chemical, Electromagnetical Weapons* and *Computer Risks*[.]"[165] Chemical, Bio-Chemical, Electromagnetical Weapons and Computer Risks are defined in Appendix 1 as follows:

> Loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from
> i) any chemical, biological, bio-chemical or electromagnetic weapon
> ii) the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.[166]

Furthermore, Skuld has expressly stated in their Optional Covers Terms & Conditions that any optional P&I cover from them "shall not cover the Assured for any liabilities, losses,

---

[163] *Id.* at 114.

[164] *Id.* at 114-115.

[165] Skuld Owners' Fixed P&I Terms & Conditions, as of 20 February 2022, https://www.skuld.com/contentassets/3f2bd77d4a1d434f8aa44efcb37438dc/2022_skuld_owners_fixed_pi_tc.pdf.

[166] *Id.* at Appendix 1.

expenses or costs directly or indirectly caused by or contributed to by or arising from . . . the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."[167]

Skuld therefore excludes cyber-attacks from its main coverage, and does not offer a buy-back to close the coverage gap. The language mirrors that of the cyber exclusion clauses which firmly excludes cyber incidents "as a use of inflicting harm." Nothing is said about whether cyber accidents remain covered. While it can be inferred that all acts that fall outside the "as a means of inflicting harm" remain covered, the terms of the insurance contract have not made this clear. This is especially noteworthy as clause LMA5403, which reaffirms coverage for non-malicious acts that would otherwise be covered but for the exclusion clause, is commonly used in other marine insurance policies. Due to the widespread use of LMA5403 and the level of sophistication of the company, one can only assume that Skuld has actively chosen not to mirror the language of LMA5403. The status of cyber accidents thus remains unclear.

While Gard has similar coverage to Skuld, the exclusion of cyber risks is worded significantly different. The language used by Gard is as follows:

> The Association shall not be liable for any losses, liabilities, costs or expenses directly or indirectly caused by or contributed to by or arising from:
> i. any chemical, biological, bio-chemical or electromagnetic weapon;
> ii. the use or operation, as a means for inflicting harm, of any computer virus;
> iii. Clause 4 (ii) above will not operate to exclude losses (which would otherwise be covered under the terms of this policy) 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 missil.[168]

On the following page, the cover for cyber incidents is reinstated on very specific terms relating to injury, illness, or death of any seaman, and for legal costs and expenses incurred when attempting to avoiding or minimizing liability:

---

[167] Part 3, 3.1, Skuld Optional Covers Terms & Conditions, as of 20 February 2022, https://www.skuld.com/contentassets/4b6729a9be4a4ab5bf41669c8126492d/2022_skuld_optional_covers_tc.pdf.

[168] Appendix 1, Clause 4, Gard Rules 2022, https://www.gard.no/Content/33063275/cache=20221803124344/Gard%20Rules%202022_web.pdf; *see also* Gard Additional Covers, Terms and Conditions 2022, https://www.gard.no/Content/33146286/cache=20222102083904/Gard_Additional_covers_Terms_and_Conditions_2022.pdf.

1.1 Subject to the terms and conditions set out herein, cover is extended to include the liability of the Member:

a to pay damages, compensation or expenses in consequence of the personal injury to or illness or death of any seaman . . .

b for the legal cost and expenses incurred solely for the purpose of avoiding or minimizing any liability or risk insured by the Association (other than the Omnibus Rule)

1.2 where such liability would be recoverable under either

a cover provided by the Association for such liabilities, costs, losses and expenses as would be covered under the Rules for Ships but for the exclusion of war risks in Rule 58 of the Rules for Ships; or

b any other policy of insurance providing equivalent cover

1.3 save only for the operation of an exclusion of liabilities, costs, losses and expenses directly or indirectly caused by or contributed to by or arising from . . .

b the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any other electronic system[.][169]

The above language will only reinstate coverage where there has been an injury, illness, or death of a seaman, or the assured has incurred expenses solely for the purpose of avoiding or minimizing liability or risk insured where a computer virus has been the cause of such loss. A similar reinstatement of coverage is not included in the standards terms or additional coverage provided by Skuld.

The fact that the general Gard exclusion only refers to "any computer virus" is noteworthy. The limited language means that any other malicious cyber-attack which do not necessarily rely on a virus to work, such as spoofing or jamming, would still be covered under the policy. Similarly, any losses covered caused by a cyber accident will still remain covered. The use of this language might have been an oversight or issue due to a lack of understanding of the complexities of the maritime cyber vulnerabilities. However, both the standard coverage of offshore units[170] and the Additional Cover Terms[171] include the LMA5403 Cyber endorsement clause in its entirety, making it clear that Gard is aware of the expanded language. Due to the use of a

[169] Gard Rules 2022, Appendix 1, at 105.

[170] Gard Rules 2022, Appendix III, Marine Cyber Endoresement, ref. Rule 40.3 Rules for Mobile Offshore Units

[171] Gard Rules 2022, Section 24 paragraph 2 (2), excluding cyber by referring to the Marine Cyber Endorsement clause, listed in its entirety in Appendix 7.

standard CEC other places in the policy, the limitation of the exclusion to cover computer viruses only must be seen as intentional.

It is worth mentioning that both Skuld and Gard place their cyber limitation clauses with their exclusion of coverage for losses arising from biological, chemical, bio-chemical, and electromagnetic weapons.[172] While this does not have an impact on the exclusions themselves, it does indicate that cyber incidents are still considered to be incredibly rare and uncertain situations. While this is true to some extent, there is still a lot the assured can do to minimize the risk of cyber incidents, and as the number of cyber incidents keeps increasing, the risks are becoming more real to the assured.

To conclude, the cyber exclusions in the respective policies mean that losses due to cyber-attacks are not covered by Skuld, and losses due to computer viruses are not covered by Gard, with the narrow exception related to bodily injury and costs to minimize or avoid losses as outlined above. Cyber accidents remain covered for both.

4.5 "As a Means of Inflicting Harm" – Identifying the Malicious Actor

All the CECs include the language "as a means of inflicting harm" as a qualifier for exclusion of coverage. In the context of cyber incidents, it can be challenging to determine whether the act has been conducted "as a means of inflicting harm." First, it is generally difficult to find the source of a cyber-attack; efforts at identifying the source are costly and does not guarantee success.[173] Second, it is difficult to show that a cyber-attack was conducted "as a means of inflicting harm."

The burden of proving that the assured has suffered a covered loss falls on the assured, while the burden of proving that an exclusion applies falls on the insurer.[174] Since cyber-attacks fall under the exclusions examined above for H&M, cargo, and P&I insurance, it will be the insurer's responsibility to show that the cyber-attack was conducted as a means of inflicting harm. The burden falls on the assured in the case of war insurance.

It will likely be difficult, if not impossible, for the insurer to prove that the cyber-attack was conducted as a means of inflicting harm as the language stands today. This can, however, be changed by inserting a burden of proof clause that shift the burden onto the assured to show

---

[172] Gard Rules 2022, appendix 1, Clause 4; Skuld Owners' Fixed P&I Terms & Conditions 25.1.18.

[173] Kao, *supra* note 61, at 472; Helverschou & Bygholm, *supra* note 147.

[174] NP Cl. 12-11 first sentence, "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"; *see* NP Cl. 2-12 second sentence, "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."

that the attack was *not* conducted as a means of inflicting harm. This would be fair, as it is reasonable to assume that the mere fact that someone has gained unlawful access to the computer systems means they intend to inflict harm, regardless of what the person actually does with that access. To even out the burden of finding the source of the cyber incident, I suggest that the insurer should bear the reasonable costs associated with finding the source of a cyber incident, regardless of whether the outcome shows that they are liable for the losses resulting from the incident overall. This could also be regulated in the conditions of the insurance.

In the case of war insurance, the assured will still have to prove that the source of the attack comes from one of the named perils in the coverage. The burden will thus remain on the assured.

4.6 Duties of the Assured

The above discussion has been related to the duties and liabilities of the insurer towards the assured, but the assured also has duties towards the insurer which can impact the cyber coverage. Most importantly, the assured has a duty towards the insurer to adhere to safety regulations.[175] If the assured breaches a safety regulation, "the insurer shall only be liable to the extent that the loss is not a consequence of the breach, or that the assured has not breached the safety regulation through negligence."[176] The Nordic Plan specifically mentions the creation of the Safety Management System as a safety regulation that needs to be adhered to.[177]

Starting in 2021, all vessels must incorporate cyber security in their Safety Management System (SMS) upon the system's next review.[178] This is significant for two reasons. First, it means that more shipowners are considering cyber security where they might not have before. In Norway, cyber security risks in the maritime sector are perceived as a "standalone risk element to be dealt with by IT professionals."[179] This is contrary to considering cyber security as "another risk factor, part of the overall aggregated risk affecting maritime transport operations,"[180] which is what the incorporation into the SMS is trying to achieve. While there are no universal code or standard that must be met, this requirement brings cyber security into the

---

[175] NP Cl. 3-22, Cl. 3-25; CICG §21; Skuld does not use the same language but has similar provisions in Rule 24.6 of the Owner's Fixed Terms; Gard in Rule 8.1 (f).

[176] NP Cl. 3-25; CICG § 21 second paragraph, which reads: "If a safety regulation is infringed, the Insurer shall only be liable to the extent that it is proved that the loss is not a consequence of the infringement or that the infringement cannot be imputed to the Assured"; Skuld in Rule 24 second paragraph; Gard in Rule 8.3.

[177] NP Cl. 3-22.

[178] Int'l Maritime Org. [IMO] Res. MSC.428(98) (June 16, 2017).

[179] Stavros Karamperidis, Chronis Kapalidis & Tim Watson, *Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches*, 9 J. MAR. SCI. & ENGINEERING 1, 5 (2021).

[180] *Id.*

discussion of general risk assessment and safety protocols of the ship. To meet these safety standards, shipowners likely have or will have an obligation to appropriately train their crew on cyber hygiene and basic ways of identifying cyber incidents.

Second, the incorporation of cyber security into SMSs can alter the liability of the insured to the assured. This is because an insurer is not liable for losses resulting from an otherwise covered cyber event if the shipowner did not properly create or follow the cyber related safety protocols.[181] This will likely increase how seriously shipowners take their cyber security, as the potential consequence of not doing so can limit or exclude insurance coverage. The insurance coverage will only be excluded to the extent the losses are caused by the breach of safety protocol. In this instance, that must mean that the assured would not have suffered the loss if they had properly incorporated cyber security in their SMS.

4.7 Conclusion

To conclude, the risks posed by maritime cyber incidents are often excluded in current Norwegian marine insurance contracts. That is, the coverage of cyber incidents in the Nordic Plan and CICG is quite broad but is frequently limited through the use of Cyber Exclusion Clauses. These clauses vary in terms of what the exclude, and as a result, it is difficult to compare the coverage provided by different contracts. Similarly, there are large differences in P&I coverage for cyber incidents, as the terms vary between the clubs. It might therefore be more accurate to say that the coverage of cyber risks is broad in the Norwegian marine insurance market, but that the coverage is severely limited through individual insurance contracts.

The next section will evaluate some potential ways to protect shipowners who are left with limited or no cyber coverage.

[181] *See* note 174, remembering that cyber security is part of safety regulations.

5 Covering the Gaps – Potential Solutions

We can now look at options for covering the gaps in coverage. We will evaluate first whether there is a need for separate cyber coverage for vessels, keeping the current coverage in mind. Next, we will evaluate whether the gap can be closed by getting a general cyber insurance policy, before looking at the option of getting maritime insurance outside of Norway to cover the gaps. Lastly, we will look at non-insurance options, like allocating resources to training and better equipment, along with more information sharing.

5.1 Insurance options

5.1.1 Is There A Need For Separate Cyber Coverage For Vessels?

Since cyber is now incorporated into the general risk assessment of the vessel through SMS, cyber coverage should similarly be incorporated into the general policies. Cyber is now a part of the overall risk assessment for the vessel, and it does not make sense to extract that risk to provide a separate coverage for it. Cyber issues are now an integral part of the risk of every vessel, like navigational error or the potential for collision, and the maritime insurance market is best equipped to cover these issues.

In the alternative, insurers should consider offering the shipowner to buy back the coverage that has been excluded in the general policy. In these scenarios, it is important that the insurance providers take additional care in clarifying the terms and the coverage, and that they at a minimum cover incidents the assured would assume covered under the normal insurance policy for the vessel. The different insurance providers should also come together and create more uniform terms and definitions for use in the market. It would also greatly benefit the assured if all insurances that provide cyber coverage have the adequate personnel or third-party partnership to aid through cyber incident and preparedness, so that the shipowner gets the help they need in this very niche field both before, during, and after a cyber incident.

5.1.2 International Maritime Insurance Markets

The Norwegian maritime insurance market does not adequately protect the economic value and liabilities of a vessel subject to a cyber incident. Shipowners could therefore consider looking outside of the Norwegian market to find policies for their vessels that also cover their cyber needs. As mentioned earlier, the Norwegian maritime insurance market is a bit of a legal fiction, as the maritime insurance market by its very nature is international. As such, someone looking for insurance of a vessel generally has a lot of flexibility and freedom to shop around. There might be insurance companies established in other jurisdictions that offer more suitable coverage for vessels.

More comprehensive cyber coverage can be bought independently from, for instance, The West of England Ship Owners Mutual Insurance Association,[182] Beazley,[183] Aastara Group,[184] and SIGCo Group.[185] All of these offer some type of vessel cyber product, which is meant to fill gaps in other insurance policies, or to be combined with their general policies which are subject to Cyber Exclusion Clauses.

There are a few drawbacks to purchasing independent cyber coverage in another market. First, while offers like the ones above might be exactly what a shipowner need, it is on the shipowner to ensure that the purchased coverage covers all the gaps they need covered. Because some markets allocate risks differently between the different types of insurances, assureds should take great care in ensuring that they are actually filling the gaps they believe they are filling by purchasing independent products.

Furthermore, shipowners who are accustomed to dealing with Norwegian insurance providers should be cautious when going abroad for coverage. Both the Norwegian business model and legal system are quite different than many others and is generally more favorable to the insured than in many places. This is something to keep in mind when negotiating and relying on the terms of contracts with foreign insurance providers.

5.1.3 The General Cyber Insurance Market

We can also look to the general cyber insurance market and evaluate whether seeking out insurance there is feasible to shipowners.

The general cyber insurance market is new and not well established on the insurance scene.[186] Many of the same issues faced in relation to cyber risks in the maritime insurance market is general for all cyber insurances. For instance, many businesses do not see the point in paying the high premiums for cyber coverage, nor do they understand the terms of the policies and the obligations on the business itself to ensure any incident will be covered.[187]

---

[182] https://www.westpandi.com/products/cyber-security/.

[183] https://www.beazley.com/en-001/node/134/cyber-defence-marine.

[184] https://astaaragroup.com/underwriting-for-shipowners.

[185] https://www.sigcogroup.com/services-products/cyber-hull-insurance.php; https://www.sigcogroup.com/services-products/cyber-loh-insurance.php.

[186] Nir Kshetri, *The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis*, 44 TELECOMM. POL'Y 1, 12 (2020); ARMSTRONG ET AL., *supra* note 8, at 3.

[187] Hayretdin Bahşi, Ulrik Franke & Even Langfeldt Friberg, *The Cyber-Insurance Market in Norway*, 28 INFO. & COMPUTER SECURITY 54, 55 (2019).

Because of the interconnectedness between the IT systems on many vessels and the onshore offices of the shipowners or operators, many companies can do well in acquiring general cyber insurance for their onshore operations. Because information is often set up to flow from the vessel (for example data and readings from sensors), the IT systems in the offices of a shipowner or operator might be affected if the vessel's IT systems are affected due to a cyber incident. Any cyber incident at the business site of shipping company can lead to major disruption and significant economic losses.[188]

However, shipowners will likely not find what they need for adequate coverage of their vessels in the general cyber insurance market. The general cyber insurance market does simply not have the knowledge and expertise to give shipowners the help they need in properly insuring and securing the vessels. There is already a general resistance towards stand-alone cyber insurance policies, as many assureds wish to have cyber included as part of existing coverage with an insurer that already knows its risk exposure.[189] This problem would only increase with shipowners seeking cyber insurance for their vessels, as there are already another layer of complexity and practical know-how. Even if a cyber insurer were to offer coverage for vessels, this should be looked at with great skepticism, as there is a need for a certain level of technical understanding and support from the insurer to the assured.

5.2 Non-insurance Options

Regardless of whether the economic interests of the vessel are covered under the currenty insurance contracts, there are numerous things a shipowner could and should do to increase the vessel's cyber security and decrease the chances of both the occurrence of and the impact of cyber incidents.

5.2.1 Security Measures and Training

One non-insurance option is to strengthen the technical security and training of crew. While strengthening the cyber security of a business or vessel does not in any way guarantee that the vessel will not suffer a cyber incident, it can be effective in making the vessel much more secure.[190]

---

[188] Soyer, *supra* note 115, at 630-631.

[189] PER HÅKON MELAND ET AL., FACING UNCERTAINTY IN CYBER INSURANCE POLICIES 4-5 (2017); Middleton & Kazamia, *supra* note 118, at 195.

[190] Ulrik Franke, *The Cyber Insurance Market in Sweden*, 68 COMPUTERS & SECURITY 130, 131 (2017); Daum, *supra* note 65, at 11.

In the maritime industry, it is recommended that shipowners first spend resources on training staff on cyber security measures.[191] In order to prevent cyber accidents and untargeted cyber-attacks, the crew and managers of the vessel need some elementary education in cyber-security and cyber hygiene.[192] Crew members have varied levels of IT skills, are generally unresponsive to cyber threats, and do not know what to do if they are attacked.[193] As human failures are considered the main cause of successful cyber-attacks,[194] this should be considered a high priority item. Experts recommend that crew learn how to recognize certain cyber-attacks or failures, such as jamming attacks, and that there are practices or checklists for how to mitigate the damage as it is occurring.[195]

Despite this focus on training, more than half of the chief information officers in a survey of the shipping industry would rather invest in systems than crew competence and expertise.[196] While this is important, it makes it easy for shipowners to believe that making the vessel secure against cyber incidents is something that can be done once and not thought about again. In reality, cyber vulnerabilities are changing rapidly, and any plan, training, or technology needs to be continuously updated in order to remain useful.[197]

5.2.2 Information Sharing

The whole maritime sector could greatly benefit from sharing information and resources on the topic of cyber security. The maritime sector is generally great at cooperating on known or suspected safety issues and do a lot to self-regulate and ensure safety of the vessel and its crew and the cargo. Cyber issues are still fairly new and intangible in ways that makes it difficult for many to understand the importance of the incidents they might face. This might come with time, but it might also need some actors, whether that is shipowners, associations, insurers, or the legislature, to start the process before others will follow.

There are efforts at increasing the flow of information. In academia, it should be noted that there are current PhD projects focused on cyber information sharing in the maritime sector. Outside academia, there are more efforts to centralize information about maritime cyber

---

[191] Simon Cooper, *Cyber Risk, Liabilities and Insurance in the Marine Sector, in* MARITIME LIABILITIES IN A GLOBAL AND REGIONAL CONTEXT 103, 107 (Barış Soyer & Andrew Tettenborn eds., 2019); T P Avanesova et al., *Analysis of Cyber-Security Aspects Both Ashore and at Sea*, 872 IOP CONF. SERIES: EARTH & ENVTL. SCI. 1, 2 (2021); Daum, *supra* note 66, at 18.

[192] Avanesova et al., *supra* note 190, at 2.

[193] Daum, *supra* note 66, at 6-7; McGillivary, *supra* note 76, at 47.

[194] Daum, *supra* note 66, at 6-7.

[195] Tam & Jones, *supra* note 3, at 15-16.

[196] Avanesova et al., *supra* note 190, at 4.

[197] Daum, *supra* note 66, at 18; Tucci, *supra* note 5, at 123.

services and information. There has for instance been the establishment of the CSO Maritime Cyber Alliance, which aims to share security related information.[198]

Furthermore, DNK and the Norwegian Shipowner's Association jointly founded NORMA Cyber, the Norwegian Maritime Cyber Resilience Centre, in 2021. NORMA Cyber "delivers [centralized] cyber security services to Norwegian shipowners and other entities within the Norwegian maritime sector" and "aims to be the leading hub for operational cyber security efforts within the Norwegian maritime sector."[199] NORMA Cyber provides its members with intelligence, including warnings and vulnerability notifications, intelligence reports, and seminars, as well as response, including crisis response advice, cyber response exercises, and resource management.[200]

5.3 Conclusion

As seen above, there are a variety of different options for shipowners who feel their standard insurance policies are insufficient with regards to coverage of cyber incidents. What each shipowner chooses to do will be based on their needs, their appetite for risk, their sophistication with the international maritime insurance market, and the resources, including finances, available to them.

[198] The Norwegian Hull Club and DNK are amongst the partners of the CSO Alliance, ARMSTRONG ET AL., *supra* note 8, at 139.

[199] *About*, NORMA CYBER, https://www.normacyber.no/en/about (last visited Nov. 24, 2022).

[200] *Services*, NORMA CYBER, https://www.normacyber.no/en/services (last visited Nov. 24, 2022).

6 Conclusion

This brings us back to our original research questions: **how are cyber risks covered in the current Norwegian maritime insurance market?** After the above analysis, it is clear that cyber risks encompass more than just cyber perils; cyber incidents can manifest themselves as perils, casualties, and losses covered. Furthermore, it is now clear that these cyber incidents are treated quite differently under the standard clauses is than they are in practice because of the incorporation of cyber exclusion clauses. The reality is thus that cyber risks are generally excluded or severely limited by Norwegian maritime insurance contracts. Because the language used to exclude cyber risks is often overbroad, the effect of these exclusions impacts more of the perils traditionally insured than perhaps intended. Furthermore, the exclusions fail to recognize how cyber security is now an integral part of the overall risk assessment of a vessel and is not a stand-alone concern to be excluded in broad strokes.

As such, we have also identified a few other options for shipowners who want to move beyond the coverage in the Norwegian maritime insurance market. There are some potential options in other insurance markets, including foreign maritime markets and the general cyber insurance market. Furthermore, there are non-insurance options that shipowners can and should take advantage of in order to decrease the risk of cyber incidents, including training of crew, information sharing with others in the sector, and technical security measures.

Overall, insurers are cautious to cover cyber risks in the Norwegian maritime insurance market. Because of its history and widespread use, starting with change in the Nordic Plan can help guide the Norwegian and perhaps international maritime insurance market towards a more comprehensive understanding of cyber risks faced by vessels. Thus, there can hopefully be significant improvements done to this before the next revision of the Nordic Plan, so that a more comprehensive approach to cyber incidents can be incorporated into the conditions.

Table of References

Legal sources

Commentary to the CICG, https://cefor.no/clauses/cargo-clauses/ (click “English version” under subtitle “Commentary to Norwegian Cargo Clauses”).

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

Conditions of 1 January 2022, Den Norske Krigsforsikring For Skib.

Conditions relating to Insurance for the Carriage of Goods of 1995, Version 2004 [CICG], https://cefor.no/globalassets/documents/clauses/norwegian-cargo-clauses/cefor-cargo-clauses-261-2004-eng.pdf.

Forskrift om finansforetak og finanskonsern (finansforetaksforskriften [FOR] 2016:1502) (Nor.); FOR-2016-12-09-1502.

Forskrift om forsikringsavtaler (forsikringsavtaleforskriften [FOR] 2022:323) (Nor.); FOR-2022-03-04-323.

Gard Additional Covers, Terms and Conditions 2022, https://www.gard.no/Content/33146286/cache=20222102083904/Gard_Additional_covers_Terms_and_Conditions_2022.pdf.

Gard Rules 2022, https://www.gard.no/Content/33063275/cache=20221803124344/Gard%20Rules%202022_web.pdf.

Institute Cyber Attack Exclusion Clause, CL.380 (2003).

Int’l Maritime Org. [IMO] 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.

Int’l Maritime Org. [IMO] Res. MSC.428(98) (June 16, 2017).

LMA5402 - Marine Cyber Exclusion, LLOYD'S MARKET ASSOCIATION (2019), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx.

LMA5403 - Marine Cyber Endorsement, LLOYD'S MARKET ASSOCIATION (2019), https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx.

Lov of Forsikringsavtaler (Insurance Contract Act [ICA] 1989:69) (Nor.); LOV-1989-06-16-69.

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

Nordic Plan Agreement of 2010, with Addendum 2019, https://cefor.no/globalassets/documents/clauses/nordic-plan/agreement-nordic-plan-03-11-2010---amended-09-12-2016-with-addendum-1-21-08-2019.pdf.

Skuld Owners' Fixed P&I Terms & Conditions, as of 20 February 2022, https://www.skuld.com/contentassets/3f2bd77d4a1d434f8aa44efcb37438dc/2022_skuld_owners_fixed_pi_tc.pdf.

Skuld Optional Covers Terms & Conditions, as of 20 February 2022, https://www.skuld.com/contentassets/4b6729a9be4a4ab5bf41669c8126492d/2022_skuld_optional_covers_tc.pdf.

SOLAS regulation V/19.2.4, Carriage Requirements for Shipborne Navigational Systems and Equipment, as amended by Resolution A.1106(29).

Journal articles

Avanesova T P et al., *Analysis of Cyber-Security Aspects Both Ashore and at Sea*, 872 IOP CONF. SERIES: EARTH & ENVTL. SCI. 1 (2021).

Awan, Malik Shahzad Kaleem & Al Ghamdi, Mohammed A., *Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS)*, 7 J. MAR. SCI. & ENGINEERING 1 (2019).

Bahşi, Hayretdin, Franke, Ulrik & Friberg, Even Langfeldt, *The Cyber-Insurance Market in Norway*, 28 INFO. & COMPUTER SECURITY 54 (2019).

Daum, Oliver, *Cyber Security in the Maritime Sector*, 50 J. MAR. L. & COM. 1 (2019).

Erstad, E., Ostnes, R. & Lund, M.S., *An Operational Approach to Maritime Cyber Resilience*, 15 INT'L J. ON MARINE NAVIGATION AND SAFETY OF SEA TRANSP. 27 (2021).

Franke, Ulrik, *The Cyber Insurance Market in Sweden*, 68 COMPUTERS & SECURITY 130 (2017).

Hareide, Odd Sveinung et al., *Enhancing Navigator Competence by Demonstrating Maritime Cyber Security*, J. NAVIGATION 1 (2018).

Jensen, Lars, *Challenges in Maritime Cyber-Resilience*, 5 TECH. INNOVATION MGMT. REV. 35 (2015).

Kao, M. Bob, *Cybersecurity in the Shipping Industry and English Marine Insurance Law*, 45 TUL. MAR. L.J. 467 (2021).

Karahalios, Hristos, *Appraisal of a Ship's Cybersecurity efficiency: the case of piracy*, 13 J. TRANSP. Security 179 (2020).

Karamperidis, Stavros, Kapalidis, Chronis & Watson, Tim, *Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches*, 9 J. MAR. SCI. & ENGINEERING 1 (2021).

Kshetri, Nir, *The Evolution of Cyber-Insurance Industry and Market: An Institutional Analysis*, 44 TELECOMM. POL'Y 1 (2020).

Kugler, Logan, *Why GPS Spoofing Is a Threat to Companies, Countries*, 60 COMM. ACM 18 (2017).

McGillivary, Phil, *Why Maritime Cyberseucirty is an Ocean Policy Priority and How it Can Be Addressed*, 52 MAR. TECH. SOC'Y J. 44 (2018).

Progoulakis, Iosif, Rohmeyer, Paul & Nikitakos, Nikitas, *Cyber Physical Systems Security for Maritime Assets*, 9 J. Mar. Sci. & Engineering 1 (2021).

Tam, Kimberly & Jones, Kevin, *Maritime Cybersecurity Policy: the Scope and Impact of Evolving Technology on International Shipping*, J. CYBER POL'Y (2018).

Books, chapters, and reports

ARMSTRONG, DEAN, STEWARD, THOMAS & THEKERAR, SHYAM, CYBER RISKS AND INSURANCE: THE LEGAL PRINCIPLES (2021).

BOYES, HUGH & ISBELL, ROY, INSTITUTION OF ENGINEERING AND TECHNOLOGY UK, CODE OF PRACTICE: CYBER SECURITY FOR SHIPS (2017).

Cooper, Simon, *Cyber Risk, Liabilities and Insurance in the Marine Sector, in* MARITIME LIABILITIES IN A GLOBAL AND REGIONAL CONTEXT PAGE (Barış Soyer & Andrew Tettenborn eds., 2019)

DIRENZO, JOSEPH, GOWARD, DANA A. & ROBERTS, FRED S., THE LITTLE-KNOWN CHALLENGE OF MARITIME CYBER SECURITY (2015).

DUNT, JOHN, MARINE CARGO INSURANCE (Second ed. 2016).

FALKANGER, THOR, BULL, HANS JACOB & BRAUTASET, LASSE, SCANDINAVIAN MARITIME LAW: THE NORWEGIAN PERSPECTIVE (4th ed. 2017).

GOLD, EDGAR, GARD HANDBOOK ON P&I INSURANCE (5th ed. 2002).

Kennedy, Rónán, *Doctrinal Analysis: The Real 'Law in Action', in* LEGAL RESEARCH METHODS: PRINCIPLES AND PRACTICALITIES 21 (Laura Cahillane & Jennifer Schweppe eds., 2016).

LUND, MASS SOLDAL ET AL., INTEGRITY OF INTEGRATED NAVIGATION SYSTEMS (2018).

MELAND, PER HÅKON ET AL., FACING UNCERTAINTY IN CYBER INSURANCE POLICIES (2017).

Middleton, Kirsty & Kazamia, Maria, *Cyber Insurance: Underwriting, Scope of Cover, Benefits and Concerns, in* THE "DEMATERIALIZED" INSURANCE 185 (Pierpaolo Marano et. al. ed., 2016).

NORMA CYBER, ANNUAL THREAT ASSESSMENT 2022, 8 (2022).

SALTER, MICHAEL & MASON, JULIE, WRITING LAW DISSERTATIONS (2007).

Soyer, Baris, *Cyber Risks Insurance in the Maritime Sector: Growing Pains and Legal Problems, in* MARITIME LAW IN MOTION 627 (Proshanto K. Mukherjee et al. ed., 2020).

Tucci, Andrew E., *Cyber Risks in the Marine Transportation System*, *in* CYBER-PHYSICAL SECURITY: PROTECTING CRITICAL INFRASTRUCTURE AT THE STATE AND LOCAL LEVEL 113 (Robert M. Clark & Simon Hakim ed. 2017).

WILHELMSEN, TRINE-LISE & BULL, HANS JACOB, HANDBOOK ON HULL INSURANCE (2nd ed. 2017).

Wilhelmsen, Trine-Lise & Bull, Hans Jacob, *Hull Insurance of Autonomous Ships According to Nordic Law: What Are the Challenges? in* AUTONOMOUS SHIPS AND THE LAW 175 (Henrik Ringbom, Eris Røsæg & Trond Solvang eds., 2021).

WILHELMSEN, TRINE-LISE & BULL, HANS JACOB, NORWEGIAN CARGO INSURANCE (2012).

Electronic sources

About, NORMA CYBER, https://www.normacyber.no/en/about (last visited Nov. 24, 2022).

Chatfield, Chris, *Cyber Exclusion Clauses - Are They Fit for Purpose?*, KENNEDYS LAW (June 19, 2018), https://kennedyslaw.com/thought-leadership/article/cyber-exclusion-clauses-are-they-fit-for-purpose/.

Clark, Julian, *The Changing Face of Maritime Law and Risk – Cyber, E-Commerce, Automation of Vessels,* SHIPPING LAWS AND REGULATIONS 2021, ICLG (Aug. 6, 2021), https://iclg.com/practice-areas/shipping-laws-and-regulations/1-the-changing-face-of-maritime-law-and-risk-cyber-e-commerce-automation-of-vessels (last visited June 1, 2022).

Glossary: Virus, COMPUTER SECURITY RESOURCE CENTER, https://csrc.nist.gov/glossary/term/virus (last visited Nov. 24, 2022).

Greenwald, Judy, *Insurers Develop Cyber Cover for Maritime Industry*, 48 BUS. INS. (May 12, 2014), https://link.gale.com/apps/doc/A368265643/AONE?u=oslo&sid=bookmark-AONE&xid=39cb4a3e.

Greenwald, Judy, *Marine Sector Struggles with Cyber Risks; Navigation Systems Vulnerable to Attack*, 48 BUS. INS. (2014).

Helverschou, Preben B. & Bygholm, Susanne Kjær, *Norway: The Future of Cyber Cover in the Nordic Marine Insurance Markey*, MONDAYQ (Jan. 26, 2021), https://www.mondaq.com/reinsurance/201029500/the-future-of-cyber-cover-in-the-nordic-marine-insurance-market.

Lloyd's Register, *Can a lack of cyber security send cargo ships off course?*, LR (July 27, 2021), https://www.lr.org/en/insights/articles/can-a-lack-of-cyber-security-send-cargo-ships-off-course/.

Marine Digital, *Cybersecurity in shipping and port technologies: examples of cyber attacks in maritime*, https://marine-digital.com/cybersecurity_in_shipping_and_ports (last visited Sep. 21, 2022).

Marine Cyber Risk and Insurance, HOWDEN GROUP (Nov. 6, 2020), https://www.howden-group.com/ae-en/marine-cyber-risk-and-insurance-howden (last visited Nov. 6, 2022).

Ransomware, INTERNET CRIME COMPLAINT CENTER, https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf (last visited Nov. 24, 2022).

Services, NORMA CYBER, https://www.normacyber.no/en/services (last visited Nov. 24, 2022).

The Nordic Marine Insurance Plan of 2013, Version 2023, CEFOR, https://cefor.no/clauses/nordic-plan/ (last visited Oct. 13, 2022).

Wee, Vincent, *Naval Dome exposes vessel vulnerabilities to cyber attack*, SEATRADE MARITIME NEWS (Dec. 22, 2017), https://www.seatrade-maritime.com/asia/naval-dome-exposes-vessel-vulnerabilities-cyber-attack.

WTW Partners with Falvey Cargo Underwriting for Affirmative Cargo Cyber Coverage Solution, WTW (Feb. 16, 2022), https://www.wtwco.com/en-US/News/2022/02/wtw-partners-with-falvey-cargo-underwriting-for-affirmative-cargo-cyber-coverage-solution (last visited Nov. 9, 2022).