NUS Centre for Maritime Law Working Paper 2026/3

NUS Law Working Paper 2026/009

CAN A CYBER-ATTACK ON A MOBILISED VESSEL QUALIFY AS CAPTURE AND SEIZURE UNDER ENGLISH MARINE INSURANCE LAW?

Dr Fatıma Özcan

Research Fellow, Centre for Maritime Law

[Uploaded May 2026]

Can a cyber-attack on a mobilised vessel qualify as capture and seizure under English marine insurance law?

Dr Fatıma Özcan*

ABSTRACT

The increasing digitalisation of maritime operations and the advent of autonomous vessels have exposed vessels to cyber risks capable of disrupting navigation, engine control and onboard operations. Traditionally, marine insurance law recognises capture and seizure as perils involving physical dispossession or overt control by a hostile third party. However, cyber-attacks do not fall within the scope of 'capture and seizure' peril under English law, despite often resulting in similar types of losses.

This paper explores whether a cyber-attack on a mobilised vessel, autonomous or otherwise, could be classified as a capture and seizure peril. Through doctrinal analysis, key case law, and market practice, it argues that cyber-attacks, notwithstanding their catastrophic consequences, fail to satisfy the physicality requirement inherent to capture and seizure in its current legal formulation. The paper concludes by highlighting the need for doctrinal and contractual evolution and by proposing the adoption of hybrid insurance policies to address emerging maritime risks.

Keywords: marine insurance, capture, seizure, autonomous vessels, cyber-attack, constructive total loss, cyber-enabled loss, hybrid policies

* Research Fellow, Centre for Maritime Law (CML), National University of Singapore. This paper is drawn from the author's PhD thesis. I thank Professor Stephen Girvin for his guidance and insightful suggestions, and Professor Özlem Gürses for her valuable feedback. I am also grateful to the Centre for Maritime Law, National University of Singapore, for its support. The usual disclaimer applies. A revised version of this paper is forthcoming in [2027] J of Business Law.

1 Introduction

Maritime shipping is undergoing a comprehensive digital transformation, with Maritime Autonomous Surface Ships (MASS) gradually becoming a 21st-century reality, driven by the construction of pioneering vessels, such as the *Yara Birkeland*,[1] since 2021. Modern vessels have become progressively more dependent on electronic systems for communication, navigation, and operational functions.[2]

This reliance introduces new security vulnerabilities, particularly with respect to cyber-attack threats, creating unique risks not typically found in conventional ships and requiring a reassessment of traditional risk approaches for modern vessels. The importance of this issue lies in the fact that, as the transition toward autonomous ships advances, reliance on digital systems will also increase substantially. Consequently, the potential impact and losses from a cyber-attack on such vessels could be severe.

The risk is not merely hypothetical. Well-documented cyber-attack scenarios,[3] such as the Shen attack[4] and the Bashe attack,[5] illustrate the potential scale of disruption and financial loss, while real-world incidents, including WannaCry, NotPetya, and Petya,[6] have demonstrated that such impacts can and do occur in practice. While the full scope of potential

---

1 Asle Skredderberget, 'The First Ever Zero Emission Autonomous Ship' (YARA) <https://www.yara.com/knowledge-grows/game-changer-for-the-environment/> accessed 22 April 2026

2 By thoroughly understanding a ship's operational, communication, and technical systems, one can identify potential points of cyber vulnerability. This is particularly important because modern vessels depend heavily on electronic systems, making them more susceptible to cyber-attacks. See generally, Hongchu Yu, Qiang Meng, Zhixiang Fang and Jingxian Liu, 'Literature Review on Maritime Cybersecurity: State-of-the-art' (2023) 76 J of Navigation 453.

3 Here, Shen Attack and Bashe Attack are taken as examples, which are hypothetical large-scale cyber-attack scenarios targeting Asia–Pacific ports, developed by the Cambridge Centre for Risk Studies in collaboration with Lloyd's. These scenarios illustrate how malware-induced disruptions to shipping databases could result in losses amounting to billions of dollars.

4 Lloyd's of London, Cambridge Centre for Risk Studies, Nanyang Technological University, *Shen Attack: Cyber Risk in Asia Pacific Ports* (2019) <https://www.transre.com/wp-content/uploads/2019/10/CyRiM-ShenAttack-Report-October-2019.pdf> accessed 22 April 2026.

5 Lloyd's of London, Cambridge Centre for Risk Studies, Nanyang Technological University, *Bashe Attack: Cyber Risk in Asia Pacific Ports* (2019) <https://assets.lloyds.com/assets/pdf-bashe-attack-cyrimbasheattack-finalbashe-attack/1/pdf-bashe-attack-CyRiMBasheAttack_FINALbashe-attack.pdf> accessed 22 April 2026.

6 Alex Hern, 'WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017' (*The Guardian*, 30 December 2017) <https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware> accessed 22 April 2026.

harm from cyber-attacks on autonomous ships remains uncertain, the likelihood of such incidents is considered substantial.

Capture and seizure are listed among marine perils under the Marine Insurance Act 1906 (MIA)[7] and standardised in the Institute War Clauses.[8] In response to evolving cyber risks, insurers have introduced dedicated cyber insurance policies, acknowledging that such risks are substantively distinct from conventional war perils. Nevertheless, although traditional war risk policies do not expressly provide cover for cyber-attacks, cyber incidents may exhibit functional similarities to several recognised war risk perils, including capture and seizure.

Historically, 'capture' includes any act of seizing by an enemy, while 'seizure' is broader, involving any forcible possession by lawful authority or overpowering force.[9] Recent case law, affirmed by Calver J, clarifies that 'seizure' should be interpreted according to its ordinary and natural meaning, encompassing all acts of forcible possession by lawful authority or an overpowering force, and is not limited to actions carried out under any law, order, decree, or regulation of a governing authority.[10]

Cyber-attacks, however, disrupt this traditional understanding of risk. Unlike conventional threats, they are typically executed remotely, without requiring any physical presence on board. Despite their intangible nature, such attacks can have consequences comparable to those of physical capture and seizure: vessels may be navigationally incapacitated, engines may become inoperable, or cargo systems may be hijacked. In some instances, an unauthorised party may gain operational control remotely, effectively 'seizing' the vessel without physically boarding it. This functional deprivation, though real and economically significant, falls outside the doctrinal scope of capture and seizure, which highlights a gap between conventional marine insurance law and digital risks.

---

7 MIA 1906, s 3(2)(c): '"Maritime perils" means the perils consequent on, or incidental to, the navigation of the sea, that is to say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seizures, restraints, and detainments of princes and peoples, jettisons, barratry, and any other perils, either of the like kind or which may be designated by the policy.'

8 Institute War and Strikes Clauses (Hulls-Time) (1/11/95) cl 1.5: 'Subject always to the exclusions hereinafter referred to, this insurance covers loss of or damage to the Vessel caused by... capture, seizure, arrest, restraint or detainment, and the consequences thereof or any attempt thereat ...'

9 *Cory & Sons v Burr* (1883) 8 App Cas 393.

10 *Hamilton Corporate Member Ltd v Afghan Global Insurance Ltd* [2024] EWHC 1426 (Comm), [2025] Lloyd's Rep IR 31.

In a likely autonomous ship scenario, capture and seizure could occur through both physical boarding by external hostile forces and cyber hijacking. The absence of crew significantly facilitates the capture process by eliminating or substantially reducing on-site human resistance; however, operators may still attempt to intervene remotely, for example, by shutting down the ship's system. Such actions could prevent the vessel from being moved or create additional risk if captors attempt to gain control by force.

Cyber hijacking, on the other hand, replicates the effects of capture and seizure by remotely taking control of the ship's operational systems. In the context of MASS, such digital capture incidents are most likely realised through deliberate, intentional, and externally initiated cyber-attacks rather than accidental system failures.

This paper examines whether cyber-attacks on mobilised vessels can be classified as perils of capture and seizure under English marine insurance law. It analyses the traditional elements and limitations of the peril of capture and seizure, considers the potential classification of cyber-attacks as such perils, and evaluates the arguments for and against this approach.

2 Cyber-attacks in autonomous shipping

As technology advances, the maritime industry's growing reliance on the internet increases its vulnerability to cyber-attacks. This vulnerability arises from the interconnected nature of components within the maritime sector, including ports, shipping companies, and vessels. The integration of the maritime network has the potential to significantly impact the global economy, affecting sectors such as transportation, aviation, aerospace, manufacturing, and retail.[11] Although it was a fictional scenario, Shen's cyber-attack simulation illustrated the potential impact of a malware incident on fifteen Asian ports, with estimated damages of approximately US$110 billion.[12]

Ships rely on technology but often function in remote areas where assistance may not be readily available.[13] Furthermore, with the increasing adoption of autonomous vessels and the

[11] Gary C Kessler and Steven D Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers* (2nd edn, Independently published 2022) 90.

[12] (n 4) 6.

[13] Brian Wilson, 'Maritime Cyber Security' in James Kraska and Young-Kil Park (eds), *Emerging Technology and the Law of the Sea* (Cambridge University Press 2022) 160.

removal of human operators onboard, the potential for significant damage may rise. Advancements in technology in this century have enabled the development of autonomous vessels with differing levels of automation. The term 'autonomous' describes a vessel's capability to perform a sequence of predefined operations with minimal or no intervention from the bridge crew.[14] While this does not categorically indicate the absolute absence of personnel on board,[15] the number of individuals present may vary depending on the vessel's level of automation. According to Ringbom and Collin, a system is considered autonomous if it fulfils two primary criteria: (1) it must demonstrate the technical capability to make independent decisions and (2) possess the capacity to implement those decisions without external assistance.[16]

The International Maritime Organisation (IMO) has classified autonomous vessels into four distinct levels of autonomy, from basic automation to full autonomy.[17] Degree one describes a 'Ship with automated processes and decision support,' where onboard systems and activities are operated and managed by seafarers.[18] Degree two describes a 'Remotely controlled ship with seafarers on board.' In this context, the vessel is navigated using a remote-control system operated by engineers and deck personnel from a control centre.[19] Degree three is defined as a 'Remotely controlled ship without seafarers on board.'[20] Although Degree three autonomy shares certain characteristics with Degree two, it is distinguished by the complete absence of seafarers on board. A vessel classified as 'Fully autonomous' at Degree four operates through an advanced system capable of independently determining courses of action and executing decisions without any human involvement. [21]A fully autonomous vessel represents the highest level of autonomy achievable in maritime operations. Given the range of autonomy levels, cyber risks pose a substantial concern for MASS.

---

[14] Ørnulf Jan Rødseth and Håvard Nordahl, 'Definitions for Autonomous Merchant Ships' (2020) 7 <https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/autonom-defs.pdf> accessed 22 April 2026.

[15] Ibid.

[16] Ibid.

[17] 'Autonomous Shipping' (IMO) <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx> accessed 22 April 2026.

[18] 'The Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS), MSC.1/Circ.1638' (2021) 5.

[19] Ibid.

[20] Ibid.

[21] Ibid 6.

Cybersecurity risk represents a critical concern across the maritime industry, affecting not only autonomous vessels but also a wide range of internet-connected portals and devices. Vessels engaged in commercial operations depend on internet connectivity to support essential navigation systems, including the Radio Detection and Ranging (RADAR), Electronic Chart Display and Information System (ECDIS), and Automatic Identification System (AIS).[22] Consequently, given their reliance on internet connectivity and digitalisation, these systems are already at substantial risk of cyber-attack.

Greater interconnectivity enables individuals with internet access and technical expertise to access operational systems on ships, such as the AIS system, cargo records, location data, and bridge or engineering controls.[23] Shipping companies, therefore, face a spectrum of risks, including data breaches, business interruptions, property damage, intellectual property theft, and industry-specific threats, such as navigational failures and safety hazards at sea.[24] Moreover, the impact of cyber incidents extends beyond vessels to encompass onshore operations, shipowners, operators, seafarers, ports, terminals, and logistics companies.[25] Unlike traditional maritime risks, which are largely dependent on fortuitous events,[26] cyber risks may be initiated by any individual with computer access and are not confined by geographic boundaries.[27]

This wide-ranging exposure has led the insurance sector to adopt the term 'cyber' to encompass a broad array of information technology risks, including those related to cloud computing, hardware, software, IT consulting, and data processing.[28] As a result, almost any subject related to information technology may be classified as a cyber matter. Although cyber-attacks have occurred since the late 1980s,[29] when computer networks, the internet, and

---

22 Yu et al (n 2) 453.

23 Simon Cooper, 'Cyber Risk, Liabilities and Insurance in the Marine Sector' in B Soyer and A Tettenborn (eds), *Maritime Liabilities in a Global and Regional Context* (Informa Law from Routledge, 2018) 103.

24 M Bob Kao, 'Cybersecurity in the Shipping Industry and English Marine Insurance Law' (2021) 45 Tul Mar LJ 485.

25 Cooper (n 23) 103.

26 Feng Wang, 'The Warranty of Seaworthiness and Cyber Risk of Unmanned Ships' [2020] JBL 311.

27 Ibid.

28 Leo P Martinez, 'Cyber Risks: Three Basic Structural Issues to Resolve' in P Marano and K Noussia (eds), *InsurTech: A Legal and Regulatory View* (Springer, 2020) 212.

29 The very first cyber-attack in history is the Morris Worm, which dates from 1988. See Lindsay Lennon, 'The "Morris Worm": A Notorious Chapter of the Internet's Infancy' (*Cornell Alumni,* 2023) <https://alumni.cornell.edu/cornellians/morris-worm/> accessed 22 April 2026.

communication technologies were first adopted, the term 'cyber-attack' still lacks an internationally recognised definition.[30]

In the maritime sector, however, greater clarity is provided by the Baltic and International Maritime Council (BIMCO), which defines a cyber-attack as any offensive action directed at IT and OT systems, computer networks, or personal computing devices, intended to compromise, destroy, or gain unauthorised access to company and vessel systems and data.[31] From this perspective, a cyber-attack is a deliberate, hostile action undertaken by a malicious actor to compromise a system. As this involves intentional conduct, it excludes risks arising from negligence or accidental behaviour. The objectives of such attacks may include damaging, disrupting, destroying, or manipulating computer systems, as well as altering, blocking, erasing, modifying, or acquiring data retained on these systems.

Understanding the motivations of the perpetrators is crucial in assessing the extent to which capture and seizure perils align with cyber risks. According to the BIMCO *Guidelines*,[32] motivations may include revenge, media attention, reputational damage, financial gain, espionage, political reasons, and more. However, the 2025 Data Breach Investigations Report[33] indicates that over 95 per cent of cyber-attacks are financially motivated.

However, cyber-risk in the maritime context is not confined to deliberate attacks. Accidental or negligent actions can also create vulnerabilities within maritime systems. According to IMO's Interim Guidelines, maritime cyber risk refers to an assessment of the vulnerability of Computer-Based Systems (CBS) to potential events or circumstances that could cause shipping-related operational, safety, or security failures through the corruption, loss, or compromise of data or systems.[34]

---

30 Julia Constantino Chagas Lessa and Belma Bulut, 'A New Era, a New Risk! A Study on the Impact of the Developments of New Technologies in the Shipping Industry and Marine Insurance Market' in Marano and Leo Martinez (n 28) 315.

31 BIMCO, *The Guidelines on Cyber Security Onboard Ships v5.0* (Intercargo 2024) 82.

32 Ibid 12.

33 Financial motives account for 99% of breaches affecting small businesses and 95% of those affecting large businesses. David Haylender et al, 'Verizon 2025 Data Breach Investigations Report' (2025) 85 <https://www.verizon.com/business/resources/infographics/2025-dbir-smb-snapshot.pdf> accessed 22 April 2026.

34 Maritime Safety Committee of IMO*, Guidelines on Cyber Risk Management* (2025) (MSC-FAL.1/Circ.3/Rev.3).

To further categorise these threats, the Institute of Risk Management (IRM) identifies three types of cyber risks based on their characteristics:

(1) "Deliberate and unauthorised breaches of security to gain access to information systems for the purposes of espionage, extortion or embarrassment,
(2) Unintentional or accidental breaches of security, which nevertheless may still constitute an exposure that needs to be addressed,
(3) Operational information technology risks due to poor systems integrity or other factors."[35]

These frameworks indicate that cyber risks in maritime operations can originate from multiple sources, including deliberate, unintentional, and operational, and each type has distinct attributes that require special consideration. For the purpose of capture and seizure perils, however, digital capture and seizure incidents are more likely to result from deliberate, intentional and externally initiated cyber-attacks, rather than from accidental or operational risks.

Significantly, such attacks can disrupt a vessel's operations, causing cargo delays and financial or reputational losses, even where the ship remains physically unaffected but loses operational control. This result is similar to those arising from the acts of capture and seizure. Unlike capture and seizure, which entail direct physical possession, cyber-attacks operate through remote or intangible means. This distinction is particularly significant when considering whether English law might recognise cyber interference as a peril covered under marine insurance. Despite increasing attention to autonomous shipping and cybersecurity technologies, the specific risk of cyber-induced capture and seizure remains insufficiently examined within academic and insurance discourse.

Drawing on this, the following section examines the doctrines of capture and seizure within the framework of English marine insurance law. It evaluates the extent to which cyber risks may be differentiated from, and in certain respects, aligned with, the traditional components of this peril, with reference to English case law.

[35] Institute of Risk Management (IRM), 'Cyber Risk Resources for Practitioners' (2014) 10 <https://www.theirm.org/media/7237/irm-cyber-risk-resources-for-practitioners.pdf> accessed 22 April 2026.

3 Capture and seizure in marine insurance law

The continuous advancement of technology in the marine industry has introduced a range of emerging risks, with cyber-attacks on vessels now considered one of the most significant threats. [36] While traditional war risk policies typically exclude cyber risks, such incidents can produce outcomes similar to conventional perils, particularly capture and seizure, by resulting in shipowners losing control of their vessels. In the case of autonomous ships, cyber-attacks may achieve this remotely, without physical boarding or dispossession. Although these incidents share key characteristics with traditional war perils, such as unauthorised control, external threats, and political or military motives, the absence of physical force complicates their classification under established doctrines. This raises a critical question: can the concept of capture and seizure be interpreted broadly enough to encompass cyber-attacks, given that the intent and consequences of both perils are effectively aligned?

3.1. Historical and statutory background

Consider a scenario in which hackers illegally seize control of a ship, disrupt its cybersecurity system, redirect it to a different port, and refuse to release it for months. This scenario illustrates the perils of capture and seizure in marine insurance, showing that a vessel may become effectively unusable whether it is physically seized or remotely taken over. In both cases, it is arguable that no physical loss or damage to the ship or its cargo is required. This section, therefore, focuses on the key elements of capture and seizure and critically examines whether a cyber-attack on a mobilised vessel could fall within the scope of this marine insurance peril.

Capture and seizure, though closely related, do not describe the identical actions. Capture represents, in the event of a war, taking by the opponent as a reward, or as retaliation, to deprive the owner of any sovereignty or right of property over the property acquired.[37]

---

[36] A recent survey shows that 71% of maritime professionals view their assets as increasingly vulnerable to cyber-attacks, with the same proportion identifying cybersecurity as their organisation's greatest business risk: Svante Einarsson, 'Tackling a growing cybersecurity threat in an increasingly connected industry' (*DNV*, 12 December 2024) <https://www.dnv.com/expert-story/maritime-impact/tackling-a-growing-cybersecurity-threat-in-an-increasingly-connected-industry/> accessed 22 April 2026.

[37] Mark Templeman KC et al, *Arnould: Law of Marine Insurance and Average* (21st edn, Sweet & Maxwell Ltd 2024) [24-23].

Seizure, on the other hand, includes various types of takings and is not strictly restricted to state-sanctioned actions.[38] It can include, for example, the seizure of a vessel by pirates, passengers, or locals with the intent to plunder.[39] As such, the perpetrators and circumstances of capture and seizure vary.

The distinction between capture and seizure was clarified in *Cory & Sons v Burr*, where Lord Fitzgerald[40] noted:

> 'Capture' would seem properly to include every act of seizing or taking by an enemy or belligerent. 'Seizure' seems to be a larger term than 'capture', and goes beyond it, and may reasonably be interpreted to embrace every act of taking forcible possession either by a lawful authority or by overpowering force.

Thus, while capture is limited to acts by belligerents,[41] seizure involves two broader elements: the lack of possession and the use of force.[42] In *Cory*, it is also held that a non-belligerent taking, such as the arrest of a vessel by revenue officers, fell within the scope of seizure, leaving open the question of whether a belligerent taking could similarly qualify, given that such acts were already covered by capture.[43]

The distinction is further elaborated in *Robinson Gold Mining Co v Alliance Insurance Co*, where Phillimore J observed:[44]

> … Was this taking a capture, seizure, or detention within the terms of the clause of exception? It has been suggested that these words point to hostile taking, and to hostile taking only. That is probably true of capture. But seizure is an additional word. (…) 'Seizure' signifies 'the taking of a ship by the act of governments or other public authority for a violation of the laws of trade, or some rule or regulation instituted as a matter of municipal police, or in consequence of an existing state of war.

---

38 Ibid.
39 Ibid.
40 *Cory* (n 9).
41 Robert Merkin, *Colinvaux's Law of Insurance* (14th edn, Sweet & Maxwell 2025) [26-044].
42 FD Rose, *Marine Insurance: Law and Practice* (2nd edn, Informa Law from Routledge 2012) [17.51].
43 Colinvaux (n 41) [26-044].
44 [1901] 2 KB 919, 925- 926 (Phillimore J).

Returning to the cyber-attack scenario introduced above, these distinctions raise an important question: can a cyber-attack be covered under the peril of capture and seizure? The following sections undertake a detailed analysis of capture and seizure, taking into account the evolving characteristics of cyber risks.

3.2 Elements and limits of the peril

This section analyses four constituent elements of the perils of capture and seizure, namely: (1) reasons and motivation, (2) the requirement of an actual force, (3) action by a third party, and (4) physical dispossession or overt control, drawing upon relevant case law to inform the discussion.

3.2.1 *Reasons and motivations*

In the context of a cyber-attack, the attackers' motivation plays a central role in establishing its connection to the marine and war risk perils. As noted earlier, cyber incidents can arise for a variety of reasons, ranging from financial gain to political or strategic objectives.[45] It is therefore necessary to consider the intended outcome of the attack. For example, the intent to detain a vessel, even temporarily, or to coerce those on board, may result in different implications for capture, seizure, and cyber-attacks. The key question is whether a cyber incident is covered when the vessel is only held temporarily or when the crew is subject to blackmail.

Looking at the case law, in *Johnston & Co v Hogg*,[46] the court did not require an initial or continuous intention to deprive the owner of their property permanently;[47] the attackers' focus on looting the cargo was sufficient.[48] Similarly, in the cyber context, hackers may not intend to retain the vessel itself, but rather aim to steal data or demand a ransom through system lockouts, such as in ransomware attacks.

---

[45] See BIMCO report (2024) (n 31) and Verizon Data Breach Investigations Report (2025) (n 33).

[46] (1883) 10 QBD 432.

[47] Howard Bennett, *The Law of Marine Insurance* (2nd edn, Oxford University Press 2006) para 13.47.

[48] Michael Davey, James Davey and Oliver Caplin, *Miller's Marine War Risks* (4th edn, Informa Law from Routledge 2020) [12.2].

It is important to note that not every cyber incident involving a vessel will engage the peril of capture or seizure, even where a financial motive exists. Specifically, a cyber-attack resulting solely in data theft or compromise of commercially sensitive records does not, by itself, constitute a maritime peril within the meaning of s 3(2)(c) of MIA 1906, as maritime perils are confined to those consequents on, or incidental to, the navigation of sea.[49]

A ransomware attack that locks down a shipping company's sensitive information or leaks cargo manifests and financial data does not meet this requirement. In that case, the ship itself remains under the owner's operational control, and there is no loss of ownership. Therefore, the capture and seizure analysis only applies when the cyber-attack has operational consequences on the ship's navigation, propulsion, or control systems, i.e., when the owner is deprived of the ability to steer or operate the ship. Cyber-attacks that do not affect the ship's operational activities, but only cause economic or informational damage, are excluded from this risk and should be addressed through specific cyber insurance provisions.

The case of *Banque Monetaca & Carystuiaki v Motor Union Insurance Co*[50] illustrates the importance of the underlying motivation, drawing a fine line between loss from seizure and loss from piracy. It was determined that since the political and military motivations of those influencing the seizure seemed to be the primary causes, it was considered a seizure, despite strong personal gains.[51]

A further illustration is provided by *Bayview Motors Ltd v Mitsui Marine & Fire Insurance Co Ltd,*[52] in which David Steel J observed:

> When the customs officers converted the cars by refusing to release them, the cars had already been voluntarily placed in their custody and control in the bonded car park. Misappropriation in this manner does not constitute the taking of forcible possession. Further, there was no taking by lawful authority. The customs officers were not acting

[49] MIA 1906, s 3(2)(c).
[50] (1923) 14 Ll L Rep 48. See also *Miller's Marine War Risks* (n 48) [12.23].
[51] Ibid.
[52] [2002] EWCA Civ 1605, [2003] 1 Lloyd's Rep 131.

> as organs of the state, lawfully or otherwise. They were acting solely in their own interests.[53]

This demonstrates that when public officials misuse property for private purposes, the act is considered theft, rather than a seizure.[54] Accordingly, the motivation behind an act, whether physical or cyber, is a decisive factor in determining whether it falls within the capture and seizure peril.

3.2.2 *The requirement of an actual force*

Another critical element is whether the use of force is necessary to classify an incident as capture or seizure. This raises two questions: (1) which perils require actual force; and (2) can a cyber-attack be considered forceful? In this technology-driven era, cyber-attacks occur remotely, exploiting vulnerabilities in a vessel's digital systems. As a result, attackers are unlikely to resort to physical violence against a vessel during a cyber-attack. Traditionally, as highlighted in *Cory,*[55] forcible possession is a necessary element of seizure. Similarly, in *Robinson Gold Mining Co,*[56] Phillimore J accepted that 'seizure implies force' and that the taking in question was forcible, even though it was constitutionally and lawfully effected. Likewise, *The Minden* affirmed that forcible taking is a required element for a seizure.[57] However, sixty years later, a subsequent case further refined this requirement. In *Bayview Motors Ltd,*[58] the court held that actual force is not strictly necessary for the action to be considered a capture and seizure, though a threat of force or its indication is required.

In the cyber context, although no physical force is involved, companies may still receive threats or ransom demands that compel them to pay in order to secure the release of their valuable information. Prior to stealing, altering or disclosing data, hackers frequently disable a company's system and demand a ransom. This situation can be considered a form of 'threat

---

53 Ibid.
54 Rose (n 42) [17.48].
55 Above (n 9).
56 Above (n 44) 925 (Phillimore J).
57 [1942] AC 50 (HL).
58 Above (n 52).

force or its indications,' as it involves compelling the company to act under threat of significant harm, in line with the revised interpretation of force in *Bayview Motors Ltd*.[59]

A recent study highlights the growing significance of such threats. In 2023, the average cost of restoring access to computer systems following cyber-attacks reached US$3.2 million, while maritime companies reported an increasing willingness to pay ransomware demands.[60] A survey conducted by HFW and CyberOwl involving more than 150 maritime industry experts revealed that 14 per cent of maritime companies paid ransoms that year, a sharp rise from 3 per cent in the previous year.[61] This 11 per cent increase illustrates the industry's escalating vulnerability to ransomware attacks and highlights the substantial impact and coercive nature of such incidents. Given that case law has evolved to reinterpret the type of force required to meet societal needs, it is reasonable to argue that cyber-attack methods could also be understood as a form of force within the principles of capture and seizure.

The next section will explore the role of actions taken by third parties, illustrating actions by masters, crew and passengers in capture and seizure incidents, and how these principles may extend to cyber risks.

3.2.3 *Action by a third party*

In assessing whether a cyber-attack falls within the scope of capture and seizure, the roles of the master, crew, and people outside these groups are particularly significant. Marine insurance policies are traditionally framed with manned vessels in mind, yet the increasing use of automation complicates this assessment. In a conventional vessel, if a cyber-attack occurs, the crew will typically remain on board even if they lose operational control, since the intrusion is likely to be digital rather than physical in nature. The question then becomes whether possession of the vessel can be considered lost when the crew is still physically present but is compelled or overridden by an external actor.

---

[59] Ibid.

[60] Paul Peachey, 'Shipping Names Pay Multimillion-Dollar Ransoms After Cyber Attacks' (TradeWinds News, October 2023) <https://www.tradewindsnews.com/technology/shipping-names-pay-multimillion-dollar-ransoms-after-cyber-attacks/2-1-1536556> accessed 22 April 2026.

[61] Martyn Wingrove, '14% of Maritime Industry Hit by Ransomware Payments' (Riviera, November 2023) <https://www.rivieramm.com/news-content-hub/news-content-hub/cyber-security-solution-unveiled-as-maritime-incidents-rise-78685> accessed 22 April 2026.

This issue was addressed in *The Anita,*[62] where the court held that if the master and crew are forced to obey the instructions of a third party, possession is effectively lost to the owners. The rationale was that, in such cases, the master and crew no longer hold the vessel for the owner but for the third-party exercising control. By analogy, in a cyber-attack, even if hackers do not directly engage with the crew, their ability to remotely alter the vessel's route or systems may achieve the same outcome. Should the crew be forced to comply with hackers' instructions, the situation would more clearly align with capture and seizure perils.

Another question concerns the identity of the perpetrators: who would be responsible for the cyber-attack in terms of taking possession of the vessel, and how would this resonate in capture and seizure as a peril? In theory, possession of a vessel can be taken by the master, crew, passengers, or external third parties. Thus, determining whether a cyber-attack scenario fits within the established categories is critical.

As explained in *Miller's Marine War Risks*, the abuse of authority by the master or crew does not constitute seizure,[63] since they already hold legitimate possession of the vessel. Similarly, in *Salem,*[64] the misuse of cargo by a shipowner acting as bailee was held not to amount to a 'taking at sea,' which is similar to a seizure.[65] The reasoning was that because the shipowner was already in control, they would abuse that trust. There was no forcible or clandestine taking. Applying this logic to cyber incidents, if the attack originates from insiders such as the master, crew, or shipowner, it would generally fall outside the scope of capture and seizure, as the perpetrators are already entrusted with control.

On the other hand, different considerations apply when the perpetrators are passengers. In *Naylor v Palmer,*[66] coolie immigrants travelling from Canton to Callao deliberately killed the captain and part of the crew and forcibly took the ship and the remaining crew, which was considered an act of piracy within the policy.[67] This reasoning was affirmed in *Kleinwort v Shepard,*[68] where a similar mutiny by immigrants was treated as a seizure. Likewise, the

[62] [1970] 2 Lloyd's Rep 365.
[63] Above (n 48) [12.5].
[64] [1983] 2 AC 375 (HL).
[65] *Miller's Marine War Risks* (n 48) [12.5].
[66] (1853) 8 Ex 739.
[67] *Arnould* (n 37) [23.34].
[68] (1859) 1 E & E 447.

authors of *Miller's War Risks* noted that, if the passengers take control of the ship, the act constitutes a seizure, as passengers are not deemed lawful possessors on behalf of the owner.[69] Moreover, s 8 of the MIA 1906 extends the definition of piracy to include passengers who mutiny. Therefore, depending on the specific circumstances and intentions, participating in mutiny or attacking the ship may constitute piracy or seizure.

Although cyber-attacks differ in method, the analogy is quite similar. Just as insiders, such as crew members or passengers, undermine the vessel's control and lead to capture, seizure, or piracy in maritime journeys, a malicious individual, whether external or an insider, can exploit vulnerabilities to seize control of digital systems and compromise data.

The perpetrators of cyber-attacks may range from state actors and organised groups to individuals, or even unknown third parties. Nevertheless, as with piracy and mutiny, insiders also play a significant role. A malicious insider is an employee who discloses company secrets and exploits weaknesses within the organisation.[70] In the case of a vessel, these vulnerabilities could include information about cargo or the identities of people on board. These actors might have a variety of motivations for providing access to systems and, as a result, revealing sensitive data. It does not necessarily mean that these people should be at the company at that time. Rather, they could simply be former employees[71], business associates,[72] or anyone with an interest in the company.

---

69 Above (n 48) [12.6].

70 '8 Common Cyber Attack Vectors & How to Avoid Them' (Balbix) <https://www.balbix.com/insights/attack-vectors-and-breach-methods/> accessed 22 April 2026.

71 In 2001, 49-year-old Australian Vitek Boden executed the first known cyber-attack on critical infrastructure by manipulating the Maroochy Shire sewer control system, resulting in the release of 265,000 gallons of untreated sewage into nearby parks and rivers and causing significant environmental harm. The attack followed his rejection for a local Council job while he was employed by the company that installed the system, suggesting he leveraged specialised knowledge of its vulnerabilities. This case exemplifies how cyberattacks can originate from current or former employees. See Gary Cohen, 'Throwback Attack: An Insider Releases 265,000 Gallons of Sewage on the Maroochy Shire' (Industrial Cyber Security Pulse, 2021) <https://www.industrialcybersecuritypulse.com/facilities/throwback-attack-an-insider-releases-265000-gallons-of-sewage-on-the-maroochy-shire/> accessed 22 April 2026.

72 Robert Grimmick, 'What is an Insider Threat? Definition and Examples' (Varonis, 12 June 2023) <https://www.varonis.com/blog/insider-threats/> accessed 22 April 2026.

Based on statistics from November 2023, 37.45 per cent of intentional or accidental data breaches were attributed to internal actors.[73] While such breaches may be more challenging to execute in a live vessel context due to the risks presented to safety and security, the data emphasises the seriousness of insider threats. Accordingly, each incident must be carefully examined in light of both traditional principles of capture and seizure and the evolving realities of cyber risk.

3.2.4 *Physical dispossession or overt control*

A further constituent element of the peril is physical dispossession, understood as the act of forcibly depriving individuals of their goods or property through the assumption of possession and control. A modern illustration of 'capture' can be seen in *Kuwait Airways Corp v Kuwait Insurance Co SAK*,[74] where, during Iraq's invasion of Kuwait in August 1990, the insurers acknowledged that the Iraqi forces' actions concerning certain aircraft constituted capture.[75] This case demonstrates that capture is fundamentally associated with the transfer of possession and control, rather than mere obstruction or interference. Similarly, seizure has been characterised as including 'every act of taking forcible possession either by a lawful authority or by overpowering force',[76] emphasising the necessity of acquiring possession through force.

Applying these principles to cyber perils presents distinct challenges. Unlike conventional forms of capture or seizure, cyber-attacks operate in a digital, intangible domain, involving neither the physical boarding of the vessel nor the physical removal of property. Nevertheless, the assumption of control over a ship's digital systems may amount to a functional equivalent of capture, insofar as it effectively deprives the assured of operational control. Where hackers override navigation, propulsion or engine systems, the owner may be prevented from using or directing the vessel, even though legal title formally remains unchanged.

---

[73] 'Orange Cyberdefense Releases Security Navigator 2024' (Orange Cyberdefense, 30 November 2023) <https://www.orangecyberdefense.com/global/news/research/orange-cyberdefense-releases-security-navigator-2024> accessed 22 April 2026.

[74] [1996] 1 Lloyd's Rep 664.

[75] John Dunt, *Marine Cargo Insurance* (2nd edn, Informa Law from Routledge 2020) [10.18].

[76] See *Cory* (n 9) 405 (Lord Fitzgerald).

4 Loss: Constructive total loss in capture and seizure cases

The satisfaction of a capture or seizure peril is a necessary, but not sufficient, condition for recovery under a marine insurance policy. A separate question is whether that peril has given rise to a compensable loss. The occurrence of an insured peril does not, of itself, establish a recoverable loss: the assured must also demonstrate that the peril has produced a loss of the kind contemplated by the policy. In the context of capture and seizure, the principal mechanism for establishing such loss is the doctrine of constructive total loss (CTL). Conflating the existence of the peril with the occurrence of a loss risks obscuring the distinct legal requirements governing each and may lead to erroneous conclusions regarding coverage. Therefore, this section examines how CTL operates in capture and seizure cases and considers the extent to which those principles can be applied to cyber-induced deprivation of control.

CTL refers to a loss that, while not total in a physical sense, is treated as economically equivalent to a total loss and may be claimed as such at the assured's option.[77] Importantly, CTL does not entail a transfer of ownership to the captors; rather, it arises where the insured peril renders the vessel a total loss in fact or in law. Where the requirements for CTL are satisfied, the assured may recover as for a total loss, even though the vessel has not been physically destroyed.[78] Under MIA 1906, a CTL exists where recovery of the insured property is unlikely, or where the cost of recovery would exceed the vessel's post-recovery value.[79] The inquiry, therefore, focuses not on the intrinsic character of the peril itself, but on the legal and factual consequences it produces for the assured. Accordingly, the decisive question is not whether the vessel has been physically destroyed or seized, but whether the assured has been deprived of it in circumstances where recovery cannot reasonably be anticipated. This was articulated in *Mitchell v Edie,* where Buller J explained that:[80]

"A total loss is of two sorts: one, where in fact the whole of the property perishes… the other, where the property exists, but the voyage is lost, or the expense of pursuing it exceeds the benefit arising

[77] Özlem Gürses, *Marine Insurance Law* (3rd edn, Routledge 2023) 300.
[78] Ibid.
[79] MIA 1906, s 60(2).
[80] (1787) 1 Term Rep 608, 615.

from it … where the voyage is lost, but the property is saved, the owners have an option to abandon; but that unless they do elect to abandon, it is only an average loss."

In the context of capture and seizure, the second category is of central importance: the vessel may remain physically intact yet be effectively lost to the assured where deprivation of possession renders recovery unlikely. This section focuses on the conditions under which this threshold is met.

A note of caution is warranted when relying on pre-1906 authorities on CTL by loss of possession. Under the common law as it stood prior to the MIA 1906, capture or seizure was treated as constituting a total loss, on the basis that the prospects of recovery were uncertain at the point of seizure.[81] The principle was subject to limited exceptions[82] and was subsequently refined through a line of decisions arising from the Napoleonic Wars, which established that the validity of an offer of abandonment was to be assessed as at the date judicial proceedings were commenced rather than the date the notice was served.[83]

The MIA 1906, however, introduced a material change to this position. Section 60 departed from the common law uncertainty standard by substituting the requirement that recovery be shown to be unlikely.[84] Pre-1906 authorities are accordingly no longer directly authoritative on the requirements for CTL under the modern statutory framework and should be treated only as illustrative of the doctrine's historical development. The relevant principles are now governed by s 60, as interpreted in the post-1906 case law, to which this section turns.

The decision in *Polurrian Steamship Co Ltd v Young*[85] clarifies that uncertainty of recovery alone is insufficient to establish a CTL; rather, recovery must be shown to be 'unlikely.' In that case, a neutral steamship carrying coal to Constantinople was detained by a Greek warship on

---

81 *Goss v Withers* (1758) 2 Burr 683; Rob Merkin, *Marine Insurance: A Legal History* (Edward Elgar Publishing 2021) [7-054].

82 Ibid. Lord Mansfield recognised two exceptions: (i) where a vessel suffered only a small, temporary hindrance and escaped within a day or two, the loss would be partial only, limited to the costs of escape; and (ii) where a vessel was taken and released on payment of a ransom, the loss would be partial, confined to the ransom sum.

83 Merkin (n 81) [7-058].

84 Marine Insurance Act 1906, s 60(2)(i): 'In particular, there is a constructive total loss, (i)Where the assured is deprived of the possession of his ship or goods by a peril insured against, and (a) it is unlikely that he can recover the ship or goods, as the case may be, or (b) the cost of recovering the ship or goods, as the case may be, would exceed their value when recovered.'

85 [1915] 1 KB 922 (CA).

suspicion of carrying contraband. After six weeks of detention, the assured claimed a CTL. To succeed, the assured had to establish conclusively two points: first, that at the time this action was initiated, they had been deprived of possession of the *Polurrian*; and second, that it was not merely doubtful whether the vessel would be recovered within a reasonable period, but the recovery was more probably impossible.[86] The Court of Appeal rejected the claim, holding that although recovery was uncertain, it could not be regarded as unlikely.[87]

Warrington J drew a sharp distinction between uncertainty and the unlikelihood of recovery, stating:

> … [I]t is one thing to predicate that a total loss reasonably appears to be unavoidable and another to predicate that its recovery is unlikely … the test of 'unlikelihood of recovery' has now been substituted for 'uncertainty of recovery'… the recovery of *Polurrian* by her owners was quite uncertain, [but] I do not feel myself justified in holding…that such recovery was 'unlikely'. This being so, the plaintiffs have failed to make out their case, and this appeal must be dismissed.[88]

This insistence on probabilistic unlikelihood, rather than mere doubt, establishes a demanding threshold for CTL claims. However, subsequent case law demonstrates a gradual doctrinal shift away from formalistic notions of possession towards a more functional understanding of deprivation.

By contrast, *The Bamburi*[89] recognised that functional deprivation, even in the absence of physical boarding or dispossession, may be sufficient to trigger CTL, where the owner is wholly deprived of meaningful use of the vessel. In that case, the vessel was indefinitely detained in Iraq during the Iran-Iraq war. Although crew members remained on board and no foreign authority asserted ownership over the vessel, Staughton J adopted a broader conception of 'deprivation of possession,' observing:[90]

---

[86] Gürses (n 77) 313.
[87] *Polurrian* (n 85).
[88] Ibid.
[89] [1982] 1 Lloyd's Rep 312.
[90] Ibid.

> The concept of possession in English law was never simple … if possession has its narrowest legal significance in the present case, the claimants have not been deprived of it. There are still four crew members on board … there is no Iraqi presence on board; and neither the Iraqi nor the Iranian government asserts any right to, interest in or claim over the vessel. On the other hand … the owners have been wholly deprived of the free use and disposal of their vessel. All movement is prohibited… and she must remain as idle as a painted ship.

This reasoning establishes that deprivation may be assessed by reference to practical control and utility, rather than formal possession alone. *The Bamburi* thus represents a significant doctrinal development: it is no longer necessary to show that a hostile party has physically boarded or taken formal possession of the vessel; it is sufficient that the owner has been deprived of all free use and disposal of it.

The approach was further affirmed in *Navigators Insurance Co Ltd v Atlasnavios-Navegacao LDA*, where the Supreme Court held that unlawful detention for a continuous period of six months constituted a CTL.[91] It is important, however, to distinguish this judicial finding from the contractual deemed CTL provisions found in standard policy wordings. The Institute War and Strikes Clauses Hulls-Time (1/11/95) provide that where the vessel is deprived of free use and disposal for a continuous period of 12 months, the assured may treat the vessel as a constructive total loss.[92] The six-month period in *Navigators* was therefore a fact-specific judicial assessment under particular policy language and does not establish a general threshold applicable to all policies.

---

[91] '… which is relevant under the wording of this policy; detection, detainment and its continuation for a period of at least six continuous months were equally essential contributing causes of any loss'*: Navigators Insurance Co Ltd v Atlasnavios-Navegacao LDA (formerly Bnavios-Navegacao LDA)* [2018] UKSC 26, [2019] AC 136 [43] (Lord Mance DPSC).

[92] Institute War and Strikes Clauses Hulls-Time (1/11/95), cl 3 (Detainment): 'In the event that the Vessel shall have been the subject of capture seizure arrest restraint detainment confiscation or expropriation, and the Assured shall thereby have lost the free use and disposal of the Vessel for a continuous period of 12 months then for the purpose of ascertaining whether the Vessel is a constructive total loss the Assured shall be deemed to have been deprived of the possession of the Vessel without any likelihood of recovery.'

The existence of a CTL is determined by objective facts,[93] and where such facts are prospective or unknown, the assessment must be based on a reasonable evaluation of probabilities.[94] The court must assess the position as it stood at the time of the notice of abandonment or the commencement of proceedings, not with the benefit of hindsight. This probabilistic inquiry is of particular significance when considering deprivation arising from non-physical causes.

In the context of marine insurance, a cyber-attack may temporarily disable a vessel's navigation or otherwise prevent its operation, depriving the owner of effective operational control. Crucially, however, such attacks do not entail a transfer of ownership or legal possession; the vessel remains formally under the owner's title. Unlike traditional capture, cyber-induced immobilisation does not place the vessel in the hands of a captor in the conventional sense. This raises the central question: whether deprivation of operational control, absent physical seizure, can satisfy the CTL threshold under s. 60.

Although contextually distinct from traditional capture, cyber-attacks may produce functional consequences that engage the CTL framework. In August 2025, the hacker group Lab-Dookhtegan disrupted communications on over 60 Iranian tankers and cargo vessels[95] by gaining root-level access to their Linux-based satellite control systems.[96] The group stated that full restoration of communications would take several weeks.[97] Applying the *Polurrian* standard to these facts, the question is whether, at the point the owners became aware of the disruption, recovery of operational control within a reasonable time could be regarded as 'unlikely' rather than merely uncertain.

Given the group's own acknowledgement that restoration would require several weeks, and the scale of the disruption across an entire fleet, there is a credible argument that the unlikelihood threshold under s 60(2)(i) could be satisfied on such facts. The owners were,

---

93 '… The test is an objective test and the Court must determine, on the basis of the evidence the cost of the reasonably necessary repairs …' (Jeremy Lionel Cooke IJ) in *PT Adidaya Energy Mandiri v MS First Capital Insurance Ltd* [2022] SGHC(I) 14, [2023] Lloyd's Rep IR 143 [175].

94 Gürses (n 77) 300.

95 This attack targeted conventional ship fleets; however, if it were to occur against autonomous vessels, the resulting damage would likely be significantly more catastrophic.

96 Gary Dixon, 'Hackers disable communications on more than 60 Iranian tankers and cargo ships' (Trade Winds, August 2025) <https://www.tradewindsnews.com/tankers/hackers-disable-communications-on-more-than-60-iranian-tankers-and-cargo-ships/2-1-1861711> accessed 22 April 2026.

97 Ibid.

moreover, wholly deprived of free use and disposal of their vessels during the period of disruption, which is the functional equivalent of the deprivation recognised in *The Bamburi*. Whether such deprivation would constitute a CTL in any given case is a question of objective assessment and must be determined by reference to the specific policy wording.

Under the MIA 1906, a CTL arises only where recovery is unlikely,[98] and many policies further specify a minimum period of deprivation before CTL is triggered. In principle, however, there is no reason why the same logic should not apply to cyber-induced deprivation, including the above incidents involving multiple vessels or even an entire fleet, provided the policy wording permits.

From the standpoint of legal coherence and justice, the same principles ought to govern regardless of the nature of the peril. The doctrinal rationale of CTL lies not in the form of the peril but in its effect: the deprivation of the assured's ability to use or control the insured property. Although cyber-attacks may not involve an 'overt' act in the traditional sense or produce immediately visible effects, they may nonetheless satisfy the criteria for deprivation. Therefore, extending the CTL principles to cover cyber-induced immobilisation aligns with the broader purpose of marine insurance law, namely, to provide a remedy where the assured has lost the practical benefit of the insured vessel.

Ultimately, the law is concerned not only with physical seizures but also with the loss of control and operational capacity. Situating cyber-attacks within this framework underscores the need for doctrinal adaptation in response to technological change. Such adaptation ensures that marine insurance remains capable of addressing modern operational risks.

Building on this foundation, the following section addresses the central research question of this paper: can – and should – a cyber-attack on a mobilised vessel be classified as a peril of capture or seizure under marine insurance law?

[98] MIA 1906, s 60(2)(i).

5 'Should' cyber-attacks be classified as capture or seizure?

Under standard marine insurance practice, a cyber-attack alone is not treated as a capture or seizure,[99] as coverage under such policies typically requires physical intervention and intent to deprive the owner of the vessel. Traditional doctrines, largely developed in the nineteenth and early twentieth centuries,[100] fail to accommodate the intangible and non-physical nature of cyber perils. As a result, the existing marine insurance regime has yet to evolve fully in response to these risks.

However, the consequences of a cyber-attack may, in certain circumstances, constitute a covered peril, particularly where cyber intrusion facilitates or results in physical seizure or effective control over the vessel. In practice, cyber risks are frequently excluded by default through various cyber exclusion clauses,[101] requiring either a specific endorsement or a standalone cyber policy to provide coverage for cyber-related risks. Such instruments define the scope of coverage and specify the conditions under which a cyber-related event qualifies as an insurable loss.

6 Evaluating the arguments

The primary objection to classifying cyber-related risks as capture or seizure, consistently emphasised in the case law,[102] is that these perils have traditionally required physical dispossession. In the absence of such tangible deprivation, a cyber incident cannot, in strict doctrinal terms, satisfy the criteria for capture or seizure. While cyber-attacks may be profoundly disruptive, they do not involve the physical transfer of possession of the vessel from its lawful owner.[103] That being said, as illustrated in *Johnston & Co v Hogg,* the intention to deprive permanently is not a prerequisite.[104] Consequently, the temporary hostage-taking

[99] For insured perils, see MIA 1906, s 3(2)(c).

[100] See generally early case law and MIA 1906 & Institute War and Strikes Clauses 1983.

[101] CL 380, LMA 5402, and LMA 5403 explicitly exclude losses caused by cyber incidents, unless a separate cyber insurance policy is purchased. For other non-marine cyber war clauses published by Lloyd's Market Association, please see the exhaustive list here: <https://www.lmalloyds.com/LMA/Underwriting/Non-Marine/Cyber_Clauses/cyber_war_clauses.aspx> accessed 22 April 2026.

[102] *Cory* (n 9); *Kuwait Airways Corp* (n 74); *Polurrian* (n 85).

[103] In *Hogg* (n 46), the court also did not require an initial or ongoing intention to permanently deprive the owner of their property, which is similar to the case in cyber-attacks.

[104] Ibid.

of a vessel, whether autonomous or otherwise, for purposes such as extorting ransom or accessing sensitive systems, aligns with the traditional understanding of the peril. Although the method may be non-physical, the underlying elements of coercion, disruption, and loss of control closely mirror those inherent in capture and seizure.

From this perspective, a purposive interpretation of the relevant provision, focusing on the underlying intent rather than literal wording, may support the argument that deprivation of use or control over a vessel, its cargo, or related systems constitutes a functional equivalent of physical dispossession. On that basis, such deprivation could suffice to meet the criterion for the peril.

A further challenge arises from market practice, which has historically differentiated cyber risks from conventional perils through the widespread use of cyber exclusion clauses[105] and the development of standalone cyber insurance policies. Where coverage is specifically tailored to cyber risks, standard clauses neither contemplate nor extend to such risks, as they fall outside the policy wording. This approach is both doctrinally and commercially coherent.

It is not suggested, however, that the doctrines of capture and seizure should be automatically extended to cover cyber risks in their current form. Instead, with carefully refined definitions and the development of hybrid policy structures, it may be conceivable to extend coverage in a manner consistent with the underlying principles of the peril. By explicitly integrating cyber elements into policy language– through, for example, a refined conception of 'force' or a precise articulation of what constitutes deprivation of property– standard clauses could, in appropriate circumstances, be adapted to address cyber risks.

The increasing integration of AI and machine learning into Degree two and higher automation systems introduces an additional layer of complexity. If a third party manipulates these AI decision-making models to seize control of the vessel, without deploying physical force or directly interfacing with the ship's command systems, could such manipulation constitute 'force' in the legal sense? Could a code injection or algorithmic rerouting, entirely devoid of physical presence, qualify as a seizure if it results in a total loss of functional control? These

[105] Above (n 101).

questions highlight the difficulty of interpreting 'actual force' in cyber contexts and whether digital acts alone can satisfy traditional legal requirements under maritime law.

A few precedents provide guidance. Authorities such as *Cory,*[106] *Robinson Gold Mining Co,*[107] and *The Minden*[108] emphasise that some degree of physical force is generally required. However, in *Bayview Motors Ltd,*[109] the courts recognised that the threat of force or its indications may suffice. Translated to the digital context, a cyber threat against MASS, through unauthorised system access or encryption of essential functions, could meet this threshold, even in the absence of physical intervention. Expanding the definitions of 'capture' and 'seizure' to encompass cyber risks thus reflects the evolving nature of maritime threats, recognising that control and coercion may now be exercised digitally.

For Degree 1 and 2 automation, if a limited crew on board is compelled to follow the orders from hackers following a physical or digital takeover, does this constitute capture and seizure when control is exercised indirectly? According to *Anita,*[110] the answer is affirmative. When the crew is forced to obey a third party rather than the shipowner, possession is effectively lost,[111] amounting to capture and seizure.

Similarly, if a crew member (for Degree 2) or remote-control centre staff [112] (for Degrees 2 and 3) were to hack the vessel, could this qualify as capture and seizure? Under *The Salem,*[113] abuse of possession by the shipowner does not constitute 'taking at sea.' However, cases such as *Naylor v Palmer*[114] and *Kleinwort v Shepard*[115] demonstrate that when control is taken by others, such as passengers or immigrants, it qualifies as a seizure. By analogy, internal cyber takeovers on MASS could likewise fall within this peril.

---

[106] Above (n 9).
[107] Above (n 44).
[108] Above (n 57).
[109] Above (n 52).
[110] Above (n 62).
[111] Ibid.
[112] In this scenario, remote control operators are recognised and treated as part of the crew; however, it is also conceivable that they could instead be classified differently.
[113] Above (n 64).
[114] Above (n 66).
[115] Above (n 68).

This distinction is particularly significant for MASS. Suppose a remote-control operator (for Degree 3) or an onboard technician (for Degree 2) initiates or facilitates a cyber-attack, the classification depends on whether their actions were trust-based and whether they exceeded the scope of their authority. Courts may need to reconsider whether digital acts that disrupt the command hierarchy, without a traditional 'taking,' can nonetheless be treated as capture or seizure.

In practice, when control of a MASS is seized by a trusted party, such as the crew or remote-control staff, it is generally not classified as capture and seizure, since these individuals already hold lawful possession and are merely abusing entrusted authority. Conversely, when control is taken by unauthorised individuals, whether onboard, such as passengers or external hackers, it falls within the definition of capture and seizure. In the cyber context, unauthorised access and control over the vessel systems mirrors the traditional elements of capture and seizure, despite the absence of a physical takeover.

Beyond the question of possession, the motives behind cyber interference often resemble those associated with traditional capture and seizure, driven by strategic, economic, or coercive objectives. While courts are unlikely to broaden the definition of force absent explicit policy language, shifts in judicial interpretation suggest a potential basis for doctrinal evolution to accommodate modern maritime risks. From a motivational standpoint, only cyber-attacks undertaken for political or military purposes,[116] rather than personal[117] or financial[118] reasons, fall within the narrow scope comparable to traditional capture and seizure.

7 Policy solution: Hybrid insurance

Historically, the perils of capture and seizure have been closely associated with physical dispossession. However, this conceptualisation requires reconsideration. Today's maritime landscape, with autonomous vessels and escalating cyber threats, renders standard clauses and century-old definitions increasingly outdated. While it is understandable that courts may

[116] *Banque Monetaca & Carystuiaki* (n 50).
[117] *Bayview Motors Ltd* (n 52).
[118] See Verizon Data Breach Investigations (2025) Report (n 33).

be cautious in extending traditional definitions too far, given the potential for uncertainty and the scarcity of case law addressing cyber-attacks on autonomous ships, the evolution of maritime technology and risk necessitates a degree of interpretative flexibility.

Although the law maintains a requirement of physicality, cyber-attacks can produce functionally equivalent deprivation of control and operational capacity. Such equivalence should not be disregarded when assessing capture and seizure in modern marine insurance. Accordingly, while cyber-attacks can incapacitate a vessel as effectively as a traditional seizure, the current legal framework inadequately accommodates these intangible perils.

To address the growing risk of cyber-induced capture or seizure on MASS, insurance policies should adopt hybrid coverage models that cover both digital breaches and their operational consequences. This is particularly critical when cyber-attacks directly increase the likelihood of physical vessel capture, for instance, by interfering with navigation or communication systems, leaving a ship exposed to pirates or hostile actors. Hybrid policies should explicitly cover losses resulting from cyber-related capture or seizure incidents. The aim of hybrid coverage is to provide comprehensive protection against both digital and physical risks, which are closely interconnected and make it impractical to address one without the other. For example, a hybrid policy could account for a cyber-attack that disrupts tracking systems, facilitating a hostile boarding that causes operational interruptions, ransom exposure, and physical damage.

Such hybrid policies offer comprehensive protection by incorporating cyber risks into traditional coverage. While premiums may increase to reflect additional exposure, this is likely more manageable than creating a standalone cyber policy, given the operational complexities and uncertainties associated with MASS technologies. Furthermore, separating cyber and physical coverage could leave critical gaps, which hybrid models are designed to address.

In conclusion, cyber risks should be considered alongside capture and seizure perils for conventional and autonomous vessels, as they share fundamental characteristics, including forcible possession, unauthorised access, and exposure to external threats. Nevertheless, the specific motivations behind attacks and the nature of the force involved require careful delineation. To ensure comprehensive coverage, policy language should explicitly address

these considerations, whether through hybrid coverage arrangements or refined definitions of the peril itself.

8 Conclusion

The shift from manned to autonomous vessels represents a profound transformation in the maritime sector, offering significant opportunities while simultaneously introducing complex, unprecedented risks that challenge existing legal and insurance frameworks. Cyber-driven operational disruptions that may result in vessel capture or seizure highlight the limitations of traditional marine insurance policies, which were not designed to address advanced technological systems.

Through case studies and real-world examples, this paper shows that cyberattacks can materially increase the risk of hostile boarding, hijacking, or unlawful seizure. Yet, broad cyber exclusions and ambiguous causation between cyber and physical risks leave MASS operators facing uncertainty and inadequate coverage.

Cyber-attacks are inherently intangible, often anonymous, and generally lack visible coercive force. Nevertheless, they can inflict losses functionally equivalent to those arising from traditional capture and seizure. While they do not entail physical possession, cyber-attacks can materially impair or entirely obstruct the shipowner's ability to operate the vessel, overlapping with the principles of capture and seizure and reflecting comparable deprivation of control and economic use. A broad interpretation of 'capture and seizure' could encompass cyber-induced loss of control, subject to the policy's specific terms. Cases such as *Cory*[119] and *Robinson Gold Mining Co*[120] link taking to physical coercion. By contrast, cyber-attacks can disrupt or hijack digital systems, redirecting or immobilising the vessels without physical harm.

Threats of system shutdowns, ransom demands, or data breaches may effectively coerce compliance, aligning with the principle in *Bayview Motors Ltd*,[121] which recognises that threats or indications of harm can fulfil the requirement of force. Accordingly, cyber capture and

[119] *Cory* (n 9).
[120] *Robinson Gold Mining* (n 44).
[121] Above (n 52).

seizure can be understood as the loss of operational control over the vessel, potentially constituting a CTL despite the vessel's physical integrity.

Functional similarities between cyber-attacks and traditional capture or seizure are clear, but acknowledging this in practice requires explicit updates to the Institute Clauses or the introduction of dedicated cyber-specific provisions as part of hybrid insurance policies. The framework established by MIA 1906 and standard clauses is ill-suited to modern cyber risks, highlighting the need for contractual and potentially statutory reform.

To support a resilient legal framework, marine insurance must evolve. Hybrid insurance models that integrate both cyber and physical loss coverage provide a practical solution, requiring re-examination of conventional maritime risks and reconsideration of causation in an era where cyber-enabled interventions may trigger incidents. Consequently, while direct physical capture remains the traditional understanding, a cyber-attack that deprives an autonomous ship of control could potentially fall under the peril of capture and seizure, provided the policy language and circumstances support such an interpretation.