NUS Centre for Maritime Law Working Paper 24/07

NUS Law Working Paper 24/012

CYBERSECURITY BREACHES AND ATTACKS: A NEW ERA OF PIRACY, ACTS OF WAR, AND TERRORISM?

Elizaveta Katerina Nteeva

Research Fellow, Centre for Maritime Law

[Uploaded November 2024]

Cybersecurity breaches and attacks: a new era of piracy, acts of war, and terrorism?

Elizaveta Katerina Nteeva[*]

ABSTRACT

The introduction of digitalisation to shipping and increasing interconnectivity and automation both ashore and onboard inevitably leads to new risks associated with cybersecurity. These add to dangers such as piracy, terrorism, and war risks, which already exist.

This paper will examine whether there is a difference between cybersecurity breaches and cyber-attacks. This may require consideration of whether one is a prerequisite for the other, whether they can (co)exist separately, and whether these two events can be perceived as distinct risks. The paper reviews the existing coverage available for the risks of piracy, terrorism, and war and then considers whether new emerging risks can be included within the existing concepts.

Emerging piracy and terrorism in cyberspace may mean that existing insurance coverage is not fit for purpose. This paper will examine a new category of risks, 'cyber-piracy' and 'cyber-terrorism', which may be managed with tailor-made coverage.

This paper will also study the impact of cyber insecurity and the vulnerability of existing systems. Finally, based on a review of the existing literature, the paper tries to answer who will most likely undertake the costs of these new risks.

Keywords: Marine insurance; Cyber-security; piracy; terrorism; war risks; autonomous vessels.

---

[*] Research Fellow, Centre for Maritime Law, NUS. The author would like to thank Professor Stephen Girvin for his valuable revisions, suggestions, and mentorship and Richard Kilpatrick Jr for his comments and suggestions. The usual disclaimer applies.

Cybersecurity breaches and attacks: a new era of piracy, acts of war, and terrorism?

1 Historical background

1.1 Piracy

Piracy historically was first depicted in ancient Greece,[1] the Roman Empire,[2] and during Viking times.[3] In Athens, for instance, piracy[4] enabled Athenians to become richer overseas. Thus, an Athenian in 4 BCE who sold his land and bought a trireme in which he sailed to Crete, presumably in a plundering expedition, is an example of an individual motivated by a private interest in gaining wealth.[5] Another example of piracy can be found in Syracuse, Italy, where pirates and mercenaries were not easily distinguishable.[6] Robbers of the seas and notorious pirates,[7] usually known as *hostes humani generis*[8] (or enemies of the human race[9]), closely followed merchandisers as they discovered new routes to transfer their goods.

---

1 Matthew Trundle, 'The Limits of Nationalism: Brigandage: Piracy and Mercenary Service in Fourth Century BCE Athens' in Richard Evans and Martine de Marre (eds), *Piracy, Pillage and Plunder in Antiquity: Appropriation and the Ancient World* (Routledge 2020). See also the leading study by Philip de Souza, *Piracy in the Graeco-Roman World* (CUP 1999).

2 See Alfred P Rubin, *The Law of Piracy* (2nd edn, Transnational Publishers Inc 1998) 6-19; Aaron L Beek, 'Campaigning Against Pirate Mercenaries? A Very Roman Strategy?' in Evans and de Marre (n 1).

3 See Rob Merkin, *Marine Insurance, A Legal History* vol 1 (Edward Elgar Publishing 2021) [1-007-1.008].

4 Cf Rubin (n 2) 2-6 who disagrees with the meaning of piracy in ancient times.

5 See Trundle (n 1) 28-34.

6 See further, Richard Evans, 'Piracy and Pseudo-Piracy in Classical Syracuse: Financial replenishment through outsourcing, sacking Temples and Forced Migrations' in Evans and de Marre (n 1) 38-42.

7 This included women. See 'The Extraordinary Life of Grace O'Malley' (Royal Museum Greenwich): <https://www.rmg.co.uk/stories/grace-o-malley-pirate-history-fact-fiction-legend> accessed 2 August 2024.

8 See the opinion of Wilmot CJ referring to pirates as *hostes humani generis* and falling within the description of foreign enemies in the insurance clause 'invasion and foreign enemy', being a hostile attack upon the nation: *Drinkwater v The Royal Exchange Assurance Co* (1767) Wilm 282, 290. Cf *Republic of Bolivia v Indemnity Mutual Marine Assurance Co Ltd* [1909] 1 KB 785 (CA), 804, where Kennedy LJ distinguished pirates as *hostes humani generis* acting for their private gain, from those seizing insured goods from a vessel 'in furtherance of a political adventure'.

9 Longmore LJ refers to pirates as 'enemies of the human race' and falling within the exemption of 'public enemies' in Art IV, r 2(f) of the Hague Rules and the Hague-Visby Rules: see *Trafigura Beheer BV v Navigazione Montanari SpA (The Valle di Cordoba)* [2015] EWCA Civ 91, [2015] 1 Lloyd's Rep 529, [2].

Piracy was the first stage of criminal activity against commercial vessels. The distinctive motivation of private gain as opposed to the service to the state[10] can be used to distinguish privateers from pirates, but this is not always so clear either.[11] The legal definition could be separated into two situations: actions which were either recognised or not by domestic law as piratical[12] and actions against the universal law and all mankind.[13] The term piracy describes many different notions, depending on the time, the source cited, and even the origin[14] and perception of the source.[15] The fact that piracy is sometimes included as a war risk can be explained because, during times of war, privateers[16] were allowed by Letters of Marque to seize enemy property or property destined for the enemy and take this 'prize' to the competent court to sell them and receive part of the proceeds. [17] A Letter of Reprisal, [18] issued during times of peace, followed the seizure of the vessel of the letter's holder and allowed him to retaliate by seizing a vessel of the nation from where the first seizure initiator came.[19]

Another point of interest related to the capture of the vessel. English privateers took hostages to secure ransom payments, and sometimes, the captain or a crew member volunteered to undertake such a role. The captain or crew were sometimes compensated for their lost wages

---

[10] Merkin describes the acts of belligerents during wartime or under state license as not being acts of piracy: see (n 3) [1-008]; *Marshes v Palachies* (1615) 1 Polle 175.

[11] Attacks by privateers during times of peace led to them being treated as pirates: Merkin, ibid; *The Diamond* (1602) SS XL.

[12] If this happened on the high seas, the common law courts would not recognise them as piratical: Merkin, ibid; *The Hercules* (1819) 2 Dods 353.

[13] Merkin, ibid [1-088–1-089].

[14] Thus, Sir Thomas Stamford Raffles, in his letters, referred to the Malayan aristocracy conducting piracy: see Rubin (n 4) 1-2. For a fuller treatment, see Donald B Freeman, *The Straits of Malacca: Gateway or Gauntlett?* (McGill-Queen's UP 2003) ch 18; Stefan Eklöf Amirell, *Pirates of Empire: Colonisation and Maritime Violence in Southeast Asia* (CUP 2019) 103 et seq.

[15] Thus, for example, Rubin (n 2) distinguishes between six different meanings of piracy.

[16] Similar situations existed both in the Mediterranean and the Atlantic and Caribbean where the theoretical distinction between the lawful raiders (similar to privateers) and raiders without licencing during peacetime was not easy to make in practice: see John D Ford, *The Emergence of Privateering* (Brill Nijhoff 2023) 204.

[17] Letters of Marque were based on thirteenth-century treaties, and until the growth of the number of privateers in the seventeenth century, the Letters of Marque were used to describe Letters of Reprisal, which provided for the right of seizure during peaceful times: see Merkin (n 3) [1-091–1-140].

[18] Unlike in times of war, a license had to be obtained before the seizure of the ship and the goods. A court decision had to follow in order to allow the lawful possession of the obtained in reprisal: Ford (n 16) ch 1.

[19] Ibid, [1-107–1-108].

and food expenses while imprisoned, with their claims secured against the vessel initially seized.[20] Ransom bonds were enforceable and partially paid by insurers, with the gold and silver used exempted from export restrictions. The Admiralty controlled the privateers and warships regarding ransom, and it became a necessity in the mid-eighteenth century, followed by a complete ban at the end of the eighteenth century.[21]

Piracy has been defined in the case law as (1) a robbery or forcible depredation upon the high seas with felonious intent, irrespective if the attempt was successful or frustrated,[22] (2) private acts of hatred, revenge or abuse of power without the robbery against another ship or by the revolted crew or passengers against their own ship[23] (3) hostilities done without authorisation from a specific state,[24] (4) happening in the high sea, territorial sea and inland waterways like lakes and rivers,[25] (5) by person(s) motivated by their personal gain or vengeance rather than by 'public, political, religious or ideological nature'.[26] Additional characteristics are that the theft or attack must be carried out from the vessel against coastal property or from the shore against the vessel, must be successful, and that violence or the threat or the intention to use it must be present.[27]

After the United Nations Convention on the Law of the Sea (UNCLOS) entered into force, piracy as an action committed on the high seas was regulated in Arts 100-107.[28] The definition of piracy in Art 101 was tighter than the one adopted through the centuries of the common law

---

[20] *Wilson v Bird* (1694) 1 Ld Raym 22; *Jamieson v Hutton* (1753) Mor 2023; *Loch v Home* (1769) Mor 2025; *Yates v Hall* (1785) 1 TR 73; *Hope v Winter* (1709) 2 Eq Ca Aber 690. See also ibid, [1-135].

[21] Ransom payments were banned by the Ransom Act 1782, 22 Geo 3, c 25. See also ibid, [1-136].

[22] Peter MacDonald Eggers QC, 'What is a Pirate? A Common Law Answer to an Age-old Question' in Douglas Guilfoyle (ed), *Modern Piracy: Legal Challenges and Responses* (Edward Elgar Publishing 2013) 252–255.

[23] Ibid, 255–262.

[24] Ibid.

[25] Ibid, 261–262.

[26] Ibid 263–265.

[27] Ibid 265–266.

[28] See <https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf> accessed 3 May 2024 and the discussion below in 2.3.

jurisprudence.[29] IMO Resolution A.922 (22) introduced the notion of armed robbery in territorial seas.[30] Further, actions that were similar to both piracy and armed robbery but had political reasons behind them, rather than the hijacking of the vessel, kidnapping of the crew, and demanding of a ransom for the crew and the cargo and the vessel, were named terrorism and regulated separately.[31]

1.2 Terrorism

Terrorism developed differently. It started with maritime attacks of non-state actors in the 1970s and 1980s with various demands relating to various groups. However, this resulted in only a few fatalities.[32] The situation changed in the 1990s when fatalities increased. It has continued to grow in the noughties with suicide attacks.[33] As is widely known, Houthis use small craft and sometimes uncrewed boats to attack vessels off the coasts of Yemen and in the Red Sea.[34]

1.3 War risks

War risks were originally part of the marine perils.[35] They were covered together with piracy under the SG Form from the seventeenth century until the end of the nineteenth century. From 1756 to 1815, blockades, embargoes, and privateering over enemy vessels increased

---

[29] MacDonald Eggers QC (n 22) 266 – 267.

[30] Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships adopted by the 22nd regular session of the IMO Assembly, as amended by the Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery Against Ships, adopted on 2 December 2009 by Resolution A.1025(26) of the IMO Assembly, <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/A.1025.pdf> accessed 3 May 2024. The definition of piracy in art 2.1 follows the definition in UNCLOS, art 101 <https://www.imo.org/en/OurWork/Security/Pages/PiracyArmedRobberydefault.aspx> accessed 3 May 2024.

[31] See International Convention for the Suppression of the Financing of Terrorism, <https://treaties.un.org/doc/db/terrorism/english-18-11.pdf> accessed 3 May 2024.

[32] See further Robin Bowley, *Preventing Terrorist Attacks at Sea: Maritime Terrorism Risk and International Law* (Routledge 2023) 24.

[33] Ibid, 25.

[34] See further, 'Recent Incidents, United Kingdom Maritime Trade Operations' (UKMTO) <https://www.ukmto.org/indian-ocean/recent-incidents> accessed 28 August 2024.

[35] Mark Templeman KC et al, *Arnould: Law of Marine Insurance and Average* (21st edn, Sweet & Maxwell 2024) [2-39].

exponentially, leading to the exclusion of capture and seizure coverage from insurance contracts covering marine perils.[36] The wording of marine perils insurance initially incorporated terms like 'men of war',[37] and the fact of war was considered a matter of common knowledge that did not have to be disclosed by the assured.[38] Additionally, the protection of vessels against privateers and war risks in the form of policy requirements for minimum numbers of guns and crew meant that there were warranties for those prerequisites, and non-compliance would lead to the discharging of the insurers.[39]

This marked the beginning of a separate insurance contract covering war and warlike risks.[40] The FC & S Clause excludes war risks,[41] and today, the Malicious Damage Clause (seen in the Institute Clauses of 1987, 2006 and later) was imported into the War Risk Policy.[42] The War and Strikes insurance, separate from marine insurance, would cover every war risk, including terrorism, except losses, damages or liabilities caused by nuclear energy or weapons.[43] This, however, has a drawback if the assured has to simultaneously sue his marine and war risk insurers when the causes of a loss cannot be attributed to marine or war risks.[44]

---

[36] Thus, during the American War of Independence in August 1780, the combined French and Spanish fleets captured a convoy of British ships carrying commercial cargo and military supplies, resulting in losses so significant that some underwriters went bankrupt: Merkin (n 3) [6-004–6-005].

[37] Ibid, [6.025–6.026].

[38] Ibid, [6.071–6.072].

[39] As noted in *Pawson v Watson* (1778) 2 Cowp 785; ibid, [6-099].

[40] Richard L Kilpatrick Jr, 'Revisiting the Five Powers War Risk Exclusion' (2024) 73 ICLQ 551.

[41] Part of the war risks cover was provided by way of exclusion of the FC &S Clause from the SG Form and reinstatement would be provided by the Institute Clauses incorporated into the insurance contract: Arnould (n 35) [2-39].

[42] Michael Davey et al, *Miller's Marine War Risks* (4th edn, Informa Law from Routledge 2020) [1.8–1.9]; [1.25–1.27].

[43] Ibid, [1.27].

[44] Ibid, [1.29–1.30]; Arnould (n 35) [2-39]. See also *Munro Brice v War Risk Insurance Ltd* [1918] 2 KB 78.

2 Current risks for shipping

2.1 Piracy and armed robbery

Under English law, piracy is 'a robbery within the jurisdiction of the Admiralty',[45] and a pirate is someone who, to enrich himself, attacks merchants on the high seas and commits acts of robbery to obtain their goods.[46] Piracy affects not only the vessel and the crew but also the relationship between the charterer and the shipowner when disputing whether a charterparty off-hire clause[47] or a piracy clause covers piracy[48] Piracy can also affect a port's security level and give a shipowner the right to refuse to operate in an endangered area, to ask for additional insurance, or to demand hire even after the pirates seize the vessel.[49]

Piracy in its modern form remains a threat to global shipping[50] with pirates continuing to board and hijack vessels. However, unlike their historical predecessors,[51] modern pirates are also interested in taking hostages and asking for ransom, not simply stealing the vessel with its cargo and forcing the crew to abandon the ship.[52] Piracy in the twentieth century could lead to the

---

[45] *Attorney-General for Hong Kong v Kwok-a-Sing* LR 5 PC 179, 200 (Mellish LJ), quoting Holt CJ in *R v Dawson* (1696) 12 St Tr 451. See also *China Navigation Co Ltd v Attorney-General* [1932] 2 KB 197 (CA).

[46] See, further, *China Navigation*, ibid, quoting *Hawkins' Pleas of the Crown*, Vol 1, 251.

[47] Stephen Girvin, *Carriage of Goods by Sea* (3rd edn, OUP 2022) [34.82-34.83].

[48] Ibid [34.103].

[49] Ibid [21.48]. See, eg, *COSCO Bulk Carrier Co Ltd v Team-Up Owning Co Ltd (The Saldanha)* [2010] EWHC 1340 (Comm), [2011] 1 Lloyd's Rep 187; *Osmium Shipping Corporation v Cargill International SA (The Captain Stefanos)* [2012] EWHC 571 (Comm), [2012] 2 Lloyd's Rep 46; *Herculito Maritime Ltd v Gunvor International BV (The Polar)* [2024] UKSC 2, [2024] 1 Lloyd's Rep 85.

[50] See ICC Commercial Crime Services, 'IMB Piracy & Armed Robbery Map 2024' <https://www.icc-ccs.org/piracy-reporting-centre/live-piracy-map> accessed 27 August 2024.

[51] See further Rob Merkin, *Marine Insurance: A Legal History* vol 2 (Edward Elgar Publishing 2021) [14-092]; *Attorney-General for Hong Kong* (n 45).

[52] In the eighteenth and nineteenth century, this usually meant the killing of the master and the crew: see *China Navigation* (n 45).

stealing of the vessel and the cargo, killing of the crew,[53] hijacking the vessel, kidnapping of the crew, and demanding a ransom for their release.[54]

Since 1986, statistics of cases involving piracy have shown an increase and a revival after decades of lower numbers of incidents. In 1992, this led to the creation of the International Maritime Bureau (IMB) Piracy Reporting Centre by the International Commercial Chamber (ICC)[55] and further enhanced by the establishment in 2006 of the Information Sharing Center (ISC) of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP).[56] A vivid depiction can be drawn from the statistical data from the five years from 2007 to 2011,[57] which was a tipping point of piracy and armed robbery incidents, and comparing this with data from 2010 to 2022.[58]

A distinction must be made when reviewing different data depicting the incidents of piracy and armed robbery worldwide from the data for such incidents in Asia. Thus, for the five years from 2007 to 2011, the IMB reports show a constant increase from 263 in 2007 to 293 in 2008, followed by a rapid increase to 410 in 2009, 445 in 2010, and a decrease in 2011 to 439 incidents. Most of

---

[53] Paul Todd, *Maritime Fraud and Piracy* (2nd edn, Lloyd's List 2010) 1–2; *Petroships Pte Ltd v Petec Trading and Investment Corp (The Petro Ranger)* [2000] 2 Lloyd's Rep 348.

[54] See Joshua Minchin, 'EU Issues Piracy Warning After Abdullah Release' *Lloyd's List* (London, 16 April 2024); Richard Meade, 'Somali Piracy is Back and a Show of Force From India May not be Enough to Stop it' *Lloyd's List* (London, 25 March 2024).

[55] International Maritime Bureau, ICC Commercial Crime Services <https://www.icc-ccs.org/index.php/icc/imb> accessed 8 August 2024.

[56] Agreed on 11 November 2004. See ReCAAP Information Sharing Centre, 'About ReCAAP Information Sharing Centre' (ReCAAP ISC, 2023) <https://www.recaap.org/about_ReCAAP-ISC> accessed 5 August 2024.

[57] See further Hideshi Ueno, 'Piracy and Armed Robbery Against Ships in the Year 2011 from IMB Annual Report' (From the Oceans, Sasakawa Pearce Foundation, Intelligence Analysis, January 2012) tabs 3; 5 <https://www.spf.org/oceans/analysis_en/c1201-1.html> accessed 5 August 2024; ReCAAP Information Sharing Centre, 'ReCAAP Information Sharing Centre's Classification of Piracy and Armed Robbery Incidents' (ReCAAP ISC, 2023) <https://www.recaap.org/classification_of_incidents> accessed 5 August 2024.

[58] Martin Placek, 'Pirate Attacks – Statistics and Facts' (Statista, 10 January 2024) <https://www.statista.com/topics/1290/pirate-attacks/> accessed 2 August 2024. The IMB figures depict both armed robberies and piracy. Thus, from the 439 reported incidents (both of piracy and of armed robbery), 221 were actual attacks, and 218 were attempted attacks. In contrast, out of the total of 895 incidents of violence against vessels involved in the incidents, 802 represented hostage situations, 42 injuries, 27 threats, 10 kidnappings, 8 killed and 6 assaulted crew members: see Ueno, ibid.

the incidents in 2008 and 2009 were in the Gulf of Aden, attributable to Somali pirates, and in 2010, the Somalian coast took the lead in numbers.[59]

During the same period, as per the ReCAAP, the numbers from 100 in 2007 fell to 96 in 2008 and slightly increased to 102 in 2009. They reached 167 in 2010 and again dropped to 155 in 2011. For these reasons, regional tendencies must be examined separately from those occurring globally. The ReCAAP reports classify all incidents as follows: a) CAT 1, with a large number of armed perpetrators and with the ship hijacked or cargo stolen; b) CAT 2, with fewer armed perpetrators and the crew threatened or held as hostages for a shorter period and the violence less severe; c) CAT 3, where the perpetrators are smaller in number and the crew was not harmed, but with minor losses to stores and engines spares; d) CAT 4, where perpetrators were small groups, not armed and the crew was not harmed and there was no theft.[60]

Multiple incidents are reported in Live Piracy and Armed Robbery Reports by the ICC Commercial Crime Services.[61] While practically eliminated in some areas, pirate attacks[62] and armed robbery incidents[63] are alarmingly persistent and even increasing in certain areas.[64] Due to geopolitical changes or when a particular route becomes more significant, the numbers can fluctuate from none to very many and vice versa in a matter of years or even months.[65]

---

[59] Above (n 57), tabs 3; 5.

[60] Ibid.

[61] See further 'Live Piracy & Armed Robbery Report 2023' (ICC Commercial Crime Services, 2023), <https://www.icc-ccs.org/index.php/piracy-reporting-centre/live-piracy-report/details/179/2149> accessed 8 August 2024.

[62] Four piracy incidents with hijacking have been reported during 2024: IMB Piracy and Armed Robbery Map 2024 ICC Commercial Crime Services, IMB Piracy & Armed Robbery Map 2024 <https://www.icc-ccs.org/index.php/piracy-reporting-centre/live-piracy-map/piracy-map-2019> accessed 8 August 2024.

[63] The majority of armed robbery incidents in 2024 appeared in the Singapore Straits, the Malacca Straits, and Indonesia, whereas substantially fewer incidents of boarding were reported in Bangladesh: IMB Piracy and Armed Robbery Map 2024 (n 62).

[64] See, eg, Chris Lo, 'Redrawing the Piracy Map for 2020' (Ship Technology Global, May 2020), <https://ship.nridigital.com/ship_may20/piracy_shipping_routes> accessed 2 August 2024.

[65] The coronavirus (COVID-19) pandemic saw the number of piracy attacks and armed robberies worldwide increase from 162 incidents in 2019 (the lowest number after the peak during the years 2010 and 2011) to 195 incidents in 2020. The next year, 2021, saw the numbers drop again to a new lowest amount on record at just 132 incidents: Placek (n 58).

Depending on the territory, the action might be piracy[66] (international seas) or armed robbery[67] (internal waters). For the present paper, 'piracy' is more expansive and can also include armed robbery when there is an action against the ship.[68]

Piracy is monitored mainly voluntarily, both internationally and regionally. Thus, the vessels, the member states to the IMO, the reporting organisations, and entities report the actual or attempted attacks by pirates or armed robbers against ships, and the data is uploaded to the GISIS (Global Integrated Shipping Information System).[69] The IMO also provides Maritime Facts and Figures with general statistics regarding shipping.[70] Finally, an additional source of information is BIMCO's Weekly Piracy Reports and Analysis,[71] which uses information provided by the US Office of Naval Intelligence Portal on a weekly and monthly basis.[72]

As noted earlier,[73] piracy is regulated by UNCLOS in Arts 100 to 107. The definition of piracy in Art 101(a) refers to 'any illegal acts of violence or detention, or any act of depredation' provided this is 'committed for private ends by the crew or passengers of a private ship' and directed 'on the high seas, against another ship … or against persons or property on board such ship …'[74] or 'against a ship … persons or property in a place outside the jurisdiction of any State'.[75] Piracy may

---

66 See IMB Piracy and Armed Robbery Map 2024 (n 62).

67 Ibid.

68 Cf also Aref Fakhry, 'Piracy across Maritime Law: Is there a Problem of Definition?' in Aldo Chircop, Ted McDorman and Norman Letalik (eds), *The Regulation of International Shipping: International and Comparative Perspectives* (Brill 2012) 97.

69 The IMO has open access piracy monthly and yearly reports of 'acts of piracy and armed robbery allegedly attempted against ships reported by Member States or International organizations in consultative status': see further IMO, 'Piracy Reports' <https://www.imo.org/en/OurWork/Security/Pages/Piracy-Reports-Default.aspx> accessed 8 August 2024.

70 See <https://www.imo.org/en/KnowledgeCentre/Pages/MaritimeFactsFigures-Default.aspx> accessed 8 August 2024.

71 Currently data is available of unclassified Worldwide Threat to Shipping (WTS) Reports from the Office of Naval Intelligence and the Kennedy Maritime Analysis Centre: <https://www.bimco.org/ships-ports-and-voyage-planning/security/piracy-reports> accessed 24 October 2024.

72 Office of Naval Intelligence, Worldwide Threat to Shipping (ONI Reports) <https://www.oni.navy.mil/ONI-Reports/Shipping-Threat-Reports/Worldwide-Threat-to-Shipping/> accessed 13 August 2024.

73 Above, text to n 28.

74 See art 101(a)(i).

75 Ibid, art 101(a)(ii).

also involve 'voluntary participation in the operation of a ship … with knowledge of facts making it a pirate ship …'[76] and 'any act of inciting or of intentionally facilitating an act' of the types previously defined.[77]

Apart from this general approach, all States must cooperate in the 'repression of piracy on the high seas or in any other place outside the jurisdiction of any State' (Art 100). Furthermore, piracy is assimilated with a private ship or aircraft where committed by a warship, government ship or government aircraft whose crew has mutinied (Art 102). In order for a ship to fall within the scope of the definition, a person in dominant control must intend to use it for an act of piracy act, or it must have been used to commit an act of piracy, provided it remains under the dominant control of a person guilty of piracy (Art 103). A pirate ship might lose or retain its nationality depending on the provisions of the flag state (Art 104). A pirate ship and a ship under the control of pirates can be subject to seizure by another state (Art 105), in which case the entitlement to carry out that action is reserved to warships 'or other ships … clearly marked and identifiable as being on government service and authorized to that effect' (Art 107). Seizure without adequate grounds might involve liability to the flag state of the seized vessel (Art 106).

It is arguable that piracy actions in EEZ are also subject to the above provisions. Moreover, because there is no geographic limitation as to the voluntary participation in the operation of a ship with knowledge of the facts which make it a pirate ship (Art 101(b)) and acts of incitement or intentional facilitation of piracy (Art 101(c)), activities ashore also fall within the definition of piracy.[78] This approach reinforces the idea that if the cyber attacks are considered cyber piracy, even if partially conducted ashore, they would still be characterized as cyber piracy and fall within

[76] Ibid, art 101(b).
[77] Ibid, art 101(c).
[78] Robin Churchill, Vaughan Lowe, Amy Sander, *The Law of the Sea* (4th edn, Manchester University Press 2022) 385-386.

the definition. One must not, however, confuse piracy with armed robbery against a ship.[79] According to IMO Resolution A.1025 (26), 'Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships',[80] cl 2.2, this is defined as:

1. any illegal act of violence or detention, or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship, or against persons or property on board such ship, within a State's internal waters, archipelagic waters and territorial sea;
2. any act of inciting or of intentionally facilitating an act described above.

According to the IMB, the consequences for crew, vessel and cargo include opportunistic and cargo theft, taking crew hostage, assault and injury, kidnapping, and the death of a crew member.[81]

---

[79] From the statistical data available, armed robbery incidents had dropped from 158 in 2015 to double digits through 2016 to 2022, but in 2023, increased to 100: 'Executive Director's Report 2023' (ReCAAP Information Sharing Centre, 2023) <https://www.recaap.org/resources/ck/files/reports/ED%20Report/ED%20report%202023.pdf> 'Annual Report 2023 Piracy and Armed Robbery Against Ships in Asia, January-December 2023', (ReCAAP Information Sharing Centre) <https://www.recaap.org/resources/ck/files/reports/annual/ReCAAP%20ISC%20Annual%20Report%202023.pdf>, both sources accessed 3 May 2024. Similar information is available in the same sources for 2024.

[80] Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery Against Ships was adopted on 2 December 2009 by Resolution A.1025(26) of the IMO Assembly, <https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/A.1025.pdf> accessed 3 May 2024. This amended the Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships adopted through resolution A.922(22) by the 22nd regular session of the IMO Assembly. The definition of piracy in art 2.1 follows the definition in UNCLOS, art 101: <https://www.imo.org/en/OurWork/Security/Pages/PiracyArmedRobberydefault.aspx> accessed 3 May 2024.

[81] 'Piracy and Armed Robbery Against Ships, Report for the period 1 January–31 December 2022' (ICC International Maritime Bureau, ICC Commercial Crime Services) 3. <https://www.iccccs.org/reports/2022%20Annual%20IMB%20Piracy%20and%20Armed%20Robbery%20Report.pdf> accessed 3 May 2024.

One aspect of piracy and armed robbery, which usually goes unnoticed, is the tangible cost to the maritime industry. Apart from the cost of insurance and reinsurance,[82] there is also the cost falling on the shipowner and charterer when called to pay ransom. One very characteristic picture can be drawn from a rarely publicly available table of the amounts of ransoms in December 2011, with the amounts ranging from as low as US$0.2m and US$2.1m and up to US$11.5m and US$13.5m. The average ransom payments were from US$4m to US$6m.[83]

A ransom attack might be used to fund terrorism.[84] In such a scenario, the attack would no longer be considered piracy but fall within the action of terrorism financing and be treated accordingly.

2.2 Acts of war

It must be noted that there are two different approaches as to where the piracy risks are to be allocated, depending on whether the shipowner chooses the Nordic Plan[85] or English law. Thus, the Nordic Plan considers piracy a 'war risk',[86] and, for this reason, the insurance of marine perils does not cover piracy.[87] On the other hand, English policy wording places piracy among 'marine perils', meaning that if the insurance provides coverage only for 'war risks', piracy will not be covered as it is a marine peril.[88] Therefore, depending on which policy coverage is chosen, piracy can be either included in war risks or excluded and instead covered as a marine peril. This can become critical when the assured has insurance with both jurisdictions for different causes, and

---

[82] In 2011, the estimates for insurance contracts of War Risk (covering the Indian Ocean, Gulf of Aden, Red Sea and the Gulf of Oman) were US$420,287,250 and for Kidnap and Ransom (K&R) US$214,620,000 covering an estimated amount of 42,450 vessels for the period between January 2011 and August 2011 with the total insurance premiums reaching US$635 million: see Hideshi Ueno, 'Somali Piracy's Impact on the Global Economy Various Cost Estimates of Anti-piracy Efforts from US Think Tank Report' (Sasakawa Peace Foundation, 2011) <https://www.spf.org/oceans/analysis_en/c1203.html> accessed 18 October 2024.

[83] See further Ueno, ibid, fig 2.

[84] Todd (n 53) 4.

[85] Thor Falkanger, Hans Jacob Bull, Lasse Brautaset, *Scandinavian Maritime Law: The Norwegian Perspective* (4th edn, Universitetsforlaget 2017) [22.5.2].

[86] The Nordic Marine Insurance Plan of 2013, v 2023, §2-9, letter d <https://www.nordicplan.org/the-plan/part-one/chapter-2/section-2/#clause-2-8 > accessed 27 August 2024.

[87] Ibid, §2-8, letter a.

[88] Arnould (n 35) ch 23.

the case is decided before the Norwegian or English courts. Thus, the Norwegian courts would examine the influence on the risk occurrence. If neither of the perils is the dominant cause, the court would find both insurers liable[89] for the percentage of the loss for the risk they covered. The English courts would prorate the marine perils as 'dominant' to the war perils, thus exposing the assured and releasing the insurer, which provided coverage for war risks.[90]

War risk coverage is sometimes cancelled following a Notice of Cancellation by the insurers, as was done recently for the Indian Ocean, Gulf of Aden, and Southern Red Sea,[91] in some cases possibly providing a buyback option[92] for the cancelled cover. War risks provided by a P&I insurer may also exclude some losses, damages and expenses arising from acts of terrorism when related to special insurance coverage.[93]

2.3 Terrorism

There is no one unilaterally recognised definition of terrorism. Instead, there are multiple approaches by the United Nations,[94] as well as regional and national approaches. The only

---

89 Nordic Plan 2013, v 2023 (n 85), §2-14, §2-16.

90 Ibid. See also Nordic Plan 2013, ibid, Commentary, §2-8 <https://www.nordicplan.org/commentary/part-one/chapter-2/section-2/#clause-2-8> accessed 27 August 2024.

91 Gard, 'Member Circular No 19/23: Notice of Cancellation for War Risks' (14 February 2024) <https://gard.no/circulars/19-2023-notice-of-cancellation-for-war-risks/> accessed 27 August 2024.

92 Following a notice of cancellation, Gard offered agreed terms on a case-by-case basis and provided the charterer's buyback cover did not exceed a limit of US$150m for each voyage: Gard, 'Member Circular 21/2023: Red Sea Buyback- Charterers' Liability Cover' (20 February 2024) <https://gard.no/circulars/21-2023-red-sea-buyback-charterers-liability-cover/> accessed 27 August 2024.

93 See, eg, the TOPIA 2006 exclusion from special war risk P&I insurance: see Gard, 'Member Circular No 15/2023: Reinsurance Arrangements for the 2024 Policy Year Arranged Through the International Group of P&I Clubs – Special P&I War Risks Cover' (20 December 2023) <https://gard.no/circulars/15-2023-reinsurance-arrangements-for-2024-policy-year-arranged-through-international-group-p-i-clubs-special-p-i-war-risks-cover/> accessed 27 August 2024. For TOPIA, see Colin de la Rue, Charles Anderson, and Jonathan Hare, *Shipping and the Environment: Law and Practice* (3rd edn, Informa Law from Routledge 2023) 213 et seq.

94 See UNODC, United Nations Office on Drugs and Crime website, Defining Terrorism, <https://www.unodc.org/e4j/en/terrorism/module-4/key-issues/defining-terrorism.html>, accessed 3 May 2024.

exception is the definition provided by the International Convention for the Suspension of the Financing of Terrorism,[95] which in Art 2.1, provides that a person commits an offence if

> that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds[96] with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out …

An act falls within the scope of the offences listed in the Annex, as per Art 2.1(a),[97] as long as it is done with the intention to affect a civilian or any person not participating actively in the hostilities in an armed conflict situation by causing death or serious bodily injury 'when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organisation to do or to abstain from doing any act' (art 2.1(b)).

In 1985, the *Achille Lauro*,[98] a passenger vessel, was hijacked by four armed men and forced to sail to Tartus in Syria instead of Port Said. One passenger was killed. The hijackers were eventually arrested on their escape flight to Tunisia,[99] and this led to the enactment of the SUA Convention 1988,[100] later amended by the 2005 Protocol.[101]

Article 3 of the SUA Convention, as amended,[102] describes an offence of international terrorism, which it was combating, as an action of any person who:

---

95 International Convention for the Suppression of the Financing of Terrorism <https://treaties.un.org/doc/db/terrorism/English-18-11.pdf> accessed 3 May 2024.

96 See art 1.1.

97 One of the Conventions listed in the Annex of the International Convention for the Suppression of the Financing of Terrorism is the Convention for the Suppression of Unlawful Acts against the Safety of Navigation 1988.

98 See *Klinghoffer v SNC Achille Lauro* 921 F2d 21, 25 (2d Cir 1990), where the family of the diseased passenger sued the terrorist organisation in court.

99 Bowley (n 32) 24-25.

100 See the official text <https://treaties.un.org/doc/db/Terrorism/Conv8-english.pdf> accessed 8 May 2024.

101 See the UN Protocol of 2005 to the Convention for the Suspension of the Unlawful Acts Against the Safety of Maritime Navigation <https://sherloc.unodc.org/cld/uploads/res/treaties/definitions/treaty/protocol_to_the_convention_for_the_suppression_of_unlawful_acts_against_the_safety_of_maritime_navigation_2005_html/Protocol_to_Maritime_Convention_E.pdf> accessed 8 May 2024.

102 The chapeau of art 3.1 of the Convention was replaced by art 4.1 of the 2005 SUA Protocol.

'unlawfully and intentionally:

a. seizes or exercises control over a ship by force or threat thereof or any other form of intimidation; or
b. performs an act of violence against a person on board a ship if that act is likely to endanger the safe navigation of that ship; or
c. destroys a ship or causes damage to a ship or to its cargo which is likely to endanger the safe navigation of that ship; or
d. places or causes to be placed on a ship, by any means whatsoever, a device or substance which is likely to destroy that ship, or cause damage to that ship or its cargo which endangers or is likely to endanger the safe navigation of that ship; or
e. destroys or seriously damages maritime navigational facilities or seriously interferes with their operation, if any such act is likely to endanger the safe navigation of a ship; or
f. communicates information which that person knows to be false, thereby endangering the safe navigation of a ship; or
g. injures or kills any person, in connection with the commission or the attempted commission of any of the offences set forth in subparagraphs (a) to (f).[103]

An offence is also treated as an attempt to commit any of the above actions (Art 3.2(a)), abetting the commission by another person or accomplice to the offender (Art 3.2(b))[104] or threat with or without a condition in accordance with the national law with the aim to compel a physical or legal person 'to do or refrain from doing any act, to commit any of the offences set forth in paragraph 1, subparagraphs (b), (c), and (e), if that threat is likely to endanger the safe navigation of the ship in question.'

[103] Pursuant to art 4.3 of the SUA 2005 Convention, the subparagraph was deleted.

[104] This provision was replaced by art 4.4 of the SUA 2005 Convention to read as follows: '[…] if that person threatens, with or without a condition, […] aimed at compelling a physical or juridical person to do or refrain from doing any act, to commit any of the offences set forth in paragraphs 1 (b), (c), and (e), if that threat is likely to endanger the safe navigation of the ship in question.'

The SUA 2005 Convention inserted Art 3bis to the SUA 1988 Convention which concerns the use against or on a ship or discharging from the ship of explosive, radioactive material or BCN weapon (Art 3*bis* (1)(a)(i)), discharging from the ship of oil, liquified natural gas or other hazardous and noxious substance (Art 3*bis* (1)(a)(ii)), use of the ship as a weapon (Art 3*bis* (1)(a)(iii)) or a threat with or without condition of such actions (Art 3*bis* (1)(a)iv)). Furthermore, the transportation of explosive or radioactive material with knowledge of the intention of the usage for the above actions (Art 3*bis* (1)(b)(i)), in order to intimidate a population or to oblige an action or abstain from an action by a government or an international organization as well as the transportation of any BCN[105] weapon (Art 3*bis* (1)(b)(ii)), transportation of fissionable materials with the knowledge of the intended use in nuclear explosion (Art 3*bis* (1)(b)(iii)) or 'any equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN weapon, with the intention that it will be used for such purpose' (Art 3*bis* (1)(b)(iv)).

There are some exclusions for actions of transferring fissionable materials provided in Art 3*bis* (2)(a) and Art 3*bis* (2)(b).

The extent of the application of the SUA Convention is quite wide, as provided in Art 4.1, extending to any actual or planned navigation of the ship 'into, through or from waters beyond the outer limit of the territorial sea of a single State, or the lateral limits of its territorial sea with adjacent States'.

Furthermore, it is also applicable when 'the offender or the alleged offender is found in the territory of a State Party other than the State referred to in paragraph 1' (Art 4.2).

There is no explicit definition of terrorism, international terrorism or terrorist attacks in the SUA 1988 Convention or the SUA 2005 Convention. However, the list of offences that the Member

[105] BCN weapon is defined in art 2.1(d) of the SUA 2005 Convention, which amended art 1 of the SUA 1988 Convention, as (i) biological weapons, (ii) chemical weapons, and (iii) nuclear weapons. The nuclear weapons are usually explicitly excluded from the terrorism risk coverages.

States to the Convention are requested to penalise and prosecute using their national laws gives an impressive number of situations that can be characterised, through analysis, as terrorism and terrorist actions. The victims of the perpetrators range from the crew and passengers to shipowners or charterers (as can be concluded from the provisions of Art 3 of the SUA 1988 Convention), population, government and international organisation (as per additional stakeholders referred to in Art 3*bis* added by the SUA Convention 2005). Thus, the coverage is as complete as possible.

Because of the broad definition of ship, it is arguable that the SUA Conventions and Protocols might be applicable when a ship involved in a maritime security incident is not manned.[106] Once the IMO creates the MASS Code,[107] it remains to be seen which relevant provisions might be applicable.

At present, autonomous boats, drones, and missiles are being used to attack merchant vessels transiting the Red Sea area and the coast of Yemen. Despite one view that terrorists are not sophisticated or sufficiently experienced to deploy marine terrorist attacks,[108] technology may yet enable them to launch attacks from the shore using electronic and internet communication, engage in cyber-terrorism, or threaten the controllers of the remotely controlled vessels. The international community is collaborating to create a convention to combat information and communications technology usage for criminal purposes, including terrorism. The draft of the

---

[106] The four categories of ships involved in a maritime security incident with the application of the SUA 1998 and 2005 Conventions are: the victim ship, the offending ship, the enforcement craft, and the third ship not involved in the incident directly: see Anna Petrig, 'Autonomous Offender Ships and International Maritime Security Law' in Henrik Ringbom, Erik Rosaeg, and Trond Solvang (eds), *Autonomous Ships and the Law* (Routledge 2023) 37-38.

[107] The MASS Code is set to be ready in a non-mandatory format in 2025. It will then be amalgamated into a mandatory Code entering into force in 2028 as planned by the IMO. See further IMO, 'Autonomous Shipping', <https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx> accessed 19 August 2024, IMO, 'Maritime Safety Committee (MSC 107), 31 May-9 June 2023' <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-107th-session.aspx> accessed 19 August 2024.

[108] Martin N Murphy, *Contemporary Piracy and Maritime Terrorism: The Threat to International Security* (Adelphi Paper 388, The International Institute for Strategic Studies 2007) 69–71.

convention, dated 1 September 2023,[109] contained multiple references to the term 'terrorism'. More specifically, terrorism was referred to: (1) as one of the criminal offences which can be considerably affected regarding its 'scale, speed and scope' with the use of a computer system (preamble s 3),[110] (2) as a type of computer-related forgery done by data alteration, deletion or suspension in an advancing way for the terrorism-related crimes (Art 11.1) [111] and (3) in the use of the means of information and communication technologies for committing terrorist acts or the collection or provision of funds for its financing.[112] After the adoption of the Draft United Nations Convention against Cybercrime, the only reference to the term terrorism remains in the preamble. In contrast, the previous versions of Arts 11 and 15 septies have been removed.[113]

3 Cybersecurity

With increased automation in the shipping industry, both ashore and offshore, the maritime industry has to face the emergence of numerical data protection issues. The possibility of unauthorised access or data leakage and access denial to the data handler due to viruses and threats has created a need for specialised protection and insurance coverage against risks associated with cyber security breaches.

---

[109] Draft text of the convention, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Sixth session, (New York, 21 August – 1 September 2023) <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf > accessed 30 August 2024.

[110] Ibid, 1.

[111] Art 11 has multiple alterations, including a reference to computer data 'conducive to terrorism-related crimes', ibid, 9-10.

[112] Art 15 septies referred also to the 'provision of logistical support for perpetrators of terrorist acts', ibid, 18–19. This, theoretically, could include cyber breaches leading to the undetected usage of logistics for criminal purposes, as occurred in the port of Antwerp (below, n 316).

[113] Art 11 was renumbered as Art 12, and the reference to terrorism was eliminated, whereas Art 15 septies was deleted completely.

3.1 Beginnings

Cyber incidents have become known since the 1980s.[114] They are attributable to the expansion of the interconnectivity between critical infrastructures, the use of software for systemic operations, and connection to the internet.

Although most cases in past occurred in other sectors, incidents in the last decade have drawn the attention of the IMO to the vulnerability of the shipping chain. Thus, the IMO has addressed maritime cybersecurity issues since 2014, generally in the Maritime Security Commission (MSC) and Facilitation Committee (FAL).[115] As a result of consultations with various stakeholders in the period 2014-2017, MSC's 98th session approved the joint MSC-FAL circular on 'Guidelines on maritime cyber risk management'.[116]

Since 2015, classification societies[117] and insurers[118] have highlighted the risks to their clients, increasing their awareness. This was reinforced by Lloyd's of London estimates placing the cost of cyber attacks for companies at US$400 billion annually,[119] listing together with financial loss (a) physical loss or damage to the ships and injuries to the crew, (b) loss of cargo, (c) pollution, (d) reputation damage and e) business interruption as side effects of the cyber incidents.[120] The movement was joined by state authorities like the Danish Centre for Cyber Security (CFCS), which identified and categorized the cyber threats and enlisted them from the highest to lowest impact,

---

[114] Such as a trojan inside a software, causing an explosion of the Trans-Siberian gas pipeline in June 1982 as claimed by Thomas C Reed, *At the Abyss: An Insider's History of the Cold War* (Ballantine Books 2004).

[115] FAL 40/INF.4 including the guidelines of cyber security onboard ships produced by BIMCO, CLIA, ICS, INTERCARGO, and INTERTANKO (ver 1.0 – January 2016).

[116] MSC.1/Circ.1526, see further Maritime Safety Committee (MSC), 98th session, 7–16 June 2017, <https://www.imo.org/en/MediaCentre/MeetingSummaries/Pages/MSC-98th-session.aspx>.

[117] 'DNV GL Reveals Top Ten Cyber Security Vulnerabilities for the Oil and Gas Industry' (DNV, 30 November 2015) <https://www.dnv.com/news/dnv-gl-reveals-top-ten-cyber-security-vulnerabilities-for-the-oil-and-gas-industry-48532> accessed 27 August 2024.

[118] 'Marine Cyber Risks at Sea' (Gard, 8 January 2016) <https://gard.no/articles/managing-cyber-risks-at-sea/> accessed 27 August 2024.

[119] Stephen Gandel, 'Lloyd's CEO: Cyber Attacks Cost Companies $400 Billion Every Year' (Fortune, 24 January 2015).

[120] 'Cyber Security Awareness in the Maritime Industry' (Gard, 31 October 2016) <https://gard.no/articles/cyber-security-awareness-maritime-industry/> accessed 27 August 2024.

starting with cyber espionage and cyber criminal offences and ending with cyber activism and terrorism.[121]

The maritime industry slowly realised the magnitude of the threat. A survey conducted in 2018 showed that nearly two in five companies experienced an attempt or a successful data breach in 2017.[122] Thus, for instance, charging seafarers' personal IT devices aboard the vessel could expose the vessel network to malware, which could then spread to ports using information exchange routes or connections via systems.[123]

Following serious cyber attacks affecting the shipping industry, many initiatives have been undertaken by ports,[124] authorities,[125] international organisations,[126] and classification societies[127] to provide guidelines and standardisation to reinforce maritime cyber safety. The IMO and FAL issued updated guidelines referencing the member States to the available information

---

[121] 'Denmark Identifies Cyber Threats in its Maritime Sector' (Gard, 24 January 2019) <https://gard.no/articles/denmark-identifies-cyber-threats-its-maritime-sector/> accessed 27 August 2024.

[122] The percentage of attempted cyber breaches was 28%, and of the completed cyber breaches 10%: see further Maritime Cybersecurity Survey (Jones Walker LLP, 2018) <https://sites-communications.joneswalker.com/38/1033/landing-pages/2018-maritime-cybersecurity-survey-landing-page-only-(rebrand).asp> accessed 19 August 2024.

[123] IAPH Cybersecurity Guidelines for Ports and Port Facilities: Version 1.0, (International Association of Ports and Harbors (IAPH), World Ports Sustainability Program (WPSP), 2021) (IAPH Cybersecurity Guidelines 2021) <https://sustainableworldports.org/wp-content/uploads/IAPH-Cybersecurity-Guidelines-version-1_0.pdf> accessed 19 August 2024, 29.

[124] IAPH – International Association of Ports and Harbors and others, 'Port Community Cyber Security' (World Ports Sustainability Program, June 2020) <https://sustainableworldports.org/> accessed 25 October 2024.

[125] The United States National Institute of Standards and Technology (NIST) <https://www.nist.gov/cyberframework> accessed 29 August 2024, produced a 'Framework for Improving Critical Infrastructure Cybersecurity: Version 1.0' issued in February 2014 updated to Version 1.1. (NIST, 16 April 2018) <https://www.nist.gov/publications> accessed 25 October 2024. The most up-to-date version is 'The NIST Cybersecurity Framework (CSF) 2.0 (NIST, 26 February 2024).

[126] BIMCO and others, 'The Guidelines on Cyber Security Onboard Ships' (Version 4), 'ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements' (ISO, Edition 3, 2022) <https://www.iso.org/standard/27001> accessed 29 August 2024 (please note that this standard edition has paid access).

[127] IACS, 'Recommendation on Cyber Resilience: No 166 (Corr.2 Apr 2022) <https://iacs.org.uk/resolutions/recommendations/161-180> accessed 29 August 2024.

for cyber risk management and encouraging the usage of available best practices from the industry.[128]

3.2 Cyber security breaches and cyber attacks

This paper differentiates between cybersecurity breaches and cyber-attacks. The former does not necessarily precede the latter, and the latter can either follow the former as a continuous situation evolution or be completely independent.

A cyber-security event occurs when a person or persons intervene(s) in the security structure of a port,[129] a shipping company,[130] a shipowner company, or vessels. The threat of using the technology maliciously and targeting port security[131] has initiated numerous discussions and reports. There are multiple scenarios regarding how a port can be attacked and compromised using technology. A recent report on good practices for the maritime security of ports identified four scenarios of cyber attacks.[132] Cyber attacks against shipping companies and vessels usually aim to blackmail the victims for ransom. However, this could change if the vessels had no crew

[128] MSC-FAL.1/Circ.3/Rev.2, Annex, 4.

[129] The report on good practices for maritime security places hacktivism, the use of technology to promote a political agenda or a social change, as a physical attack, along with piracy and terrorism, whereas malware, phishing, targeted attacks, abuse, theft and manipulation of data, phishing and geo-localisation signal spoofing and jamming are listed separately as nefarious activities and abuse. See further 'Port Cybersecurity: Good Practices for Cybersecurity in the Maritime Sector', ENISA, (European Agency for Cybersecurity (ENISA), November 2019), <https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector/at_download/fullReport> accessed 10 May 2024, 28–29.

[130] Some cyber threats like (1) nation-backed cyberattacks, (2) cyber-terrorism and (3) cyber hactivism are estimated to be less likely to affect private shipping companies, which are more exposed to the cybercriminals that will try to obtain access to the valuable cargo and the money paid for the shipping operations between the stakeholders like charterers, shippers and ports; see Rory Macfarlane, 'Cyber-risk in Shipping and its Management' in Barış Soyer and Andrew Tettenborn (eds), *Ship Operations: New Risks, Liabilities and Technologies in the Maritime Sector* (Informa Law from Routledge 2021) 70–72.

[131] The interconnectivity of ports creates a picture of the exposure to cyber threats: see, eg, *Global Trade 2024* <https://www.globaltrademag.com/european-ports/> accessed 10 May 2024.

[132] The use of targeted attack to compromise critical data and steal cargo of high value or conceal illegal trafficking, encryption, and total shutdown of port operations through ransomware, manipulation, or theft of data via targeted attack against port communication systems interconnecting all the stakeholders involved in port operations, attack on operation technologies (OT) of the port. See further ENISA Report (n 129) 32–38.

onboard[133] to report the security breach, and the situation went unnoticed until much later. This scenario was examined in simulations of an EU programme regarding cybersecurity maritime issues.

If the cyber incident leads to piracy or armed robbery, it can also be considered a cyber-piracy event. Nevertheless, because the specific provisions have been formulated concerning those incidents, creating new coverage for cases where the insured vessel is exposed to harm through cyber intervention would probably be more practical. Thus, creating cyber-piracy and cyber-terrorism risk cover products aimed at the needs and inherent particularities of the shipping industry might create a feeling of security. This is because insurers would be able to calculate the exposure of the assured, taking into account any previous incidents, and thus modulate a map of avoidable areas or a list of non-trustworthy providers of software to guide the assured. This would, inevitably, include exclusions so that risky stakeholders do not increase the premium for other assureds, placing the risk with the same insurer.

3.3 Relation to previous risks

Classical piracy requires the physical interaction of pirates, the crew, and/or the vessel. A cyber-security breach usually refers to a virtual, not tangible, interaction. This mostly takes place in the software and systems of the vessel, even if the point of entrance could be from a hardware device.

Piracy usually occurs when armed persons attempt or successfully board a vessel. Consequently, the shipowner might lose contact with the vessel, the crew might be locked up or kidnapped, and the vessel might deviate from its expected routing. Armed robbery has a provision which could meet a cyber security threat situation.

The definitions of piracy and armed robbery, if widely interpreted, do not demand the physical presence of the perpetrators aboard a vessel, as long as the vessel is affected and its crew,

[133] Oliver Daum, 'Cyber Security in the Maritime Sector' (2019) 50 JMLC 1; 7-9; 18-19.

passengers, cargo, or the vessel itself are jeopardised or sustain injuries or death or damages. Theoretically, an intervention in the data transmitted between the vessel and the centre of its operation, a third-party stakeholder like a shipper or charterer, a port facility, or an organisation (regional or international) could lead to consequences for the affected stakeholders. This might involve an action or an obligation to abstain from specific actions, the leakage of shared information to interested third parties, the exposure of the safety and security of the crew, the passengers and the cargo, or the manipulation of the charts or other means of navigation or the detectors.

In a piracy incident, two ships are involved: the pirate vessel and its victim.[134] This means that cyber incidents would need the presence of a pirate ship close to the ship being affected by a cyber breach or cyber attack. However, this requires a person's presence aboard and could be applicable: (a) to the deployment of surface or underwater unmanned vessels from a person ashore affecting the crew's ability to navigate and autonomously self-propel the vessel via hacking or cyber attack and asking for a ransom to release the crew and the vessel; (b) to the threat or use of physical violence against the shore-based operator of a remotely controlled unmanned vessel by a person who wants to steal the cargo from the vessel; (c) to the use of craft to surround the unmanned vessel while on its way so that it slows down or stops to avoid the collision, as it is programmed to do for safety reasons, and consequent boarding of pirates on it in order to steal the cargo from it.[135] It would be inapplicable to (a) a land-based cyber attack on an unmanned vessel by hacking the navigation or propulsion systems of the vessel because there would be no crew to experience the threat or violence forced on it,[136] (b) remotely controlled vessels approaching an unmanned vessel, invading into its systems and connecting with it and taking control of its navigation and propulsion, again due to the absence of persons aboard any of the

---

[134] See Petrig (n 106) 32-35.

[135] Luci Carey, 'Autonomous Ships and Hull and Machinery Marine Insurance' in Stephen Girvin and Vibe Ulfbeck (eds), *Maritime Organisation, Management and Liability: A Legal Analysis of New Challenges in the Maritime Industry* (Hart Publishing 2021) 265-267.

[136] Ibid.

vessels. These last two scenarios would, however, be covered as cyber risk.[137] Examples include two reported attempted attacks by Houthis on a tanker vessel, the *Chios Lion*,[138] and a bulker vessel,[139] the *Tutor*, with a remotely controlled vessel loaded with explosives. As the crew realised this was happening, they fired against the approaching unmanned boat, which led to the explosion of the latter before it could reach the tanker, the *Pumba*.[140] It is a significant concern that according to a 2017 Conflict Armament Research 'Anatomy of a 'Drone Boat,' [141] the remote controller of the unmanned vessel filled with explosives[142] can control the GPS spot of the vessel to increase and decrease its speed and to receive live video of its route. Speedboats can also be deployed in open waters and close to ports.[143]

Cyber-attacks are already considered possible acts of war by insurance regulators, but insurers[144] are very reluctant as to what they will cover because they cannot estimate the exposure before the event and usually use exclusion clauses for cyber attacks with very few exceptions. This is based on the provisions of the relevant clauses and the different categorisation of multiple cyber clauses as belonging to types 2 to 4[145] of the intervention of States inside the area of actual war activities or outside the main site of the battles. Furthermore, the exclusion[146] or inclusion[147] of

---

[137] Ibid.

[138] See Γιάννης Παπαδόπουλος, 'Η έκρηξη πριν από τη Σύγκρουση 'Έσωσε'' το Τάνκερ' (Καθημερινή, 18 July 2024) <https://www.kathimerini.gr/society/563131336/i-ekrixi-prin-apo-ti-sygkroysi-esose-to-tanker/> accessed 19 August 2024.

[139] Ibid.

[140] See Joshua Minchin, 'Red Sea Attacks Continue as Four Vessels Attacked in Past Week: Drone Boats, Missiles and Small Craft Were all Used as the Threat to Shipping Remains High' *Lloyd's List* (London, 23 July 2024).

[141] Frontline Perspective Anatomy of a 'Drone Boat': A Water-Borne Improvised Explosive Device (WBIED) Constructed in Yemen (Conflict Armament Research, December 2017) <https://www.conflictarm.com/download-file/?report_id=2550&file_id=2564> accessed 19 August 2024, 3-5.

[142] Daum (n 133) 8-10.

[143] The report refers to an attack by fast, explosive-fitted boats to target the Saudi-led coalition off the port city of Al Hudayadah in January 2017, resulting in damage to a Royal Saudi Naval Forces frigate: ibid, 10.

[144] Dean Armstrong, Thomas Steward, and Shyam Thakerar, *Cyber Risks and Insurance: The Legal Principles* (Bloomsbury 2021) ch 8.

[145] Rachel Turk, 'State-backed Cyber-attacks Wordings' (Lloyd's Market Bulletin Y5433, 14 May 2024) <https://assets.lloyds.com/media/6335bcb0-e2a2-4378-8328-1ddf54828f2f/Y5433.pdf> accessed 9 August 2024, 5-6.

[146] CL365, CL380, JS.001.

[147] The excluded cyber threats are covered when the policy provides explicit coverage for war risks or terrorism: see CL365 cl 1.2, JS.001 cl 1.2, CL380 cl 1.2.

the clauses covering cyber-attacks is associated chiefly with war risks, and part of war risks are acts of war. Lastly, cyber incidents and cyber-attacks are already identified in the most widely used insurance clause and are covered or excluded, depending on the coverage.[148]

The US Coast Guard (USCG) has identified that terrorist attacks can have both cyber and physical incidents. It is, therefore, possible that a physical attack will follow the cyber incident or that the cyber suspicious activity or breach of security was undertaken in order to spot the vulnerabilities of the attacked facility or vessel.[149] In these cases, as identified in the report, 'Harmonization of Cyber Incident Reporting to the Federal Government',[150] the owners and operators of vessels, maritime facilities, and/or outer continental shelf facilities are advised to inform the US Coast Guard without delay of an activity and/or incident of 'breaches of security, suspicious activities and/or activities that may result in a transportation security incident'.

Cyber threats are perceived as having several levels of risk, from less impactful to ones with more severe consequences, namely cyber incidents, cyber breaches, and cyber-attacks.[151] The term 'cyber incident' is broader than 'cyber breach' and 'cyber attack' and describes an event affecting cyber systems involved in the shipping chain. This has practical implications, as the term already exists in cyber insurance clauses and can be understood as relating to cyber risks. If this is confusing, a new term describing the first stage of the cyber-system exposure could be adopted. Cyber risks related to marine perils could be referred to as 'cyber marine perils' and categorised further into cyber piracy, cyber war, and cyber terrorism, with each of the risks having all of the

---

[148] CL 380.

[149] Reporting Suspicious Activity and Breaches of Security, US Department of Homeland Security (USCG, 14 December 2016 <https://www.dco.uscg.mil/Portals/10/Cyber/Cyber-Readiness/CG-5P%20Policy%20Letter%2008-16%20-%20Reporting%20Suspicious%20Activity%20and%20BoS.pdf?ver=2020-05-26-173911-100&timestamp=1590758815625>, accessed 10 May 2024.

[150] Prepared by the Department of Homeland Security's Office of Strategy, Policy and Plans on behalf of the Secretary for Strategy, Policy and Plans, Homeland Security, in 2023, implementing a requirement in paragraph 107 (d) (1) of the Cyber Incident Reporting for critical Infrastructure Act of 2022.

[151] According to the Guidelines on Cyber Security Onboard Ships, cyber-attacks are conducted in stages: see further FAL 40/INF.4, Annex, 9-10.

three levels of cyber events, depending on the significance of the intervention to the cyber systems and the effects for the shipping chain. Thus, drawing parallels with attempted boardings by pirates or armed robbers, cyber piracy could be a cyber incident, expressed as an attempt to intrude on the cyber system of the vessel or the shore-based part of the shipping chain.[152] This scenario could raise another question of whether there should be different protection depending on whether the affected insured is ashore or offshore or if it is a combination of both, for instance, a shipping company chartering or managing ships and the chartered or managed vessel. For example, an email with a malicious program could be sent from ashore to the vessel or contain a malicious program hardware device connected to the bridge's primary computing system and is then sent to an international organisation or the port authority, affecting these receivers with the malicious software as well. As will be shown, this might be treated as one inclusive exposure to cyber risk.

A cyber war risk could be perceived as an attempt of hostile act to espionage and be characterised as a cyber incident, as actual espionage when a cyber breach happens, and as a cyber attack when both software and hardware are used. Cyber terrorism could be either an attempted compromise as a cyber incident, an accomplished cyber breach with exposure of the cyber systems of the victim of the terrorists, or a cyber attack when the terrorist act impacts the victim and affects its functionality.

Every insurance product would have three levels of cyber protection, with potentially different premiums increasing as the cost of a possible incident recovery increases. There can also be a distinction between the cyber risks to which an organisation, e.g., IMO, EMSA, port authorities, port logistics companies, and companies owning, managing, chartering, servicing, or surveilling a vessel or the vessel itself, are exposed. What will characterise it as cyber piracy, cyber war/act of war, or cyber terrorism will be the fact that it is affecting, stopping or disrupting the normal functionality of the shipping chain. However, the proximity of the cyber event to the shipping

[152] An example would be unsuccessfully sending a phishing email.

industry should constantly be considered. Thus, if there is a cyber security incident which affects the flights of the crew and they cannot board the vessel on time, or the master of the vessel or the CEO of the shipping company receives phishing emails to their personal computers, these events would not constitute marine cyber perils. The criteria would be if the event could affect the crew, the master and the CEO in their professional capacity and compromise the cyber system security through their connection to the vessel or shipping company through their personal computers. [153] If the same criteria are met, the following can constitute cyber marine perils: (1) the cyber event affects the bank account used for the payment of the plane tickets of the exchange crew, (2) the personal computers of the master of the vessels or the CEO of the shipping company are used to send malicious emails autonomously,[154] without the master's or CEO's intervention and knowledge, to all the connections in the contact list. Lastly, some past incidents also meeting the criteria of being cyber marine perils would include the manipulation of the booking system of the shipper or the port logistics systems, causing the cargo to be wrongly allocated and delivered or the unnoticed transport of illicit cargo.

It should be irrelevant whether the malicious code was designed and sent or if the cyber breach was undertaken by humans or programs created by humans or by another program with some input from humans. The vital part of characterising an event as falling within cyber marine peril is whether the shipping chain is affected. Furthermore, it is no different if the affected part is manned or unmanned and if there was a human intervention which exposed the mechanism affected by the cyber event or if the absence of the human was the reason why the event happened (for cyber incidents and cyber attacks) or went unnoticed for some time (for cyber breaches). Nevertheless, because of the increase of automation ashore and aboard and the inevitable interconnections between the two parts of the shipping chain, further study is needed

---

[153] This would probably be covered by policies providing general coverage for cyber threats, such as the Hiscox Cyber Clear Policy 2019 and the Beazley Breach Response Policy 2019: see Celso de Azevedo, *Cyber Risks Insurance* (2nd edn, Sweet and Maxwell 2019) A1-001; A2-001.

[154] For instance, remotely controlled by hackers or automatically following the default malicious program functionality to reproduce itself and send emails to other addresses from the contact list of the computer affected.

to determine if the presence or absence of a human in the communication, processes or functions inside the shipping chain could potentially increase or moderate the cyber risk exposure. In the aftermath, if the presence of a person or his ability to control and intervene from away into the proceeding positively affected the outcome of a cyber event, then the human element would be a prerequisite for insurance coverage.[155] This would not mean that the failure of the person to intervene promptly and prevent the risk from happening or that the expected mitigation is higher than the actual loss mitigation success would give the insurer the right to waive its obligation or create liability for the person. The non-employment of a person when the insurance contract requires his presence might mean the risk occurring will not be covered. Still, the contract will be revived once he is back on duty if the absence is for a short period and the risk occurs under the Insurance Act 2015. Alternatively, this is not assumed at all if the person was never employed and instructed to be present despite the provision of the insurance contract.

On the other hand, if the presence of unauthorised, non-specialised persons or persons would jeopardise the cyber security of a facility or the ship, then the fact of their presence would mean cyber coverage is waived or does not commence.

This could be done to give insurers the certainty of minimisation of cyber risks and require the assured to employ specialised and trained personnel at all times and safeguard access to cyber security facilities from unauthorised persons. This could create a more or less secure environment for cyber systems and confidence to each party to the insurance contract they have complied with their obligations.[156]

To ensure the above behaviour and to create stable feedback for risk management and forecasts, a new clause could be introduced in the cyber marine peril coverages. The 'Notification and Compliance' clause could create an obligation to notify of any cyber risk event, even a simple

---

[155] See functionalism theory discussed in AXM Ntovas, 'Functionalism and Maritime Autonomous Surface Ships' in J Kraska J and Y-K Park (eds), *Emerging Technology and the Law of the Sea* (CUP 2022) 214.

[156] Barış Soyer, 'Cyber-Risk Insurance – Developing a New Cover in the Market' in Soyer and Tettenborn (n 130) ch 7.

cyber incident with a malicious attachment to an email or a phishing email. This would help to build a database with past cyber threats and assist in the evaluation of the magnitude of the risks of each category, leading to more accurate premium requirements. The database would then be used to create instructions for eliminating similar cyber risks and preventative measures to avoid these risks in the future, and it would then be sent to all cyber risk policyholders for compliance. The compliance part of the clause would oblige the assured, after the occurrence of the insured risk for which he was covered, to follow the insurer's preventative measures, instructions and guidelines. In the case of noncompliance, the insurance coverage would cease to exist. The notification and compliance will also be reviewed upon renewal of the insurance contract. In case of significant non-compliance, the insurer would have the right to deny renewal simply because the assured's behaviour increased the risk occurrence probability) whereas in cases of minor non-compliance, premiums could be increased.

3.4 Incidents

There are multiple possible exposures a facility or a vessel could experience, depending on its importance, its interconnectivity, and its potentially dangerous nature. Thus, a cybersecurity breach or attack incident on a port operating flammable or toxic goods or on a vessel transporting them could be considered more urgent and have a higher public security profile compared with bulk carriers or containerised goods transportation, assuming the latter does not transfer flammable cargo. However, the potential delays and costs for lost or damaged goods could be significantly higher. If passengers are exposed to dangers from a cybersecurity breach, this could lead to public outrage and require immediate measures to safeguard lives. Each scenario has different stakes but shares sudden and unexpected vulnerability.

In 2023, there was an attack on the logistics company DP World in Australia, which handles 40 per cent of the containers coming into Australian ports[157] and affected four significant ports and 30,000 cargo containers.[158] The absence of a ransom demand raised questions about the motives behind the attack.[159] In 2022, multiple European ports experienced cyber-attacks affecting their IT services and creating operational delays.[160] The same year, oil companies were affected by another cyber-attack on their loading and unloading systems.[161] On Christmas day, the port of Lisbon could not operate its website and faced a ransom demand in exchange for protecting its confidential information.[162]

However, not only ports[163] and logistics companies are exposed to ransomware attacks. One of the most infamous cases was the NotPetya cyber attack in July 2017, with a cost estimated to be between US$3 and US$3.3 billion.[164] Malware originating in the Ukraine resulted in multiple attacks worldwide. AP Møller-Maersk's exposure disrupted 17 container terminals worldwide and affected the company's global operations. Stakeholders had to manually manage and track

---

[157] The attack was characterised as nationally significant by Australia's National Cyber Security Coordinator: see Laura Dobberstein, 'Australia Declares 'Nationally Significant Cyber Incident' After Port Attack' (The Register, Security, 13 November 2023), <https://www.theregister.com/2023/11/13/asia_tech_news_roundup/> accessed 10 May 2024.

[158] The ports were Brisbane, Melbourne, Perth and Sydney: see Joao-Pierre S Ruth, 'Defending Logistics After Cyberattack on DP World Australia', (Information Week, 20 November 2023) <https://www.informationweek.com/cyber-resilience/defending-logistics-after-cyberattack-on-dp-world-australia#close-modal> accessed 10 May 2024.

[159] Cf Daniel Ziffer, Matt Bamford, 'Freight Giant DP World Recovers From Cyber Attack, but Warns Investigation And Remediation is 'Ongoing"' (ABC News, 13 November 2023), < https://www.abc.net.au/news/2023-11-13/dp-world-deals-with-impact-of-cyber-attack/103097658> accessed 10 May 2024.

[160] In 2022, there were delays at Terneuzen, Ghent, and Malta: see Jonathan Greig, 'Prosecutors Investigating Cyberattacks Affecting Multiple Belgian And Dutch Ports' (ZD Net, 3 February 2022) <https://www.zdnet.com/article/cyberattack-affecting-belgian-port-operations/> accessed 10 May 2024.

[161] See also Jonathan Greig, 'Shell Rorced to Reroute Supplies after Cyberattack on Two German Oil Companies', (ZD Net, 1 February 2022) < https://www.zdnet.com/article/shell-forced-re-route-oil-supplies-after-cyberattack-on-german-companies/> accessed 10 May 2024.

[162] The port's website was 'down' for days: see Jonathan Greig, 'Port of Lisbon Website Still Down as LockBit gang Claims Cyberattack', (The Record, Recorded Future News) 29 December 2022 <https://therecord.media/port-of-lisbon-website-still-down-as-lockbit-gang-claims-cyberattack> accessed 10 May 2024.

[163] It was reported in 2020 that the Port of Los Angeles Cyber Security Operations Center blocked some 40 million unauthorised intrusion attempts every month: see further Port Community Cyber Security (n 123) ch 4.

[164] Reinsurance News, 'Major Insurance and Reinsurance Industry Loss Events' <https://www.reinsurancene.ws/insurance-industry-losses-events-data/> accessed 9 August 2024.

shipments, causing truck backlogs to increase in four-digit numbers.[165] Other large liner shipping companies, such as COSCO,[166] MSC,[167] and CMA CGM,[168] have also been hit by cyber-attacks. The average cost to maritime companies to access their computer systems in 2023 was an average of US$550,000, compared to US$182,000 in 2022,[169] and the total ransoms paid totalled US$3.2 million in 2023, with the percentage of affected companies increasing from 3 per cent in 2022 to 14 per cent in 2023.[170]

The IMO could not avoid the same fate,[171] and in January 2023, a classification society, DNV, was targeted, affecting 70 customers and 1,000 ships.[172]

Some writers have pointed out that shipping still primarily uses paper for its operations, which is a buffer in the battle against cyber threats.[173]

---

[165] IAPH Cybersecurity Guidelines 2021 (n 115) 21.

[166] See 'COSCO Shipping Lines Falls Victim to Cyber Attack', (Offshore Energy, reproduction from World Maritime News, 25 July 2018) <https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/> accessed 19 August 2024.

[167] See James Baker, 'MSC Confirms Website Shutdown Caused by Cyber Attack' *Lloyd's List* (London, 16 April 2020).

[168] The container shipping line was hit twice in September 2020 and 2021. See further Cichen Shen, James Baker, 'CMA CGM Confirms Ransomware Attack' *Lloyd's List* (London, 28 September 2020); Sam Chambers, 'CMA CGM Hit by Another Cyber Attack' (Splash 247, 20 September 2021).

[169] Annop Khanna, 'Shipping Industry Pays an Average $3.2m in Ransom Attacks' *Asia Insurance Review* (25 October 2023), <https://www.asiainsurancereview.com/News/View-NewsLetter-Article/id/86176/type/ARM/Shipping-industry-pays-an-average-3-2m-in-ransom-attacks> accessed 10 May 2024.

[170] Paul Peachey, 'Shipping Names Pay Multimillion-dollar Ransom After Cyberattacks' *TradeWinds* (London, 17 October 2023, updated 18 October 2023, <https://www.tradewindsnews.com/technology/shipping-names-pay-multimillion-dollar-ransoms-after-cyber-attacks/2-1-1536556> accessed 10 May 2024.

[171] The cyber attack affected the IMO's website, internal intranet services and web-based services: 'IMO Security Breached by 'Sophisticated' Cyber Attack' *Lloyd's List* (London, 1 October 2020).

[172] Jonathan Greig, 'Ransomware Attack on Maritime Software Impacts 1,000 ships' (The Record, 17 January 2023), <https://therecord.media/ransomware-attack-on-maritime-software-impacts-1000-ships> accessed 10 May 2024. For more recent examples of cyber incidents see further Eric Watkins, 'US East Coast Colonial Pipeline Resumes Operations After Cyber-Attack' *Lloyd's List* (13 May 2021); Liz Hampton, 'Top US Oilfield firm Halliburton Hit by Cyberattack, Source Says' (Reuters, 22 August 2024) <https://www.reuters.com/technology/cybersecurity/top-us-oilfield-firm-halliburton-hit-by-cyberattack-2024-08-21/> accessed 24 August 2024.

[173] See further Stephen Girvin and Elson Ong, 'Electronic Bills of Lading, Blockchain and Distributed Ledger Technology (DLT)' in Girvin and Ulfbeck (n 135) 217; 'Shipping Rides Cyber Storm with Minimal Disruption' *Lloyd's List* (London, 19 July 2024).

Companies have multiple layers of exposure in the maritime industry, which interconnects with different cybersecurity service users. An example is a ransomware attack suffered by an external IT service provider of a group of companies involved with the marine and offshore energy industries, which affected the shares of the affected latter group of companies by dropping slightly at the closure of trading.[174]

According to a study presented during the Safety at Sea Week in Singapore, more than 80 per cent of cyber incidents occur shortly after the vessel leaves port, with a typical fleet of 30 vessels experiencing 80 such incidents per year. The study identified that more than half of the cases were caused by loose controls on software downloads, followed by intentional and unintentional system misconfigurations, network access from unsecured computers and poor cooperation between ashore and offshore stakeholders.[175]

3.5 Legal approach

Legislators have addressed the cybersecurity issue as part of the personal data protection of individuals and companies by enacting legislation such as the GDPR,[176] the UK Data Protection Act 2018,[177] which oblige the holder and processor of the data to notify the supervising authorities and the data subjects following a data breach. However, it still has not been included

[174] See Jovi Ho, 'Beng Kuang Marine reports' cybersecurity incident After External Vendor Suffers Ransomware Attack' (The Edge Singapore, 19 August 2024) <https://www.theedgesingapore.com/news/cybersecurity/beng-kuang-marine-reports-cybersecurity-incident-after-external-vendor-suffers> accessed 19 August 2024.

[175] State of cyber risk of shipping systems in 2023, International Safety@Sea Conference, October 2023, CYBEROWL, <https://www.safetyatseaweek.gov.sg/files/Presentation/SESSION_3/Mr_Daniel_Ng_s_Presentation_Slides.pdf> accessed 10 May 2024.

[176] The definition of the personal data breach (art 4.12) and the obligation of notification of the data breach to the supervisory authority (art 33) and of the communication of the personal data breach to the data subject (art 34); see European Parliament and Council Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L 119/1.

[177] C 12 (as amended on 8 March 2024). Art 67 provides for the notification of personal data breach to the Commissioner, and art 68 provides for communication of personal data breach to the data subject; the personal data breach is defined in art 33.1. See also Azevedo (n 153) [5-004–5-011].

as a prerequisite in marine insurance, such as the Marine Insurance Act (MIA) 1906,[178] which is applicable in Singapore,[179] and the Insurance Act (IA) 2015,[180] which is applicable only in the UK, and which has made amendments mainly as regards the warranties in the insurance contracts.[181] If cybersecurity measures are taken to safeguard a vessel from any breaches or attacks to which it might be exposed during the voyage, the vessel is considered 'reasonably fit in all respects'.[182] If cyber security perils are included in 'the ordinary perils of the seas', new legislation might not be needed since unseaworthiness releases the insurer. A warranty cannot be remedied pursuant to s 10 of the IA 2015 if the vessel has experienced a cyber security breach or a cyber attack.[183]

If attributable to organisations or states, it is still not clear how the violation of cyber security[184] will be mitigated and if it will be somehow legislated[185] or if the general provisions also apply. There is no widely available public data. Another reason for keeping the details of cybersecurity

---

[178] Marine Insurance Act 1906, 6 Edw 7, c 41.

[179] Marine Insurance Act 1906 (2020 rev edn).

[180] Insurance Act 2015, c 4.

[181] Malcolm Clarke and Barış Soyer (eds), *The Insurance Act 2015: A New Regime for Commercial and Marine Insurance Law* (Informa Law from Routledge 2016); Arnould (n 35); Özlem Gürses, *Marine Insurance Law* (3rd edn, Routledge 2023).

[182] MIA 1906, s 39(4).

[183] Arnould (n 35) ch 2, 16, 19, and 20.

[184] SVR cyber actors adapt tactics for initial cloud access, National Cyber Security Centre, <https://www.ncsc.gov.uk/news/svr-cyber-actors-adapt-tactics-for-initial-cloud-access> accessed 10 May 2024.

[185] There have been some legislative attempts from the European Union addressing 'incident's and 'large scale incidents' and defining 'cyber threat' and 'significant cyber threat' including among sectors of high criticality the inland, sea and coastal passenger and freight water transport companies, managing bodies of ports and operators of vessel traffic services; see European Parliament and the Council Regulation (EU) 2019/881 of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [2019] OJ L151/15; European Parliament and the Council Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) [2022] OJ L333/80, arts 2; 6.3-4; 6.6-7; 6.10-11, Annex I; Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers [2024] OJ L 2024/2690, art 3.

exposures private is the trustworthiness and reputation protection of the company that has been a victim of a cybersecurity breach or attack.

Many jurisdictions, including Singapore, have made disclosure obligatory. In some cases, shipping companies are obliged to report their cyber security breaches and outline actions taken after the incidents. According to s 14(1) of the Singapore Cybersecurity Act 2018,[186] the owner of critical information infrastructure has to report cybersecurity incidents and, in case of unreasonable compliance failure, faces a fine or imprisonment. Shipping companies throughout the shipping sector fall within the definition of the owners of 'critical information infrastructure' since they provide essential services via computer systems, and the loss or compromise of that system can have a 'debilitating effect on the availability of the essential service in Singapore' (s 7(1)(a)) and the computer or computer system is 'located wholly or partly in Singapore' (s 7(1)(b)).[187] Protection from data breaches is also achieved through investigating incidents by the Personal Data Protection Commission (PDPC). These can lead to suspension or discontinuation[188] of the investigation or measures following breach findings, such as warnings, directions, financial penalties or a combination of the last two.[189] Organisations must assess the data breach and make it known to the PDPC if it is notifiable.[190] In order to remain compliant with the Personal Data Protection Act 2012, such organisations which 'potentially contravened' the Act may make voluntary undertakings[191] by proposing a remediation plan to address the breach and any

[186] No 9 of 2018.

[187] See further s 7.

[188] Personal Data Protection Act (PDPA) 2012 (2020 rev ed), s 50.

[189] See ss 48I–48K and ss 50-51. See also *Guide on Active Enforcement: Revised on 1 October 2022* (Personal Data Protection Commission Singapore) 14 <https://www.pdpc.gov.sg/help-and-resources/2019/05/guide-on-active-enforcement> accessed 30 August 2024.

[190] See s 26B; s 26D.

[191] The written voluntary undertaking is given when there are reasonable grounds for non-compliance now or in the future (s 48L(1)) and the CDPC has the discretion to accept it and may make additional suggestions and comments (s 48L(3)). The publication of the undertaking might be part of the undertaking of the organisation (s 48L(2)(c)) or might be performed by the Commission if it was part of the undertaking and the organisation fails to complete it. However, if the publication is not part of the undertaking, it will not be published (s 48L(5)).

systemic shortcomings in the future to remain compliant.[192] However, this does not waive their responsibility if they breach the Act and enforcement measures will still be taken against them. The number of voluntary undertakings fluctuates but is increasing.[193] The number of decisions of the PDPC regarding data breaches outnumbers[194] the undertakings, perhaps because of the reputation protection of the organisations in breach of the data protection legislation. For instance, an incident with a ferry operator with unauthorised access to the personal data of 108,488 individuals who booked tickets on its website only appears on the enforcement decisions list.[195] However, cases like the logistics, trucking and freight-forwarding services providers appear in both lists.[196]

This legal obligation creates a feeling of security in the light of the upcoming trial of digital ship identities known as Marine Vessel Pass (MVP) in Singapore for vessels transiting between the Port of Singapore and the Port of Rotterdam for quicker port clearance and bunkering or refuelling

---

[192] Personal Data Protection Commission Singapore (PDPC), 'Undertakings' <https://www.pdpc.gov.sg/undertakings> accessed 30 August 2024.

[193] The number of cases increased from single to double digits from 2020 to 2023, with a small decline in 2022. In three trimesters of the 2024 there were 29 cases: ibid.

[194] Personal Data Protection Commission, 'Enforcement Decisions' <https://www.pdpc.gov.sg/all-commissions-decisions> accessed 30 August 2024.

[195] The Singapore-based ferry operator, which notified in April 2023 the Commission about a data breach had previously been fined in 2019 for another personal data breach on its website and received a warning in October 2020 for 'failing to have reasonable security arrangements to protect the personal data' in its email account. See further, Horizon Fast Ferry Pte Ltd [2024] SGPDPC 1, Case No. DP-2304-C0943 (Personal Data Protection Commission Decision, 21 February 2024) 1; 30; 32. <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_keppel-telecommunications--transportation-ltd_14052024.pdf> accessed 30 August 2024.

[196] The breach of the data protection obligation continued for more than two years, resulting in the exposure of data of approximately 22,659 individuals and possible data exfiltration of up to 7,184 of them with, among others, specimen signatures, identification cards and/or bank account numbers and images. See Keppel Telecommunications & Transportation Ltd [2024] SGPDPC 3, Case No. DP-2210-C0378 (Personal Data Protection Commission, 14 May 2024) 1; 5-7; 9-12; 36-41 <https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/commissions-decisions/gd_keppel-telecommunications--transportation-ltd_14052024.pdf> and Personal Data Protection Commission, 'Undertaking by Geodis Logistics Singapore Pte Ltd' <https://www.pdpc.gov.sg/undertakings/undertaking-by-geodis-logistics-singapore-pte-ltd> accessed 30 August 2024.

operations.[197] Following the testing process, during the regular operation of the system, any disruptions in the verification of ship credentials will be notified and dealt with, creating previous experience and identifying any cyber security gaps in the process.

The UN General Assembly has also taken steps to combat cybercrime, adopting The UN Convention against Cybercrime on 7 August 2024. The preamble includes a declaration of the states to prosecute cyber crimes 'wherever they occur', in effect creating a crime against humanity, similar to piracy.[198] The Convention encourages the collaboration and sharing of information among the member states to eliminate cybercrime, which it identified as (a) the illegal access to information and communication technologies (Art 7), (b) the illegal interception of non-public data transmissions of electronic data (Art 8), (c) different ways of illegal interference with data, information and communication systems (Arts 9 and 10), (d) misuse of devices for those purposes (Art 11), (e) information and communications technology system related forgery, theft and fraud (Arts 12 and 13). The liability expands from natural persons to legal persons and to participation and attempt (Arts 18 and 19).

4 Insurance cover

Insurance coverage is usually set by the primary insurance market (insurance), sometimes followed by a secondary insurance market (reinsurance). Standard insurance clauses are usually used, sometimes modified for the safety and certainty of the contracting parties. These clauses are available from the Lloyd's Market Association in the Lloyd's Wording Repository (LWR),[199] and are updated and revised when required by the industry.

---

[197] Esther Loi, 'Ships to Trial Use of Singpass-like Digital Identity for Port Clearance and Refuelling' *The Straits Times* (Singapore, 16 April 2024) <https://www.straitstimes.com/singapore/transport/ships-to-trial-use-of-singpass-like-digital-identity-for-port-clearance-and-refuelling> accessed 29 August 2024.

[198] A/AC.291/L.15.

[199] The Repository, launched in August 2006, includes the wording developed by the Lloyd's Market Association (LMA) and by other industry organisations, individual managing agents, other insurers and brokers. See further

4.1 MIA 1906 and IA 2015

The principal marine insurance legislation is the Marine Insurance Act 1906 (MIA 1906), as amended by the Insurance Act 2015 (IA 2015). Other former British colonies, such as India[200] and Singapore,[201] apply the MIA 1906 with minor modifications. Moreover, because marine insurance is usually based on common law and, in most cases, English law, the legislation is also applicable where a foreign court has to decide on the merits agreed upon by the parties in their marine insurance contract.

The MIA 1906 refers in s 3 to pirates, war perils and thieves. The phrase, 'any other perils, either of the kind or which may be designed by the policy', might include new kinds of perils if they are classified as marine perils and provided cybersecurity incidents are treated as 'fortuitous accidents or casualties of the seas' pursuant to Schedule 1 of the Act. Given that the vessel is exposed to this risk while at sea, the consequences of the initial cybersecurity breach can appear when the vessel is far from the port and on its way to its destination. The absence of specific software programmes and hardware backup, uninformed crew members and officers, and outdated cyber protection programmes aboard a vessel could render it unseaworthy, resulting in the insurer not being liable under s 39 of the Act. Thus, for instance, a vessel might be exposed to a cyber incident while on its way under a voyage policy (s 39(1)), exposed while in port (s 39(2)), while performing a stage of its voyage (s 39(3)), or when sent to sea in an unseaworthy state while covered by a time policy (s 39(5)). In addition, where a situation affecting the navigation of the vessel is not detected immediately, the assured could be in breach of the provisions of s 44 if the

---

Lloyd's Market Association, Underwriting Team, Wordings <https://www.lmalloyds.com/lma/Underwriting/Wordings/LMA/lma_wordings.aspx> accessed 9 August 2024; 'LMA launches London market wordings repository' *Insurance Times* (London, 25 August 2006) <https://www.insurancetimes.co.uk/lma-launches-london-market-wordings-repository/1327617.article> accessed 9 August 2024.

[200] The MIA 1906 was the prototype of the Marine Insurance Act 1963, Act No 11 of 1963.

[201] See the Marine Insurance Act 1906 (2020 rev ed). The 1906 Act has also been influential in Canada: see the Marine Insurance Act SC 1993, c 22 and Aldo Chricop et al, *Canadian Maritime Law* (2nd edn, Irwin Law 2016) 400 et seq.

vessel sails to a different destination, s 45 if the vessel changes its voyage in an apparent way, and s 46 in case of deviation from the course of the voyage designed by the policy (s 46(2)(a)) or which is usual and customary as a course (s 46 (2)(b)). It is worth mentioning that in the case of s 45(2) the policy could provide for the maintenance of the coverage when the vessel or the assured contact the insurer and notifies it that the change of voyage is the result of a cybersecurity breach or cyber attack and not a manifestation of the determination to change the voyage. In the same way, s 46(1) could foresee a previously detected and notified disturbance in ship navigation due to a cybersecurity incident as a lawful excuse that waives the discharge of liability for the insurer. However, in order for those scenarios to work, the assured would have to disclose in good faith (s 17) all the material circumstances known to him or which he is deemed to know (s 18), including any communication and information available to the assured from the vessel and ashore exposing or jeopardising the vessel.

The IA 2015 would give more opportunities to the assured to regain cover if permitted.[202] Thus, a failure to update software would make the vessel unseaworthy, but an update provided later would reinstate the insurance coverage. It is understandable that if the risk occurs due to the absence of updated software during the specific period when the vessel is vulnerable, it is most likely to be exposed and face a loss which will not be recoverable. The assured may try to prove that to the best of his ability and knowledge, he had taken all the measures before the commencement of the insurance and that there was no misrepresentation at the beginning of the voyage or when the cover was initiated.[203]

---

[202] For instance the JH009 Insurance Act 2015 Endorsement (For use with CL602 International Hull Clauses (01/11/03)) (15/08/2016) cl 10.1 excludes from application s 10(5)(a) and s 10(6) of the Insurance Act 2015 and cl 4 excludes from s 11 of the Insurance Act 2015 a whole list of clauses of International Hull Clauses (cl 4 (d) – (h)) obligation of classification (cl 4(i)).

[203] If the breach was deliberate or reckless, then the insurer will avoid the liability and might also retain the premiums paid as per s 8 and schedule 1 of the Insurance Act 2015. Otherwise the premiums will have to be returned if the insurer would not enter the contract or higher premium can be demanded. Also, unless the risk of loss is caused by the non-compliance as per s 11 of the IA 2015, the insurer will have to pay the assured. See further Rob Merkin and Özlem Gürses, 'The Insurance Act 2015: Rebalancing the Interests of Insurer and Assured' (2015) 78 MLR 1004.

4.2 Risks covered

The risks discussed earlier, starting from piracy and war risks and ending with terrorism and cyber risks, are all covered under different insurance products. Marine insurance clauses[204] provide coverage for war risks, [205] terrorism risks and piracy risks. Cyber risks[206] can be found in only a few clauses relating to marine insurance. So-called 'new risks' such as cyber war, cyber terrorism and cyber attacks are currently only covered or excluded with or without an option of write-back by general commercial cyber insurance and commercial terrorism insurance. Cybersecurity is covered in other insurance contracts not explicitly designed for the maritime industry.[207]

The usual construction of marine insurance clauses includes coverage of piracy and terrorism within the war risks when the Nordic Plan[208] is applicable and in the marine perils when subject to English law and marine insurance. Terrorism is usually covered as part of war risks, but it can also be covered as a separate risk. There are also specific provisions for insurance coverage for 'terrorism' in the LMA3030-Terrorism Insurance – Physical Loss or Physical Damage Wording, which gives protection from terrorism and sabotage as this insurance policy defines these terms. It expressly excludes war and warlike operations (s 3, cl 2) and computer hacking and computer

---

[204] *Reference Book of Marine Insurance Clauses 80th Edition 2023 (Marine Insurance Clauses 2023)* (Witherby Publishing 2023), pp iii-ix, 45; 52; 64; 81; 97.

[205] See, eg, CL255 Institute War Clauses (Cargo); CL257 Institute War Clauses; CL262 Institute War and Strike Clauses; CL270 Institute War, Atomic and Nuclear Exclusion (Cargo Reinsurance); CL271 Institute War Cancellation Clause (Cargo); CL278 Institute War Clauses (Commodity Trades); CL281 Institute War and Strikes Clauses; CL295, CL296, CL297 Institute War and Strikes Clauses; CL300 Institute War and Strikes Clauses Hulls – Time Limited Conditions; CL 303 Institute War, Atomic and Nuclear Exclusion (Hull Reinsurance); CL. 340 Institute War and Strikes Clauses Containers – Time; CL345 Institute Protection and Indemnity War Strikes Clauses Hulls – Time; CL.349 Institute War Clauses Builders' Risks; CL359 Institute Notice of Cancellation, Automatic Termination of Cover and War and Nuclear Exclusion Clause - Hulls, etc.

[206] See CL365 Institute Chemical, Biological, Bio-Chemical, Electromagnetic Weapons and Cyber Attack Exclusion Clause; JS001 Cyber Attack Exclusion Clause and Write-Back; JS005 Cyber Exclusion (Targeted Cyber Attack Write-Back), JS 006 Limited Cyber Coverage Clause (Targeted Cyber Attack Write-Back).

[207] See, eg, Hiscox Cyber Clear Policy 2019 and the Beazley Breach Response Policy 2019; Azevedo (n 153).

[208] See above n 84.

viruses unless these computer systems are used for launching or firing any weapon or missile (s 3, cl 9).[209]

The general Institute Clauses provide War and Strikes risks coverage,[210] including war, acts of war[211] and acts of terrorism but make no direct reference to piracy in the included or excluded risks. A slightly different approach can be seen in Strikes Clauses for Commodity Trades,[212]where acts of terrorism[213] are covered, but acts of war[214] are excluded, and there is no reference to piracy risks. Lastly, some clauses refer only to war risks. However, the War Clauses[215] cover only acts of war, excluding the use of nuclear weapons in such context, and completely omit any reference to terrorism and piracy as risks in the included and excluded risks lists.

The Lloyd's Market Association (LMA) introduced general Cyber Exclusion Clauses in 2018,[216] while the Cyber War and Cyber Operation Exclusion Clauses were introduced in 2021.[217] Clauses

---

[209] See further Azevedo (n 153) A16-001.

[210] See further CL397 Institute War and Strikes Clauses:(Cargo stored afloat in mechanically self-propelled vessels), 1/05/2016, cl 1.1, 1.5 .

[211] Excluding war between the big five nations as typically listed in war risks insurance coverages (cl 3.8 and cl 3.9), as well as war with the use of nuclear power weapons, and leading to automatic termination of the insurance contract: cl 14.1.1.1 and 14.1.1.2: ibid.

[212] CL398 Institute Strikes Clauses (Commodity Trades)(Agreed with The Federation of Commodity Associations), 1/05/2016.

[213] Ibid, cl 1.2.

[214] Including the usage of the nuclear weapons, ibid, cls 3.9; 3.10.

[215] CL399 Institute War Clauses (Commodity Trades) (Agreed with The Federation of Commodity Associations), 1/05/2016, cl 1.1 and 3.8. See also CL416 Institute War Clauses (FOSFA Trades) (Agreed with The Federation of Oils, Seeds and Fats Associations), 1/06/2013, cls 1.1; 3.8.

[216] LMA5322 Cyber Act and/or Denial of Service Exclusion (for use with Personal Accident and Sickness Policies), LMA5241A Cyber Loss Limited Exclusion (Property Treaty Reinsurance) No 1, LMA5327 Cyber Loss Limited Exclusion (Property Treaty Reinsurance) No 2, LMA5400 Property Cyber and Data Endorsement, LMA5401 Property Cyber and Data Exclusion, LMA5404 Cyber and Data Exclusion (for use on Consumer and Commercial Property Risks), LMA5405 Limited Cyber and Data Exclusion (for use on Consumer and Commercial Property Risks). See further Azevedo (n 153) [3-040]; [3-043–3-047]; [3-049].

[217] The LMA Cyber Business Panel drafted the clauses LMA5564, LMA5565, LMA5566 and LMA5567 all provide exclusions from War, Cyber War and Cyber Operation with some variations for the insurers and reinsurers to choose from and provide different cover levels for cyber operations between states which are not excluded by the definition of war, cyber war or cyber operations. See further Partick Davison, 'Cyber War and Cyber Operation Exclusion Clauses' (Lloyd's Market Association Bulletin, Media Centre, LMA21-042-PD, 25 November 2021) <https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA21-042-PD.aspx> accessed 9 August 2024.

referring to cyber risks and used for exclusions from marine insurance are LMA5402 Marine Cyber Exclusion and LMA5403 Marine Cyber Endorsement.[218]

Additionally, there are clauses related to marine cyber risks[219] and others that provide exclusions from cyber risks in general.[220]

The International Association of Engineering Insurers (IMIA) provide definitions of Cyber War and Cyber Terrorism in IMIA Advanced Cyber Exclusion 2018.[221] As per their wording:[222]

> Cyber War means any state of hostile conflict (whether declared or not) to resolve a matter of dispute between two or more states, nations, or political entities or organisations by using – wholly or partially – Computer Systems or the internet, to render non-functional, disrupt, subvert or make disruptive use of any Computer System, Computer Network, IT infrastructure, the internet, the intranet, telecommunications and/or its content.
>
> Cyber Terrorism means any disruptive act or series of disruptive acts or threat thereof of any person or group of persons, whether acting alone or on behalf of or in connection with any organisation through the use of Computer Systems, to destruct, disrupt, subvert or make use of any Computer System, Computer computer Network, IT infrastructure, the internet, the intranet, telecommunications and/or its content, committed for religious,

---

[218] Azevedo (n 153) [3-052].

[219] Other clauses related to marine cyber risks are: CL437 JCC Cyber Exclusion and Write-Back Clause; JC2019-004 Cyber Coverage Clause (for cargo insurance); JC2020-0014 Cyber Endorsement – Marine Cargo Cyber Exclusion and Affirmation Endorsement; JR2019-001 JRC CL 380 Buyback Endorsement; JSC2019-005 Cyber Exclusion (Targeted Attack and Write-Back); JSC2019-006 Limited Cyber Coverage Clause (Targeted Cyber Attack Write-Back), ibid, [3-053–3-054]; [3-075]; [3-059–3-060].

[220] Other clauses provide exclusions from cyber risks: See, eg, NMA2914 Electronic Data Endorsement A; NMA2915 Electronic Data Endorsement B; AVN0124 Data Event Clause. However, Cyber Loss is covered with some restrictions in reinsurance clauses in LMA5241A Cyber Loss Limited Exclusion (Property Treaty Reinsurance) No.1 and LMA5327 Cyber Loss Limited Exclusion (Property Treaty Reinsurance) No 2, which also include definitions of Cyber Loss, Cyber Act and Cyber Incident, ibid, [A3-001–A4-001]; [A9-001]; [A11-001–A12-001].

[221] Ibid, A7-001; cls 1; 2; 4.

[222] Ibid, A7-001; cl 4.

ideological or political purposes including but not limited to the influencing of any government and /or to put the public or a section of the public in fear.

The IMIA clause Endorsement – IMIA Cyber Exclusion 2018 (Short Version) allows a buyback with an additional premium, but Cyber War and Cyber Terrorism are explicitly excluded from this option.[223] This shows that these cyber risks are already defined with some broad wording and are accepted, although excluded from the existing cyber coverages.

4.3 Hull and Machinery

Depending on the Institute Hulls Clauses used, piracy may be covered as a risk.[224] For instance, piracy is listed in the coverable perils under cl 6.1.5 of the Institute Time Clauses Hulls 1/10/83,[225] in cl 4.1.5 of the Institute Voyage Clauses Hulls 1/10/83,[226] and in cl 4.1.5 of the Institute Time Clauses Hulls Port Risks 20/7/87.[227] In other clauses, such as the Institute Protection and

---

[223] The 2016 IMIA Working Group Paper questioned the need for the distinction between acts of war, terror or sabotage for losses caused by a cyber event when the motives of the attacker were not clear: see IMIA Working Group Paper 98 (16), IMIA Annual Conference 2016 – Doha, Qatar, 'Cyber Risks – Engineering Insurers Perspective' (IMIA, Rev.A002, 16 September 2016) <https://www.imia.com/wp-content/uploads/2023/09/IMIA-WGP-09816-Cyber-risks.c.pdf> accessed 30 August 2024, [5.3.1]. For the IMIA Cyber Exclusion 2018 (Short Version) Clauses, see Azevedo (n 153) A8-001; cl 1, Example for a PD/BI Buy-back.

[224] Tokio Marine Nichido Hull Insurance Clauses No. THI-21E (Tokio Marine & Nichido Fire Insurance Co Ltd) <https://www.tokiomarinenichido.co.jp/hojin/marine_site/senpaku/covenant/pdf/hull_insurance_clause_20210401.pdf> accessed 30 August 2024.

[225] Institute Time Clauses Hulls, 4/4 Collision Liability. War risk is excluded by cl 23, and terrorist actions are excluded in strikes exclusion cl 24.2. The same goes for the Institute Time Clauses Hulls, 1/10/83, cl 6.1.5, and cl 23 and 24.2, and the Institute Time Clauses – Hulls Disbursements and Increased Value (Total Loss only, including Liabilities) 1/10/83, cl 6.1.5 for piracy coverage and cls 12 and 13.2 for war risks and terrorist attacks. The same provisions can be found in the Institute Time Clauses Hulls 1/11/95, cl 6.1.5, which provides coverage for piracy, and cl 24, which excludes war risks and cl 25, excluding terrorist attacks. The International Hull Clauses 1/11/03 cover piracy as per cl 2.1.5 and excludes war (cl 29.1) and terrorism (cl 30.1).

[226] See cl 4 Perils whereas the same policy excluded war risks, see cl 20 War Exclusion and cl 22 Malicious Acts Exclusion cl 22.2 when referring to 'any weapon of war', but describes terrorist attacks as 'caused by any person acting […] from a political motive' in cl 22. In the Institute Voyage Clauses Hulls (Amended for Japanese Clauses Class No 5 (4/2010) 1/10/83 piracy as well as violent theft by persons from outside the Vessel (which can be interpreted as armed robbery) are explicitly deleted: see further cl 4.1.3; cl 4.1.5. The same occurred in the Institute Time Clauses – Hulls Total Loss Ony (Including Salvage, Salvage Charges and Sue and Labor) (Amended for Japanese Clauses Class No 2 (4/90), cl 6.1.3; cl 6.1.5.

[227] See cl 4 Perils. See also cl 22 War Exclusion and cl 24 Malicious Exclusion, which exclude war and terrorism risks.

Indemnity Clauses Hulls – Time 20/7/87,[228] war risks and terrorist actions are explicitly excluded in cls 10.1, 10.5 and 10.6. At the same time, an exception is made for piracy.

The Institute War and Strikes Clauses Hulls – Time 1/10/83 excluded piracy (cl 4.1.7) and covered war risks and terrorist attacks (cls 1.1 and 1.5), but after amendment (version 4/2010, cl 4.1.7), piracy is deleted from the exclusions. It can be understood to be covered by cl 1.2 as a seizure of the vessel.[229]

More recent editions of the Hull coverage clauses, namely CL600 International Hull Clauses 01/11/02[230] and CL601 International Hull Clauses 01/11/03,[231] cover piracy and explicitly exclude war risks and terrorism risks. International Hull Clauses 01/11/03 covers piracy in cl 2.1.5, rearranges the war risks, combining them with strikes in cl 29 and creates a combined cl 30 Terrorist, Political Motive and Malicious Acts Exclusion, including terrorism (cl 30.1) and action from political motive (cl 30.2) with malicious weapon detonation (cl 30.3).[232] Also, piracy might be covered via an endorsement.[233]

For a shipowner to be covered, it must follow the best practices guide for areas listed as highly risky for piracy attacks and take all the measures applicable and allowed by the local governments close to which territorial waters the attacks may take place.[234]

---

[228] Amended (1/060 (for Class No 2 PDC). See cl 10 of the War, Strikes, Malicious Acts and Nuclear Risks Paramount Exclusion. The same applies to the amended text (1/06) cl 10.

[229] The same can be seen in the Institute War and Strikes Clauses Hulls – Time Amended to Cover Disbursements etc. Against TLO (4/2010).

[230] Marine Insurance Clauses 2023 (n 204), cl 2.1.5, cls 29, 30.2.

[231] Ibid, cl 2.1.5, cls 29–30.

[232] See <https://www.iua.co.uk/IUA_Member/Clauses/eLibrary/Clauses_Search.aspx?CAT=Marine> accessed 29 September 2024.

[233] As in JH041 Marine Hull Electronic Date Recognition Endorsement 11/08/98, cl 2.c.v.

[234] In some jurisdictions, the use of private armed guards is allowed, whereas in others, it is prohibited, with an obligation to employ local armed guards or law enforcement agencies. Cf Guardcon 2012, downloadable from <https://www.bimco.org/contracts-and-clauses/bimco-contracts/guardcon> accessed 4 November 2024.

4.4 P&I Clubs and the International Group of P&I Clubs

Piracy is covered, among others, by the Protection and Indemnity (P&I) Clubs Hull Time insurance and is listed as a war risk[235] but excluded from cl 10. This means it would be covered in case of occurrence, as long as the insured and its servants and agents take all the reasonable measures to avert or minimize a coverable loss as per cl 8. Acts of war and terrorism, as well as war in general, are excluded from this clause.

The need for clarification of the meaning of the war risk and the inclusion or exclusion of the terrorism risk arose with the Athens Convention Protocol 2002.[236] Consequently, after multiple interventions by the interested parties, including the International Group of P&I Clubs,[237] the IMO in 2006 issued a Reservation and Guidelines for Implementation.[238] This created two distinctive insurance covers, for war risks[239] and non-war risks,[240] each of the insurers covering only their part of the insurance. The former are covered by the war insurer and the latter by the P&I Club.[241]

---

[235] CL344, Institute Protection and Indemnity Clauses Hull-Time, 20/07/1987.

[236] Following the adoption of the Athens Convention Protocol 2002, only four ratifications of the required ten were deposited until 2006. The main concerns of the states related to the ability of the insurance market to provide adequate cover of the 'general limits' as set in the Protocol and the 'cover for injury and damage arising from acts of terrorism'. This led to the adoption by the Legal Committee of the proposed guidelines for the implementation of the Athens Convention as introduced in the Working Paper (LEG 92/WP.5). As a consequence, six more states acceded to the Athens Convention Protocol 2002, and it entered into force in April 2014: see further, 'Protocol of 2002 to the Athens Convention Relating to the Carriage of Passengers and Their Luggage by Sea, 1974: Entry into Force' (PAL.4/Circ.8, 3 May 2013).

[237] See 'Provision of Financial Security: (ii) Follow-up on resolutions adopted by the International Conference on the Revision of the Athens Convention Relating to the Carriage of Passengers and Their Luggage by Sea, 1974 – Submitted by the International Group of P&I Clubs and the International Union of Marine Insurance (IUMI)' (LEG 90/6/2, 18 March 2005).

[238] See further 'Athens Convention Relating to the Carriage of Passengers and Their Luggage by Sea (PAL)' (IMO, Conventions)<https://www.imo.org/en/About/Conventions/Pages/Athens-Convention-relating-to-the-Carriage-of-Passengers-and-their-Luggage-by-Sea-(PAL).aspx> accessed 10 November 2024.

[239] War insurance covers war risks as listed in Guidelines cl 2.2, and both the war and acts of any terrorist are included. There is no explicit exclusion of piracy from the 'capture, seizure, arrest, restraint or detainment' with their consequences or any attempt; see further IMO Guidelines for Athens Convention (n 236) Annex, 3.

[240] Non-war insurance is in general referred as covering 'all perils subject to compulsory insurance' which are not listed in the cl 2.2. It is irrelevant if they are 'subject to exemptions, limitations or requirements'of the cl 2.1. The cl 2.1 refers among others to the Institute Clause 370 (cl 2.1.1) and the Institute Clause 380 (cl 2.1.2).

[241] Examples of insurance undertakings (Blue Cards) referred to in guideline 3, 7-8, II. Model of Certificate of Insurance Referred to in Guideline 3, 9.

Further, the limited coverage by the P&I Clubs for war risks in excess of the already existing war risks changed after 9/11 and could not cover terrorism risks.[242]

The P&I Clubs individually decided to provide insurance and to seek reinsurance for war risks and non-war risks.[243] Their rulebooks provide insights into the particular provisions and can be differentiated by variations in wording.[244] Gard, for example, provides coverage of liabilities for passengers for non-war risks[245] and limited cover for the war risks derived from certificates the Club has issued previously.[246] Piracy is excluded from the Rule 58 list of non- coverable risks on the condition that ransom is not recoverable.[247] Furthermore, it provides additional war risk insurance as described in that Rule.[248] There is a special insurance cover for Container and Equipment[249] where marine war risks are covered.[250]

The Britannia P&I Club has a general exclusion for war and terrorism risks with the exception of piracy,[251] and allows for agreement in writing for the cover of war risks with some limitations

---

[242] See further 'Any Other Business: Liability Cover Under the Protocol of 2002 to the Athens Convention, 1974 – Submitted by the International Group of P&I Clubs' (LEG88/12/2 19 March 2004).

[243] See further 'Insight: Athens Convention and EU Passenger Liability Regulation 2009 (PLR)' (n 239).

[244] Only some examples of the Club rules are referred to in what follows.

[245] Rule 28.2. See further Gard Rules 2024 for Ships 2024 (Gard Rules 2024) <https://gard.no/rules-statutes-and-guidances/guidance/gard-rules-for-ships-2024/> accessed 12 November 2024.

[246] See further Rule 58.2 and Rule 58.2, ss i–vi.

[247] A discretion to the directors to decide otherwise is reserved in rule 58.1.b. See further Gard Rules 2024 (n 245).

[248] The cover 'includes the liabilities from acts of terrorism as defined in the US Terrorism Risk Insurance Act 2002 as amended, which now has been extended to 2027' (cl 2.1) but excludes loss, damage or expenses arising from an act of terrorism when the insured is liable under TOPIA 2006 (cl 3). The limit of cover is for US$500m in general (cl 5) and for a smaller amount of US$80m for transiting within all Russian waters (cl 6), all inland waters of Ukraine (cl 6.2) and areas indicated in cls 6.1, 6.3-4. See further Appendix I: Additional Insurances, ibid.

[249] See further Gard Additional Covers: Terms and Conditions 2024 <https://gard.no/rules-statutes-and-guidances/> accessed 12 November 2024.

[250] However, the cover for marine war risks (1) is terminated automatically in any hostile detonation of any nuclear weapon of war irrespective of the time and place of the occurrence (Appendix 6: Notice of Cancellation and Automatic Termination Clause (CL JL2022-020), cls 2.1. 2.1.1), (2) does not cover damages in connection with the Russia-Ukraine conflict, in any territorial area related to these states and other neighbouring countries affected by the conflict (Appendix 6: Territorial and Conflict Exclusion Clause, (Cl JL2022-019 21 December 2022) cl 1), and (3) contains an exclusion for the outbreak of war between five powers and requisition for title or use of the ship (Appendix 7: Five Powers War Exclusion).

[251] Rule 25.1 General Exclusion of War Risks: Britannia P&I Club Rules 2024/25 Class 3: Protection & Indemnity Rules <https://britanniapandi.com/wp-content/uploads/2024/08/Britannia-Rules-2024-Class-3-P_I-English.pdf> accessed 12 November 2024.

related to the prohibited areas.[252] The Club also provides cover of liabilities it undertook when issuing certificates in compliance with international conventions.[253] Additionally, the Club allows for extensions to cover for war[254] and terrorism risks for both the war and strikes clause and the exclusions, limitations and warranties clause.[255]

As a final example, NorthStandard P&I Club excludes war risks[256] subject to the guarantees, undertakings and certificates it has provided in compliance with international and national legislation.[257] Additionally, the Rules provide the P&I War Risks Clause 2024 and War Risks Clause for Additional Covers 2024, which contain provisions for exclusions and termination of cover. The War Risks Rules apply partially to British ships (Part A) and to all ships (Part B).[258] Whether an

---

[252] Rule 25.2 Provision of Cover for War Risks, see ibid.

[253] Pursuant to the compliance with the obligations of the insured under rule 25.3.7, the insurer undertakes to cover war risks related liabilities for all the certificates, as in the case of the Gard, with the exception of acts of terrorism, which creates liabilities, costs or expenses for IOPC Fund 1992 in connection with TOPIA. See further rule 25.3.1-6, see further Britannia P&I Rules 2024 (n 251).

[254] There is no exclusion of piracy in the definition of war risks in cls 1.1.2, 6.1.2 therefore the piracy is covered as well, see further Part II: Extensions to Cover, Clause War and Strikes Risks, cl 1 and , Part IV Clause Exclusions, Limitations and Warranties, cls 6.1, Britannia P&I Club 2024/25 Additional Insurance: Terms & Conditions (Version 5.00 February 2024) <https://britanniapandi.com/wp-content/uploads/2024/03/Additional-Insurances-2024.pdf> accessed 12 November 2024.

[255] The war (cl 1.1.1) and acts of terrorism (cl 1.1.5) are covered with the exception of the use of any chemical, biological, bio-chemical or electromagnetic weapon (cl 1.2) and considering the five power war exclusion (cl 1.5.1) and the automatic termination upon the usage of any nuclear weapon (cl 1.6.1), see further Part II: Extensions to Cover, Clause War and Strikes Risks, cl 1, Part IV Clause Exclusions, Limitations and Warranties, cl 6, ibid (n 269).

[256] Rule 4.3(1) provides for war and acts of terrorism whereas rule 4.3(2) excepts piracy from the exclusion of war risks: NorthStandard P&I Rules 2024/25 <https://d3cpegos94401u.cloudfront.net/publications/documents/rulebooks/pi-rule-book-2024-25-v8.pdf> accessed 11 November 2024.

[257] The list of certificates refers to (1) Section 2 of US Public Law 89-777, (2) CLC 1969 or CLC 1992, (3) IOPC Fund 1992 with STOPIA with the exception of ct of terrorism leading to liability with TOPIA, (4) Bunker Convention 2001, (5) Athens Convention Protocol 2002, (6) Wreck Removal Convention, (7) Maritime Labour Convention 2006 and (8) any undertaking issued by the Club pursuant to 'any statute, convention, treaty or law', see further rule 4.5.

[258] The Club is providing cover for partial or total loss of 'hull, materials, machinery and other parts and equipment' caused by war and acts of terrorism (rules 2.B.1.1, 2.B.1.5) and piracy (rule 2.B.1.6) provided that there is no insurance cover for Part A which applies to British ships (rule 2.B.2), see further NorthStandard War Risks Rules 2024/25<https://d3cpegos94401u.cloudfront.net/publications/documents/rulebooks/war-rule-book-2024-25.pdf> accessed 11 November 2024.

action constitutes an act of terrorism is decided finally by the P&I Directors.[259] In the case of ransom payment, this is not usually recoverable unless the Member's Committee decides otherwise, considering the shipowner's reasonable precautions 'to avoid the event that gave rise to the ransom.'[260]

Moving away from the P&I rulebooks, when coverage is provided explicitly for war, as in the Protection and Indemnity War Strikes Clauses Hull-Time,[261] piracy is excluded (cl 2.7), and war, acts of war and terrorism are covered (cls 1.1, 1.3, and 1.5). However, the usage of nuclear weapons as an act of war is not covered (cl 2.1), as well as war between the big five countries listed in the exclusion cl 2.2.[262] Apart from war risk cover, there might be an additional, special war risk P&I Insurance contract,[263] agreed with the individual member, also covering liabilities arising from 'acts of terrorism as defined in the US Terrorism Risk Insurance Act 2002'.[264] War and terrorism risks are also covered by the Athens Convention 2002 (cl 1.1)[265] but explicitly excludes cyber attack regarding the CL380 Institute Cyber Attack Exclusion Clause 10/11/03 (cl 1A.2.c).[266]

Cyber risks are explicitly excluded by the LMA5403 Marine Cyber Endorsement 11/11/2019 clauses.[267]

---

[259] UK Club P&I Rules 2024, Rule 5E <https://www.ukpandi.com/media/files/uk-p-i-club/rules/2024/rulebook-2024.pdf> accessed 30 August 2024.

[260] Ibid.

[261] CL345, Institute Protection and Indemnity Clauses Hull-Time, 20/07/1987.

[262] This refers to an outbreak of war, be it with or without a declaration of war, as long as the parties involved are at least two of the United Kingdom, the United States of America, France, the Union of Soviet Socialist Republics, and the People's Republic of China.

[263] Cf the War Risks Extension of the UK P&I Rules 2024, which excludes risks connected with the Russia-Ukraine conflict, inside territorial waters exposed to that conflict and in territorial waters of the neighbouring countries. See further UK Rules (n 235) Appendix II.

[264] As amended and extended until 2027. See further 'Gard Rules 2024 for Ships and Other Floating Structures' <https://assets.eu.ctfassets.net/jchk06tdml2i/s35xl34eA6djSnMdzWPy8/b7b4e37f0e6426179b834a95b9dba584/Rules_2024_for_ships.pdf> accessed 30 August 2024, Part II, Ch 2, Rule 58 and Appendix I, 2 War risks.

[265] The Athens 2002 PLR Extension Clause.

[266] Azevedo (n 153) [A1-001].

[267] 'Gard Additional Covers Terms and Conditions 2024'.

War risks are also reinsurable, usually by the International Group of P&I Clubs (IGP&I) Group Excess of Loss Reinsurance (GXL) programme. This was the case until the conflict between Russia and Ukraine began, which put more pressure on reinsurers. More specifically, the war cover was expressly referred to in the International Group Pooling and GXL Reinsurance contract structure for 2022[268] as the excess for it was renewed for 2022 for 12 months. In addition, it was also covered by the IGP&I Pooling and GXL Reinsurance contract for 2023/24. However, the IGs Excess War reinsurers required Territorial Exclusion language, consistent with the exclusionary language already applied by reinsurers for Primary War P&I coverage for vessels trading in waters affected by the ongoing conflict between Russia and Ukraine. The IG was negotiating the availability of sub-limited cover for affected vessels, and according to its estimations, the cover would be based on a significantly lower per-vessel limit compared to the main Excess War placement limit of US$500 million.[269] Nevertheless, the same reference is not in the IGP&I and GXL Reinsurance contract for the period 2024/25.[270]

<https://assets.eu.ctfassets.net/jchk06tdml2i/3HSTSYMEiZzBMliPX7b9jE/8c1ef076eb35ce915dd1b9bd1061784d/Gard_Additional_Covers_Terms_Conditions_2024.pdf> accessed 30 August 2024, see further Appendix 7, Marine Cyber Endorsement, 47.

[268] 'The International Group Pooling and GXL Reinsurance contract structure for 2022 has now been finalised', (News and Insights, 21 December 2021, IGP&I) <https://www.igpandi.org/article/international-group-pooling-and-gxl-reinsurance-contract-structure-2022-has-now-been-finalised/> accessed 9 May 2024.

[269] 'IG Reinsurance Contract (GXLStructure for the 2023/24 Finalized' (IGP&I) <https://www.igpandi.org/article/ig-reinsurance-contract-gxl-structure-for-the-202324-finalized/> accessed 9 May 2024.

[270] 'Reinsurance Contract (GXL) Structure for 2024/2025' (IG P&I, 19 December 2023) <https://www.igpandi.org/article/reinsurance-contract-gxl-structure-for-202425/> accessed 9 May 2024.

The IGP&I has produced informative guidance[271] in compliance with the MSC and other national,[272] regional and international[273] stakeholders to help its members avoid dangerous areas and in transit to safeguard their crew and property.

4.5 BIMCO and other contractual provisions

While piracy is a well-known marine peril, certain BIMCO contracts do not include any reference to it,[274] and in others, it is not included in war risks.[275]

Generally, piracy or acts of piracy and armed robbery, along with acts of terrorism and acts of war, are included. There are specific BIMCO War Clauses,[276] such as the BIMCO War Risks Clause for Time Chartering 2013 (Conwartime 2013),[277] where war risk is defined as any:

> […] actual, threatened or reported: war, act of war, civil war or hostilities […] acts of piracy and/or violent robbery and/or capture/seizure; acts of terrorists; acts of hostility and malicious damage;[…] by any person, body, terrorist or political group, or the government

---

[271] 'The 4th Edition of the Best Management Practices Has Now Been Released' (IG P&I, 26 August 2011) <https://www.igpandi.org/article/the-4th-edition-of-the-best-management-practices-has-now-been-released/> accessed 9 May 2024.

[272] See, for example, 'Denmark Presents its Counter-Piracy Strategy to the EU's Transport Council' (IG P&I, 16 June 2011) <https://www.igpandi.org/article/denmark-presents-its-counter-piracy-strategy-to-the-eus-transport-council/> accessed 9 May 2024, 'Best Management Practices – Piracy and Armed Robbery – West Africa' (IG P&I, 31 March 2020) <https://www.igpandi.org/article/best-management-practices-piracy-and-armed-robbery-west-africa/> accessed 9 May 2024.

[273] 'Submission to IMO MSC 90 – Guidance for Flag States on Measures to Prevent Somalia-Based Piracy – ICS, IG, ITF, BIMCO, INTERTANKO, INTERCARGO, Intermanager, ICC-IMB, IPTA, SIGTTO and WSC' (IG P&I, 12 March 2012) <https://www.igpandi.org/article/submission-to-imo-msc-90-guidance-for-flag-states-on-measures-to-prevent-somalia-based-piracy-ics-ig-itf-bimco-intertanko-intercargo-intermanager-icc-imb-ipta-sigtto-and-wsc/> accessed 9 August 2024.

[274] See, eg, Amwelsh 93, cl 27.2.b; AsbagasbillL cl 7.b.

[275] See, eg, Asbagasvoy cl 19 where 'the vessel, her master and owner shall not, unless otherwise provided expressly by the charterparty, be responsible for any loss or damage, or delay or failure in performing, arising or resulting from […] pirates or assailing thieves.'

[276] See Howard Bennett (gen ed), *Carver on Charterparties* (3rd edn, Sweet & Maxwell 2024) [4-452] et seq.

[277] BIMCO War Risks Clause for Time Chartering 2013 (Conwartime 2013), cl a.ii.

> of any state or territory whether recognised or not […] which may be dangerous or may become dangerous to the Vessel, cargo, crew or other persons on board the Vessel.

Similar provisions can be found in Amwelsh 93[278] charterparty. Clause 8 provides an exception from liability due to war, pirates or assailing thieves, and cl 27 refers to war risks, giving the right to the master to refuse to sign the bill of lading for a blockaded port (cl 27.1).

Other contracts have broader coverage. Thus, the BIMCO Bunker Terms 2018 – Standard Bunker Terms and Conditions – provides for the waiver of liabilities of both parties in case of loss, damage or delay caused by unforeseen act of war, act of terrorism or piracy characterised as force majeure. This happens provided the party invoking the clause has made all reasonable efforts to avoid, minimise or prevent the effect of those actions.

Gencon 2022[279] contains a war risks clause for voyage chartering at cl 33 (Voywar2013), and cl 34 refers to the BIMCO Piracy Clause for Single Voyage Charter Parties 2013. In comparison to Voywar 2013, where piracy (as part of war risks) is defined as 'acts of piracy and/or violent robbery and/or capture/seizure'[280] (cl (a)(ii)), the previous version of Voywar 2004, war risks included acts of war, acts of piracy and acts of terrorists (cl (a)(ii)). This also occurred with the BIMCO War Risks Clause for Time Chartering 2004 (Conwartime 2004) and the later version, Conwartime 2013.[281] The same definition of piracy can also be found in cl 39(a) of the BIMCO Piracy Clause for Time Charter Parties 2013, incorporated in the NYPE 2015 form.[282]

Cyber threat is dealt with separately in BIMCO Cyber Security Clause 2019, which refers to 'cyber security incident' as 'loss or unauthorised destruction, alteration, disclosure of, access to, or control of' digital environment, which is defined as 'systems, applications and devices and the

---

[278] Americanized Welsh Coal Charter Issued by the Association of Ship Brokers and Agents (USA), INC Recommended by BIMCO and FONASBA.

[279] Cf, as well as the earlier versions of Gencon, Gencon 1994, and Gencon 1976. For a detailed discussion, see Timothy Young et al, *Voyage Charters* (5th edn, Informa Law from Routledge 2022) ch 26.

[280] In the same way, piracy is defined in cl a of the BIMCO Piracy Clause for Single Voyage Charter Parties 2023.

[281] See also NYPE 2015, cl 34(a)(ii).

[282] Ibid, cl 39.

data in those systems'. The clause imposes some obligations on parties regarding preventing the occurrence of the incident and after the breach and gives the option to agree on the amount of liability for the breach. If left blank, cl (d) sets the limit at US$100,000.[283]

4.6 Most relevant case law

There are some cases concerning cybersecurity breaches and cyber-attacks that lead either to the violation of personal data or to compromise national security. However, there are very few cases related to the shipping industry, even though occasionally, some incidents become known from the publicity received. The actual mitigation processes and the remuneration and other obligations fulfilled by the defendants are usually not published for privacy reasons, as well as to protect the reputation and the shareholders' (for enlisted companies) and clients' trust.[284]

One of the first cases was *Glencore International AG v MSC Mediterranean Shipping Co SA*[285] in 2017. In this case, neither party disclosed that the other side was to be blamed for the exposure of its computer, but both parties received the same hacking email.

Following the NotPetya attack, there were two cases where the insurers relied on some provisions for war or warlike actions in order to avoid their liabilities. The first case was between a multinational pharmaceutical company, Merck, and multiple insurers and reinsurers providing it with twenty-six 'all risk' property policies for losses. Merck was claiming damages of US$699,475,000 due to the infection by the NotPetya of over 40,000 machines in its network. The court found that (1) the NotPetya malware was delivered in an accounting software used by

---

[283] Unless 'the breach resulted solely from the gross negligence or willful misconduct' of the party wishing to use the provision of the limitation of its liability (cl d).

[284] An insurance claim of a major fuel supplier related to cyber attack resulted in bunkering scam and led to the insurers taking the company to the court to claim the scam costs of US$ 18 million: see Steve Willams, 'Is the Maritime Industry Up to Speed on Cyber Security?' *Lloyd's List* (London, 19 May 2016).

[285] *Glencore International AG v MSC Mediterranean Shipping Co SA* [2017] EWCA Civ 365, [2017] 2 Lloyd's Rep 186. See S Rainey, 'Pinning Down Delivery: *Glencore v MSC* and the Use of PIN Codes to Effect Delivery' in Barış Soyer & Andrew Tettenborn (eds), *New Technologies, Artificial Intelligence and Shipping Law in the 21st Century* (London, Informa Law from Routledge 2019) 47; Michiel Spanjaart, 'Surrender, Release and Digital PIN Codes' in Girvin and Ulfbeck (n 135) ch 8.

Merck, (2) the malware affected leading Russian companies and other multinational companies, (3) the English and American cases referred to the court for 'the insurance meaning of war' as referring to and including only 'hostilities carried on by entities that constitute governments at least de facto in character' and (4) that 'the NotPetya attack is not sufficiently linked to a military action or objective as it was a non-military cyberattack against an accounting software provider' which meant that these actions were not similar to 'hostile or warlike action' and thus 'the exclusion was inapplicable to bar coverage for Merck's losses'.[286]

The second case was between Mondelez International and Zurich American Insurance.[287] The insured company claimed over US$100,000,000 after the NotPetya attack affected approximately 1700 of its servers and 24,000 laptops, rendering them permanently dysfunctional. The case was to be heard before a jury, but the dispute was settled before the hearing for an undisclosed amount. The insurer claimed that the damage was excluded because it was a 'hostile or warlike action' conducted by a 'government or sovereign power'. According to insurance experts, the policy was a property policy with some cyber events covered.[288] In a case relating to the cargo of cocoa with damage from condensation and mould, unsuccessfully attributed to the NotPetya cyber attack on Maersk,[289] HHJ Keyser KC stated that:

> the contention that the computer problems were not its fault because they were the result of a cyber attack represents the defence for which permission to amend was previously refused by HHJ Pelling KC and would anyway *beg the question why a cyber attack in June was still causing problems in November*.[290]

---

[286] *Merck & Co v Ace Am Inc Co* 475 NJ Super 420 (App Div 2023).

[287] *Mondelez International Inc v Zurich American Insurance Company* 2018 WL 4941760(Ill Cir Ct (Trial Pleading).

[288] Alexander Martin, 'Mondelez and Zurich Reach Settlement in NotPetya Cyberattack Insurance Suit' (The Record, 31 October 2022) <https://therecord.media/mondelez-and-zurich-reach-settlement-in-notpetya-cyberattack-insurance-suit> accessed 12 September 2024.

[289] *JB Cocoa SDN BHD v Maersk Line AS (Trading as Safmarine)* [2023] EWHC 2203 (Comm), [2024] 2 Lloyd's Rep 235. According to the defence witness statement [33], the problems caused by the NotPetya cyber attack were the underlying cause affecting Maersk's computer systems at the discharge port, which required the cargo to be manually released.

[290] Ibid, [109], emphasis added.

In November 2017, Clarksons[291] was a victim of a cyber security breach which resulted in a hacker stealing confidential data and threatening to publicise it, blackmailing the company. The shipbroker reported the incident to the police and obtained an interim injunction, which prohibited the unidentified defendant from communicating or disclosing to any third party 'certain information' without further details. Warby J banned the 'person or persons unknown' from publishing information unlawfully taken from the shipbroker's computer system,[292] and after that, Clarksons made the incident publicly known.

There are multiple possibilities for insurance coverage to be withdrawn. This can happen, for instance, in cases when the assured has not taken all measures possible and applicable to avoid a piracy attack.[293] Other options are when the acts of alleged piracy do not fall within the definition of piracy outlined in the insurance contract or the charterparty.

In the unlikely situation of insurance fraud, when piracy could only be claimed to have taken place to get the insurers' coverage, the court might decide that the insurers do not have to pay. There are other incidents where the assured claims that the incident fell within the meaning of piracy or war risk, but the court does not agree with their argument.[294]

In case of deviation from the original route, the vessel is placed in jeopardy of transit via areas with a higher risk of piracy attacks than initially declared and for which the vessel was insured.

---

[291] Davis Osler, 'Clarksons Wins High Court Judgment After "Blackmail attempt"' *Lloyd's List* (London, 7 March 2018).
[292] *Clarkson Plc v Person or Persons Unknown* [2018] EWHC 417 (QB)
[293] See Gard Rules 2024 and UK P&I Rules 2024.
[294] Todd (n 53) [1.043–1.052]. See further *Republic of Bolivia v Indemnity Mutual Marine Assurance Co Ltd* (n 8); *Athens Maritime Enterprises Corp v Hellenic Mutual War Risks Association (Bermuda) Ltd (The Andreas Lemos)* [1983] QB 647.

4.7 What about cyber risks?

Following the cyber underwriting risk letter to firms by the Bank of England in 2016[295] and the consequent Supervisory Statement 4/17,[296] cyber insurance underwriting risk was defined as risks deriving from underwriting insurance contracts exposed to cyber-related losses resulting from malicious acts[297] and non-malicious acts[298] involving both tangible and intangible assets.[299]

This created wider discussion among the underwriters, and with further letters from the Bank of England, it was established in 2019 that non-affirmative or 'silent' cyber loss should be avoided through greater clarity in the wording clauses, where it was allowed by local or regulatory requirements.[300] This led to a more strict separation of what was covered and to what extent regarding the cyber attacks and to the creation of multiple exclusion clauses. Additionally, in 2022, the notion of attacks sponsored by sovereign states was introduced, and it was suggested that

---

[295] The letter referred to the potential increase in the 'silent' losses with time due to the growth in insurance awareness and the more frequent occurrences of cyber attacks and the impact on marine coverages: see further Chris Moulder, 'Cyber Underwriting Risk – Letter to Firms' (Bank of England, 14 November 2016) <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/letter/2016/cyber-underwriting-risk.pdf> accessed 9 August 2024.

[296] The Prudential Regulatory Authority separated cyber insurance underwriting risk into affirmative cyber risk, where the insurance policies explicitly cover cyber risk, and non-affirmative or 'silent' cyber risk, where the policies do not explicitly include or exclude coverage for cyber risk: see further, Bank of England, Prudential Regulation Authority, 'Supervisory Statement SS4/17 – Cyber Insurance Underwriting Risk' (July 2017) <https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2017/ss417.pdf> accessed 9 August 2024.

[297] For example, cyber attack or infection of an IT system with malicious code.

[298] Such as loss of data, accidental acts or omissions.

[299] Bank of England, 'Cyber Insurance Underwriting Risk – Supervisory Statement 4/17' (5 July 2017) <https://www.bankofengland.co.uk/prudential-regulation/publication/2017/cyber-insurance-underwriting-risk-ss> accessed 9 August 2024.

[300] Caroline Dunn, 'Providing clarity for Lloyd's customers on coverage for cyber exposures' (Lloyd's Market Bulletin Y5258, 4 July 2019) <https://assets.lloyds.com/assets/y5258-providing-clarity-for-lloyd-s-customers-on-coverage-for-cyber-exposures/1/Y5258%20%20Providing%20clarity%20for%20Lloyd%E2%80%99s%20customers%20on%20coverage%20for%20cyber%20exposures.pdf> accessed 9 August 2024.

they be treated as a separate risk since they might occur outside the war involving physical force.[301] This finally led to the development of seven different types of exposures.[302]

> Type 1: excluding all state-backed cyber-attacks (war or non-war).
>
> Type 2: excluding state-backed cyber-attacks as part of war and all significant impairment losses for non-war.
>
> Type 3: Excluding state-backed cyber-attacks. Covering significant impairment non-war losses occurring outside the impairing state.
>
> Type 4: Cover similar as in Type 3 and additionally covering state backed cyber-attacks which are part of war outside the warring states.
>
> Type 5: Cover as in Type 2 or Type 3. Differentiation as for the 'significant impairment' threshold as a) state response by the use of force (irrespectively of declaration of war) and b) broad infrastructure impact.
>
> Type 6: Clauses granted dispensations by Lloyd's until the current dispensation expiration.
>
> Type 7: Non-compliant clauses or no clause.

[301] Tony Chaundhry, 'State backed cyber-attack exclusions' (Lloyd's Market Bulletin Y5381, 16 August 2022) <https://assets.lloyds.com/media/35926dc8-c885-497b-aed8-6d2f87c1415d/Y5381%20Market%20Bulletin%20-%20Cyber-attack%20exclusions.pdf> accessed 9 August 2024.

[302] Turk (n 145).

The LMA has adopted a different approach, enlisting multiple and different cyber attack insurance coverages and exclusions like war peril insurance[303] for exposure in marine hull, marine liability, and Marine war. [304]

Additionally, not specifically related to marine insurance but already created by the LMA, the Political Risk Cyber Endorsement[305] excludes loss, damage, liability or expense directly or indirectly from any computer system but covers using a computer system to launch, guide or fire any weapon or missile.[306] Clause 2 of the Endorsement covers the same risks caused by cyber acts or cyber Incidents, where both combined could describe the content of the cybersecurity breach.[307]

A different approach can be seen in the marine insurance clauses. Cyber attack is referred to only in a few instances in the marine insurance clauses. The first is the CL.365 Institute Chemical, Biological, Bio-Chemical, Electromagnetic Weapons and Cyber Attack Exclusion Clause, cl 1.2, which refers to 'the use or operation, as a means of inflicting harm, of any computer, computer system, computer software programme, computer virus or process or any other electronic

---

[303] Normally, the War and NCBR exposures belong to insurance classes subject to additional oversight and/or approval of Lloyd's, but when the exposure falls within cyber business, or when the cyber-attack is state-backed, it is excluded from the insurance and reinsurance policies for these exposures and covered separately as provided in Market Bulletin Y5381 and Market Bulletin Y5433 (n 150): see further, Rachel Turk, 'Performance Management-Supplemental Requirements and Guidance: 2024 Update' (Lloyd's Market Bulletin Y5434, 6 June 2024) <https://assets.lloyds.com/media/9370e179-5589-4971-b780-baadd5f725ff/Y5434.pdf> accessed 9 August 2024.

[304] The LMA's Model Cyber Clauses have risk codes B, T, and TS for Marine Hull, G, GC for Marine Liability, Q, W, WB and WX for Marine War, with affirmation and limited exclusion clauses and Exclusion clauses, without any Affiliation and Exclusion and Limited Writeback clauses. See further LMA, 'Published LM Model Cyber Clauses (all clauses' (5 March 2024) <https://www.lmalloyds.com/lma/Underwriting/Wordings/LMA/lma_wordings.aspx> accessed 25 October 2024.

[305] Political Risk Cyber Endorsement (for use with Political Risks/Political Violence Package Business), LMA54278 (15 June 2021).

[306] LMA5427B cl 1.

[307] LMA5427B cl 2.

system.' Further, as indicated for the whole CL.365, 'it shall be paramount and shall override anything contained in this insurance inconsistent therewith'.

The second reference to cyber attacks is in the Joint Specie Clauses JS.001 Cyber Attack Exclusion Clause and Write-Back. In this case, the general exclusion of cl 1.1 has similar wording as the above CL.365 cl 1.2.[308] Nevertheless, cls 1.2 and 1.3 provide cover for losses normally excluded from the cover following the cl 1.1 exclusion. Thus, cyber attack 'is covered as a risk 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'. The insurer cannot trigger clause 1.1 to avoid the coverage provided under the specific policy as this only applies to losses 'arising from the use of any computer software programme or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile'.

Moreover, in cl 1.3, the physical loss of or physical damage to the assured's property caused by a targeted cyber attack is also coverable, but the burden of proof is on the assured. The meaning of targeted cyber attack is 'where the motive is to inflict harm solely on (or upon) the insured or the insured's property'. Therefore, a cyber attack, which is either associated with the use of weapons or missiles or explicitly targeting the assured, will be covered under JS.001, provided the assured has a standing coverage for the incident in the former scenario and can prove the cover in case of the latter scenario.

Another reference to cyber attacks is the Institute Cyber Exclusion Clause,[309] which describes the cause of loss, damage, liability or expense as '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' (cl 1.1) and would be covered in policies covering

[308] CL365 was introduced on 1 November 2002 but there is no provision for malicious code as in the JC001 issued on 10 January 2018.
[309] CL380/10.11.2003.

war risks or terrorism (cl 1.2). This provision appears closer than the others to the definition of a cybersecurity breach as this action intends to harm computer systems. However, it does not clarify, as does JS001, the specific targeting of the assured. This could be interpreted as only applicable in significant incidents or where there are cybersecurity breaches or cyber-attacks caused by war or terrorism without specific association of the victim's identity with the performance of the action. This wording can also be perceived as silent cyber risk coverage with no exclusions from the coverage as long as war (and associated actions) or terrorism is determined to be the damaging cause.

A recent addition is the JE007 Joint Excess Loss Cyber Losses Clause (JX2020-007). This clause incorporates in cl 4 the definition of the Information Technology Device given in cl 17.4 of the CL432 Joint Excess Loss Committee Excess Loss Clauses as follows:

> any computer system, hardware, software, programme, code, data, process, virus, information repository, microchip, integrated circuit or similar device in or connected with computer equipment or noncomputer equipment, whether the property of a direct insured or not.

The JE007[310] excludes from the contract's cover the loss, damage and liability or expense from the use or operation of an Information Technology Device (ITD) as a means for inflicting harm (cl 1). However, this exclusion is not enforced when the losses are caused by the use of an ITD for the launching or the guidance of the firing mechanism of a weapon or missile (cl 2). Furthermore, even when the ITD was not used to inflict harm, the physical peril was a significant cause of loss, and the cover will again be provided.

The physical peril as defined in the Information Technology Hazards Clause within JELC CL432 is:[311]

---

[310] In the Joint Committee Circular it was noted that the JX2020-007 was created to meet the cyber exposures to both malicious and non-malicious cyber risks and in order to avoid the silent cyber exposure: see JX2021-016.

[311] Cl 17.3.

> theft of equipment, collision, sinking, grounding or stranding of carrying vessel, overturning or derailment of land conveyance, jettison or washing overboard, fire, lightning, explosion, aircraft or vehicle impact, falling objects […].

Arguably, the Institute Malicious Damage Clause[312] could be applied to cybersecurity incidents because the actors are doing so with intent to damage or sabotage, although the act of vandalism could also be attributable to cyber perpetrators. A similar approach could be adopted in the Institute Theft, Pilferage and Non-Delivery Clause.[313] Thus, a cyber incident resulting in theft or non-delivery of a package, such as a container, could be covered. In the case of the modified application of the Institute War Cancellation Clause,[314] the insurer or the assured could cancel the coverage for cybersecurity for the time following the attachment of the insurance before the cancellation is effective. This could create some level of certainty in the insurance market, given the fact that in the event of very high expenditure caused by a cyber incident, the insurer could cancel the cover in order to renegotiate a higher premium or to avoid possible exposure to new risks if the assured is likely to face another similar situation. The assured will have the coverage he hoped for and paid the premium for.

Clause 6.2 of the Institute Cargo Clauses (A)[315] exempts piracy from the exclusion, thus reaffirming its coverage under cl 1. The same wording in cl 1.2 refers to cl 1.1, which omits piracy without specific exclusion in cls 3 and 4. This means the Institute War Clause (Cargo) is not applicable in cases of piracy and terrorism because it cannot fall under war and any hostile act by or against a belligerent power.[316] There is a slightly different picture in the Institute War and Strikes Clauses,[317]

---

[312] CL266/1.8.1982.
[313] CL272/1.12.1982.
[314] CL271/1.12.1982.
[315] CL252/1.1.1982. See further the similar exemption in CL.270 Institute War, Atomic and Nuclear Exclusion (Cargo Reinsurance); CL280B Institute Time Clauses Hulls Restricted Perils, CL.280/ Institute Time Clauses Hulls where barratry and piracy are excluded from the cl.24 (war exclusion). Thus, both risks are covered.
[316] CL 255/1.1.1982. See further CL269 Institute Marine Policy General Provisions (Cargo), CL278/5.9.1983 Institute War Clauses (Commodity Trades) (Agreed with The Federation of Commodity Associations), ibid.
[317] CL 262/ 1.8.1982. Surprisingly, piracy might have been omitted considering that the pirates would not have boarded a mechanically self-propelled vessel with cargo stored afloat.

where the war, except for the war between specifically listed countries,[318] and terrorism are covered explicitly (cl 1.1 and 1.5), and piracy is not coverable.

Cybersecurity is unique because it can affect installations ashore and offshore. Shipping companies, ports, and vessels can be affected, and two or more insurance coverages could intersect. Thus, the cybersecurity coverage of a company ashore or facility, such as a port, might overlap with the cybersecurity coverage of the vessel or the fleet of vessels in case the cybersecurity breach or attack appears in one of the stakeholder's establishments and afterwards spreads or affects, directly or indirectly. There could be a direct incident involving data leakage, blocking access to the data, or the inability to function fully. There could be an indirect incident following infection by malware or other malicious software or program email received by another stakeholder. It is questionable whether the impact of a combined cybersecurity breach or attack involving multiple stakeholders is calculatable and, what is more, remunerable and to what extent by each stakeholder. In this case, one or more stakeholders could be substituted by their insurers or reinsurers, and the loss could be somehow claimed from the initial weak part of the chain and how that would be proved or what defences that defendant would be given, if any.

This question is more authentic if one considers that interruption in business has tangible costs. This covers both loss of profit and calculatable loss of income compared to the relevant income earned during the same period in the previous fiscal year or expected to be earned during the current month or a shorter period, taking into account the occurred disruption was not present. Other losses, such as harm to reputation, loss of future clients or collaborators, or even the loss of a market share due to bad publicity, are much more difficult to prove and calculate in a market as volatile as shipping.

Apart from the insurable third-party liability and hull and machinery damages endangered by a possible cyber-security breach situation, there are still vaguely described and unprecedented

[318] The countries are the US, France, the Union of Soviet Socialist Republics, and the People's Republic of China: see cl 3.9.

situations of malfunctioning of the navigational systems and data exchange procedure with the control points of the unmanned vessels ashore or in a remote area, close to the vessel.

Cyber-security breaches are new since autonomous vessels have not yet been deployed, and the probability of such a situation cannot be tested. Nevertheless, cyber-security professionals have expressed concern about the new technology's vulnerability and liability in actual situations causing damages.

Cyber security is usually not enlisted as a war risk and is explicitly provided for and covered by the insurer in a separate insurance contract. The P&I Clubs usually provide the primary insurance, and insurers specialise in cybersecurity coverage. Members of the IGP&I all offer relevant products that can be easily found on their websites. Insurers cover the shipping industry as a whole for cases of cyber-attacks and data breaches.[319]

Organisations such as the International Association of Classification Societies (IACS)[320] have examined safety systems aboard vessels[321] for some time and are considering introducing a cyber security requirement.[322] As most of the world's fleet is covered by classification,[323] it is possible

---

[319] For instance, AXA provides Cyber Insurance for the maritime industry located in the US and Canada <https://axaxl.com/insurance/products/cyber-insurance> accessed 9 May 2024.

[320] Generally, regarding classification societies, see Girvin (n 47) para 1.21; Yu-Chang Su, 'Assessment of Criteria of Ship Classification Societies' (2023) 50 Maritime Policy & Management 980.

[321] IACS Council Focuses on Next Generation Safety Systems, ABS, <https://ww2.eagle.org/en/news/press-room/IACS-Council-Focuses-On-Next-Generation-Safety-Systems.html> accessed 9 May 2024.

[322] Some of the recent IACS Unified Requirements rules already implemented in relation to cybersecurity aboard vessels are: UR E22 Computer based systems, UR E26 REV1 CR Cyber resilience of ships and UR E27 REV1 CLN Cyber resilience of on-board systems and equipment. The May 2024 version of rule URC6 Requirements for Lashing Software is expected to be implemented in July 2025 for all newbuilds: see IACS Unified Requirements UR E <https://iacs.org.uk/resolutions/unified-requirements/ur-e>; IACS Unified Requirements UR Implementation status 2024 <https://iacs.s3.af-south-1.amazonaws.com/wp-content/uploads/2024/10/18141253/UR-Implementation-status-2024.xlsx> accessed 18 October 2024; Marcus Hand, 'IACS Moving Towards Cyber Security Requirement' *Seatrade Maritime News* (Colchester, 17 December 2019) <https://www.seatrade-maritime.com/technology/iacs-moving-towards-cyber-security-requirement>, accessed 9 May 2024.

[323] 'Propelling Classification Through Continued Cooperation' (IACS) <https://iacs.org.uk/news/propelling-classification-through-continued-cooperation> accessed 9 May 2024.

to estimate the impact that classification may have on the cyber security resilience of the vessel, both concerning the seaworthiness[324] of the vessel and its insurability, as seaworthiness determines insurance.

During the COVID-19 pandemic,[325] P&I Clubs faced challenges because of claims arising from the pandemic and malicious cyber attacks.[326] Thus, in the 2022 renewal for the 2022/2023 policy year, the International Group of P&I Clubs (IGP&I) reinsured[327] malicious cyber risks together with COVID-19 and pandemic risks with free and unlimited cover for claims up to US$450 million excess of US$100 million, covering almost all Group Clubs' certified risks. In addition, a provision of excess of US$550 million up to US$2,15 billion of annual aggregated cover for all three risks and the excess of that was decided to pool between Group Clubs the non-reinsured risks so that there would be no change in the Members's cover.

The 2024/25 Pool and the annual IGP&I Group General Excess of Loss (GXL) Reinsurance Contract separately cover malicious cyber risks by the excess layers for the 2024/25 policy year for losses with a value greater than US$750 million directly arising from the risk. In this way, there is a separate aggregated cover for claims above US$750 million up to US$2.1 billion. The annual aggregated cover is up to US$1.35 million for malicious cyber risks. Losses below the threshold of

---

[324] An interim solution proposed by Schinas and Metzger suggests seven points to be examined in order to characterise a ship as a seaworthy, including (1) the Safety Management Manual for the most recent cyber-risks, (2) training of the crew and physical protection for the hardware and software from unathorised access, (3) cyber-security protection and updating or upgrading in both software and monitoring systems, (4) separation of the data to critical and non-critical for the operation of the ship: see Orestis Schinas and Daniel Metzger, 'Cyber-seaworthiness: A Critical Review of the Literature' (2023) 151 Marine Policy 105592-1.

[325] Cf 'Group Activities: Review of Claim Trends' (IGP&I, 22 September 2021), <https://www.igpandi.org/article/group-activities-review-claims-trends/> accessed 9 May 2024.

[326] The issue of malicious cyber was raised during the IGP&I Reinsurance Market Event 2022: see <https://www.youtube.com/watch?v=_cK6g4t2q-4> accessed 9 May 2024.

[327] It should be noted that malicious cyber, COVID-19 and pandemic were excluded from the Main General Excess of Loss coverage. The cover of up to US$450 million with excess of US$100 million was introduced for all these risks. The International Group Pooling and GXL Reinsurance contract structure for 2024 has now been finalised: see further <https://www.igpandi.org/reinsurance/> accessed 18 October 2024.

US$750 million are covered by reinsurance on a free and unlimited basis, irrespective of whether the loss is caused by one of the defined risks.[328]

There is more than one situation or behaviour on behalf of the assured, which may lead the insurer to decline coverage. Since most contracts and disputes arising from such contracts are usually resolved between the legal departments of the interested parties, obtaining publicly available information regarding the reasons for loss of coverage is challenging. Nevertheless, the Cyber Security Clause is optional, and ocean carriers may opt to exclude their liability for cyber security breaches to their electronic systems.[329] When using the web portals of carriers, which include these exclusions as part of their terms and conditions of carriage, shippers waive their right to claim any compensation in case of a data breach.[330] Those carriers choosing to insure themselves against cyber risks,[331] be it cyber security breaches or cyber-attacks, face a double challenge. Insurers are unwilling to offer such coverage because there is no efficient database to estimate the risk height and its probability of occurrence. This leads, in turn, to undercover or much higher premiums because of the perceived exposure of the insurer or the reinsurer in the case of a cyber incident.

However, in cases where the assured is not responding to the behaviour normally expected from his or her category of business and data sensitivity to breach incident and is not taking all the measures expected to be taken by an independent observer of the industry, the insurer might have a case against any claims raised.

5 Future projections

The insurance market does not stand still. This can be illustrated by the decision to modify the definition of cyber attack in CL365 in 2002 to JS001 in 2018 to include malicious code and to

---

[328] Ibid.
[329] Victor Chacón, 'Web Portals and Data Sharing by Ocean Carriers' in Girvin and Ulfbeck (n 135) 231.
[330] Ibid.
[331] Ibid.

provide coverage where the previous provision did not. It can be envisaged, therefore, that the insurance market will likely self-regulate if new means of cyber security breaches and attacks arise.

One possible solution for expanding the coverage of cyber security breaches could be to include them in a wider definition of cyber incidents. This could be done by creating three stages of cyber events: cyber incidents, security breaches, and cyber-attacks. A cyber incident could be defined as an incident affecting the cyber security of the insured when there was no breach or attack, but some actions were taken by the perpetrators, for example, to expose the vulnerabilities of the security system. The next level would be the cyber security breach, which would be either the next step after the cyber incident or an irrelevant event that would mean the security was violated. Lastly, the cyber attack would be either the logical consequence following the previous cyber incident and cyber security breach or an independent event occurring without any previous cyber event.

For the avoidance of coverage of irresponsible and non-proactive insureds, exclusions could be created for situations when : (1) there was no cyber security protection software in place, (2) the protection program was not updated, (3) there was no secondary storage facility or a cloud with secure access to it,[332] (4) there were no employed specialised cyber security personnel, (5) there were no programmed and repetitive training sessions for the personnel with access to sensitive data, (6) there was no training and simulation after any cyber security incident occurrence.

Another category could be created for the insurance coverage for ransom payment and other expenses associated with (1) business interruption, (2) delays and cancellations, and (3) fame and reputation harm caused by an incident. These covers would, of course, be provided based on the compliance of the insured with the proactive cyber policy, updated cyber protection and trained

[332] Depending on the size of the company and the sensitivity of the data transferred and stored inside and outside of the company premises

and adequately informed personnel. This would also assume that precautions were taken, the insured was updated on cybersecurity, and its personnel were adequately trained and informed.

There is also a need for the enlargement of insurance coverage and the inclusion in the existing limitation regimes of new stakeholders who will provide cybersecurity coverage and ensure the interconnectivity and automation of the onshore and offshore parts of the shipping industry. On the other hand, the insurers and the states must insist on the semi-public obligatory publication of the incidents by the affected parties and the stricter security provisions to ensure that all the possible measures to prevent a potential attack have been taken. The semi-public character of the data regarding cybersecurity incidents will protect the reputation and the economic value of the companies exposed to those incidents since the data will be only available to accredited stakeholders and probably provided on a completely anonymized basis. Another much-needed factor will be collaboration between ports and the sharing of good practices. More technologically advanced ports can help the technologically advancing and developing ports avoid the same exposure and safeguard themselves. From this perspective, the gradual development of the ports and the few pioneering ports' experiences might benefit cybersecurity resilience and ensure that the same breaching and attacking tactics and techniques will not work more than once. Cases where pirates were tricked into believing they would receive the ransom but did not receive it worked only once. This could also be applied in the case of cybersecurity breaches and attacks which were successful once but, once reported and studied, are no longer a threat.

One applicable solution is to create a mechanism spread over three levels in order to secure the coverability of the cyber risks and ensure the economic viability of the insurers and reinsurers covering such risks. Initially, assureds will have to agree to anonymously provide data after an incident to their insurers and reinsurers, and the same data will then be shared with local authorities of the port or in which EEZ territorial water the incident took place. This will build an adequate database of available information with the type of attack and the particulars, which will be analyzed by the affiliated cyber security providers with the insurers to provide a better protective net for the future. Following the incident, the insurers and reinsurers will feed an

internal generative AI systems[333] all the available data and model new upgraded insurance coverage, providing cover for the specific area where the incident occurred. This additional coverage will then be offered to the rest of the assureds, together with precautionary measures to be taken before and during the transition of the dangerous area. The offer will be voluntary, meaning that if the assureds choose not to upgrade their coverage in case of any incident in the same area and if its particulars are the same as the previously reported and coverable, the insurers will be released from their liability. From some point, it will work as the updated war risks coverages in order to provide preventive protection for the assureds cannot deviate from the dangerous location and will have to transit through it. The next level would be the creation of regular reports with recipients different stakeholders affecting the safety of the affected sea section, like the port authorities (if the incident happened while the vessel was berthed or anchored), local patrolling and coastguard and navy (if the incident took place outside of the port's jurisdiction) and wider officials (for cases when the cyber situation was created in high seas or regional seas where more than one countries exercise their sovereign like the Mediterranean Sea, Malacca Strait etc). These reports would refer to specific data related to cyber attacks like for instance unique identification codes or estimated geolocation of the source of the signal used for the breach or the attack. In case the authorities do not take into account the information provided to them by the insurers and do not eliminate the danger caused to vessels, those ports[334] and coastal and high sea areas will be listed as non cyber secure and the transiting or anchoring and berthing in them will be done, depending from the probability of the occurrence of the risk, either with separate insurance premium or non coverable at all. This will eventually motivate the non complying parties to provide a safe of cyber exposures environment, if they of course desire to retain their revenues from the shipping.

---

[333] An assumption that some marine claims could be automatically reviewed has already been proposed: see Julian Clark and David Owens, 'The Role AI and Machine Learning Will Play in Maritime and Trade Law' in Barış Soyer and Andrew Tettenborn (eds), *Disruptive Technologies, Climate Change and Shipping* (Informa Law from Routledge 2024) 99.

[334] Ntandokazi Shazi, 'An Evaluation of the Safe Port Obligation in the Light of Smart and Autonomous Ships', CML Working Paper Series, 24/02, May 2024 <https://law.nus.edu.sg/cml/publications/> accessed 30 August 2024.

Also, voluntary disclosure of incidents and breaches and the costs involved in recovery from them, if any, would help to have adequate monitoring of annual appearances or periodic occurrences of certain threats. Furthermore, it would help in a more precise calculation of the certainty or probability of future repetitive similar events, the number of assureds exposed to each category of threats, and the approximate number of potential receivers of each insurance coverage. This could help create certainty in this evolving and constantly changing risk market so that insurers could accustom the premiums to actual exposure, occurrence probability, and estimated recovery costs. Assureds providing data for the database of cyber events could be motivated by discounts or decrease in their premiums as a reward system for their cooperation. By following the instructions and guidelines generated from the analysis of past cyber events, they could be eligible for a higher level of cyber risk coverage, such as from cyber incident to cyber breach and then to cyber attack.

When autonomous vessels become more widely used, it will need to be seen whether a new window of opportunity could be created for cybercriminals to try their luck in finding security vulnerabilities and exploiting them.

The disruption of business as usual and public exposure have so far been the primary outcomes of cybersecurity incidents. However, they are usually not included in marine risks and are not covered.

As the technology used aboard vessels advances, the likelihood of some cybersecurity compromise aboard the vessel or its immediate interconnection with facilities ashore will increase.[335] The existing structures for such incidents would likely cover these dangers when cybersecurity is not involved. Nevertheless, the insured will likely demand a strict cybersecurity

[335] The requirement of the usage of a single, centralised digital platform for the collection and exchange of information with ships when they call the ports of the IMO Member States called 'Maritime Single Window' is mandatory since 1 January 2024 but currently is functioning only in Antigua and Barbuda and Port of Lobito in Angola: see IMO Maritime Single Window – Advancing Digitalization in Shipping <https://www.imo.org/en/MediaCentre/PressBriefings/pages/Maritime-Single-Window-advancing digitalization-in-shipping.aspx; Shazi, ibid, 11 (n 62).

protection policy. This policy is likely to include constant upgrading of antivirus systems and other software programs, the use of the approved specific software, staff instruction from cybersecurity specialists, drills with the use of actual previous attack simulations, and an immediate annotation system for the insurer and reinsurer to be able to handle the results as soon as possible and reduce the costs related to the reputation and trust of the assured.

A hypothetical scenario of cyber-hijacking of the vessel could be even more alarming. Unfortunately, it cannot be excluded from reality with the commercial use of unmanned vessels. There could be a situation where an unmanned vessel is hijacked via signal deviation or via infected messages exchanged between the vessel and port or offices ashore and the vessel. In this hypothetical scenario, a virus could enter via an infected email or an external hardware device or software and stay unnoticed until it is transmitted via email or other internal communication with the vessel. Once it reaches the vessel, it could alter unnoticed the vessel's destination, rerouting it to the virus senders' location so the vessel can be either boarded and robbed or used in other illegal activities by the cyber–hijackers. If one supposes that a vessel under cyber–attack is transporting inflammable cargo, such as LNG or crude oil and LPG, the vessel could threaten the national security of coastal states along the vessel's planned route or route after deviation. In this case, the premium paid to the insurer might increase because any threat of attack with such dangerous cargo to any shore facility or other vessels would mean high remuneration costs, especially without special limitation procedures for noxious and hazardous substances.[336]

The hypothetical scenario could also be characterised as an act of piracy. In this case, pirates would not physically be in control of the vessel but would nevertheless prevent the lawful shipowner from exercising its right to use and control their vessel. For the shipowner to regain their property and the cargo loaded aboard the vessel, it would be called upon to negotiate and pay ransom to the cyber–pirates. An example of the impact on the general shipping chain is an

[336] Cf the HNS Convention and the discussion in De la Rue (n 93) ch 7.

alteration of the cargo's destination.[337] When thieves manipulate the system and change the place of delivery without being noticed, such changes only become evident when the cargo is not delivered or lost.[338]

Technological progress with unmanned vessels could also create a new normal operational style for shipping companies and ports. Shipping companies would need to have special teams with navigational as well as technological and programming skills to track cyber-attacks and provide a defence wall against further actions of the attackers once the attempt or the ongoing attack is detected.[339] What is more, in order to maintain insurance coverage when passing or entering areas with a high risk of potential cyber-security threats, the shipowner would be required by the insurers and/or carriers to have a specialised cyber-security response team,[340] similar to armed guards aboard vessels in high piracy risks areas. On the other hand, where practically possible, ports could be transferred away from living areas to eliminate the threat to civilians if cyber-hijackers use an unmanned vessel as a weapon against land facilities. In parallel to a terrorist attack, a cyber-terrorist could also use the vessel as floating weapons targeting land facilities, as platforms for remote weapons launching to hit land targets, and as floating bombs against other vessels which could be at berth inside the port.[341] Also, the ports could invest more and upgrade their facilities for greater automation and integration of generative AI to eliminate human intervention and the exposure of the data to cyber breaches or cyber-attacks. Ports should also provide specialised teams to cover cyber-security threat detection, control and elimination. Consequently, the presence or absence and the expertise of the specialised teams guaranteeing

---

[337] David Osler, 'Experts highlight AIS Vulnerability to Hacker Attack' *Lloyd's List* (London, 16 October 2013).

[338] This was the case of the cyber breach in the port of Antwerp from 2011 to 2013 when a criminal organisation accessed the IT system of the port and changed the delivery address of the containers containing illicit substances. This was done in total ignorance from the port and the customs authorities. See further Chacon (n 317) 229-230; David Osler, 'Experts Highlight AIS vulnerability to hacker attack' *Lloyd's List* (London, 16 October 2013); Steve Williams, 'Is the Maritime Industry up to Speed on Cyber Security?' *Lloyd's List* (London, 19 May 2016).

[339] 'Gartner Identifies the Top Cybersecurity Trends for 2024' (Gartner, 22 February 2024) <https://www.gartner.com/en/newsroom/press-releases/2024-02-22-gartner-identifies-top-cybersecurity-trends-for-2024> accessed 30 August 2024.

[340] Ibid.

[341] Bowley (n 32) 126–130.

the safety of the vessel and the cargo on the high seas and in the port would create a similar listing to piracy high-risk areas. This would probably lead to the creation of specialised insurance products offered to shipowners and ports.

A few ports are progressively becoming more and more automated and reliant on interconnectivity.[342] This facilitates quicker data transfer between stakeholders like ports, shipowning companies, charterers, and authorities designated to collect data regarding fuel consumption, emissions, and credentials for entrance and exit from port. However, this also creates more potential security gaps that cybercriminals can exploit.[343] Research conducted by DNV in 2023[344] showed that, despite anticipating a major disruption caused by a cyber attack,[345] the shipping industry has not invested equally in operational technology (OT)[346] as it has done with IT.[347]

---

[342] Currently, the largest automated container terminal is the port in Shanghai, China. The potential malicious hacking of control signals in wireless connections is restrained with encryption. Apart from the Shanghai Port and the Singapore Tuas Terminal, other future projects worldwide include the Chancay Port Terminal. It is planned to be controlled remotely, and its equipment will be mostly unmanned, see further The World's Largest Automated Container Port' (Huawei) <https://e.huawei.com/en/case-studies/global/2018/201807050920> accessed 10 May 2024; COSCO, 'The Project', <https://coscochancay.pe/en/the-project/ >accessed 10 May 2024;

[343] Soyer (n 129) 197.

[344] 'Maritime Cyber Priority 2023' (DNV, 2023) <http://dnv.com/energycyberpriority> accessed 30 August 2024.

[345] 90% of the 801 professionals participating in the research identified the disruption of ship and fleet operations, followed by theft of property or cargo (79%) and equal percentage believed this could result in damage to port or cargo handling infrastructure and result in a strategic waterway closure (76%), ibid, 3, 8-9.

[346] According to the presentation of the IAPH Cybersecurity Guidelines for Ports and Port Facility to the Maritime Safety Committee the cyber attacks and attacks against Operational Technology (OT) from February until May in 2020 had increased four times whereas the total increase of those attacks on the OT was 900% from 2017 until 2020; see further MSC 104/7/1 (2 July 2021), 2, see also MSC 103/9/2 and the links included there for the relevant data 'Maritime Businesses See Fourfold Increase in Cyber Attacks Since February: Astaara' (Captive International, 23 June 2020) <https://www.captiveinternational.com/news/maritime-businesses-see-fourfold-increase-in-cyber-attacks-since-february-astaara-3568> accessed 19 August 2024, (Professional Mariner) <https://www.professionalmariner.com/naval-dome-maritime-cyberattacks-up-900-percent-in-three-years/> which could not be accessed on 19 August 2024.

[347] The attack in 2022 on the oil terminals of the Port of Antwerp affecting the unloading of barges and the 2023 attack on the industrial control systems of the Fincantieri Marine Group resulted in inoperability of the manufacturing equipment used in shipbuilding for clients like US government were only two incidents which showcased the seize of the problem, see further 'Major European Ports hit by Cyberattack' (Port Technology

Where the cyber security incident is attributed to terrorism, P&I Clubs and general insurers will not cover the relevant losses suffered by maritime stakeholders. In such a case, the state may step in to cover or provide guarantees to the insurer to cover extraordinary risks. Something similar has already happened with the Unity facility offering US$50 million of hull and P&I war risk cover to support shipping from ports in the Black Sea. Unity is underwritten by Lloyd's of London and backed by letters of credit from Ukraine's state-owned bank, Ukrgasbank, and confirmed by German commercial bank DZ Bank.[348] In order to provide such coverage, the state will likely require the assured to disclose all the details of the incident and provide access to its servers and any hardware and software exposed to or affected by the breach or attack.[349] Also, there is a possibility that only the situations when cyber incidents threaten the maritime transportation system or create potential threats to national, regional, and international security will receive that kind of backup and attention from the states and the insurance markets. Not all breaches and attacks will be eventually covered. Taking into account the potential cost of business disruption,[350] loss of data, negative exposure to clients and partners, and possible punitive consequences from administrations and organisations exposed to the same breach or attack, it is highly probable that individuals and companies will eventually outsource some of these functions to specialised cybersecurity companies who will safeguard the information transported and protect the reputation and budgets of their clients. It remains to be seen what direction this will take. However, different perpetrators will continue their illegal activities as long as they are profitable.

Team, 3 February 2022) <https://www.porttechnology.org/news/major-european-ports-hit-by-cyberattack/ > accessed 30 August 2024; 'US Navy Contractor Fincantieri Marine Group Hit by Cyber-Attack' (Infosecurity Magazine, 24 April 2023) <https://www.infosecurity-magazine.com/news/us-navy-contractor-cyberattack/ > accessed 30 August 2024.

[348] Ben Dyson, 'Big Task of Restoring War Insurance in Ukraine Starting with Small Steps' (S&P Global, 29 February 2024) <https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/big-task-of-restoring-war-insurance-in-ukraine-starting-with-small-steps-80642056> accessed 30 August 2024.

[349] Cf the Draft UN Convention Against Cybercrime, arts 26-30.

[350] Barış Soyer, 'Cyber Risks Insurance for Shipowners and Operators – Time for a Far-Reaching Risk Assessment' in Lia Athanassiou (ed), *10th International Conference of Maritime Law – Protecting Maritime Operators in a Changing Regulatory and Technological Environment: Reports* (Nomiki Bibliothiki 2023) 205-206.

The ransoms paid following breaches and attacks tend to support this tendency, and the future estimates are comforting.[351]

Lastly, the fact that the United Nations has recently adopted the UN Convention against Cybercrime[352] and opened it for signature signifies a new era of combating cybercrime worldwide. It underlines the dangers cyber security breaches and attacks can create for everyone.

6 Conclusions

It can be said with some certainty that there will be new kinds of insurance coverage products introduced by P&I Clubs and H&M insurers in combination with the shore-based insurers, who will cover the risks of ports, interconnected organisations and multiple clients, suppliers and contractors within the maritime sector as a whole. An event occurring in one area might create a domino effect, causing multiple implications and unforeseen costs. AI and simulation models will likely become more widely accepted, even at the pre-contractual stage of negotiations for insurance cover, so that both sides know what is being insured, from what dangers and at what cost, and act accordingly. They could be given a choice between the highest possible premium for the most inclusive coverage and the lowest premium with the outcomes for the business interruption and possible claims, which might not be limited or partially only limited.

---

[351] For the next two years, cyber insecurity will be placed fourth in the global risks (third by some governments and the private sector) and will remain in the top ten for the next ten years: see further 'Global Risks Report 2024' (World Economic Forum, 10 January 2024) <https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf> 6-7; 15, accessed 30 August 2024,. Furthermore, damages from cybercrime from US$3 trillion in 2015 doubled by 2021 and are expected to reach US$10,5 trillion by 2025. See further, 'Why we Need Global Rules to Crack Down on Cybercrime' (World Economic Forum, 2 January 2023) <https://www.weforum.org/agenda/2023/01/global-rules-crack-down-cybercrime/> accessed 30 August 2024.

[352] United Nations, General Assembly, A/AC.291/L.16 'Draft Resolution for Consideration by the General Assembly' (Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 7 August 2024) <https://documents.un.org/doc/undoc/gen/v24/055/48/pdf/v2405548.pdf?token=4NRdYd0aajjGn2K7SM&fe=true> accessed 9 August 2024.

While the maritime industry enters the new era of higher automation, it is also possible that more participants in the industry, such as cybersecurity specialised companies, producers of software and hardware, producers of measurement appliances, multiple detectors and interconnectivity instruments for vessels, will need to cover their liability from any cybersecurity incident. This might be addressed in the regulatory review of the liability regime for cybersecurity incidents arising from autonomous vessels.

This paper suggests that cyber coverage can be rearranged as cyber-piracy (involving automation or cyber breach and/or followed by cyber attack), cyber war (which already exists in some insurance coverage) and cyber-terrorism (also possible to be distinguished in some legal approaches and expected to be followed by insurance coverages). This paper also advocates for creating a new insurance scheme where cyber incidents, cyber security breaches, and cyber attacks will all be covered, and disruption of the shipping chain in general will be applied. It further suggests that for the creation of more data available for the insurance policy formulation and the calculation of the premiums, there should be some effort to make the notification of the cyber events to the insurers quasi-obligatory.

In addition, it would be advisable to reapproach the severity of the cyber exposure of the assureds, beginning with a cyber incident when there was an attempt to intervene in the cyber system of the company or individual but was blocked without any harm. Next would be the level of a cyber breach, when the cyber security was compromised, and there was an intrusion, without any tangible damage and any leakage or stealing of data, but with a risk level raised because of the intrusion. In this scenario, the above-described model could be initiated. Finally, a cyber attack would be the highest level of exposure for the assured. Because of the high cost of the cyber attack for the assured, this cyber event would only be covered if the assured took all the measures indicated by the insurer. Where there was a previous occurrence in another event, a relevant issue would be whether it was prudent for the assured to take the increased risk coverage and avoid the actions that could lead to possible cyber vulnerability.

It is not clear if the cases where there is a state or organisation behind any of the above levels of cyber intrusion should be treated only as cyber war and cyber terrorism or if they also could be treated as cyber espionage, meaning they would most likely remain on the level of cyber security breaches and continue unnoticed for a more extended period. This could lead to much more significant exposure of the victim since there is no certainty as to what data and from which moment and onwards could be stolen or, modified or affected in any other way, as each time would be applicable for the specific data type.

An example of insurance coverage for cyber security breaches and associated electronic risks can be found in the essDOC liability cover provided for electronic bills of lading.[353] A similar system of insurance with increasing amounts corresponding to different levels of cyber exposure could be adopted, offering more certainty to both sides. The assureds' marine ventures will be covered, and insurers will not be called upon to pay for the indifference and recklessness of any of the assureds, protecting other careful and proactive assureds.

It remains to be seen when and if the marine insurance market will use its potential as dedicated professionals with years of risk coverage experience to cover the new emerging cyber-related incidents. This could allow shipping to continue its business as usual and become once again a leading paradigm in the insurance world.

[353] In this case, the amount of insurance is US$20 million per electronic bill of lading. See further Girvin and Ong (n 173) 201-202.