Journal of Maritime Law & Commerce, Vol. 51, No. 2, April, 2020

Autonomous Ships And The Proximate Cause Conundrum - A Maritime And Insurance Law Tango

Mayank Suri*

I
INTRODUCTION

> *Viewing cyber security as simply an information technology (IT) issue is similar to considering the safe operation of a vessel as simply a main engine issue.*[1]

The above statement gives much needed context to the issue that is going to be addressed in this paper. Due to the fast and rapid integration of technology in all aspects of human life and business, it would be unreasonable to assume that cyber risk is an isolated issue. Truly, even ship owners have realised the extent to which cyber risks can affect their liability when carrying out business.[2] Viewed holistically, the supply chain facilitated by shipping is already cyber integrated at various stages; whether it be in the use of on-board navigational aids or in the transactional aspect (emails, document exchange, electronic transfer of funds, etc.) of carriage of goods. To this extent, it is worth acknowledging the existence of cyber risks that can cause damage or loss to the ship owner at various stages of the business. This cyber exposure to the shipping industry has recently even been acknowledged by the government

---

*Mayank Suri is a Lecturer at Jindal Global Law School. He has been a practicing lawyer in the shipping industry and holds a Master of Laws degree in International Maritime Law from Swansea University, United Kingdom.

[1]Editor, Cyber Security, Gard, (2017), http://www.gard.no/web/topics/article/21025160/cyber- security.

[2]E.g. Mediterranean Shipping Company SA v. Glencore International AG, [2017] EWCA Civ 365 (for evidence that cyber risks can ultimately result in carrier's liability).

of UK in 'Code of Practice: Cyber Security for Ships.'[3] However, from an insurance perspective these cyber risks are viewed as hazardous to the liability of the insurer, generally and historically.[4] Making this difference evident is the rise of a whole new fleet of commercial ships, under development, which will be entirely automated and remove entire crews from being present on board.[5] These vessels, which are being called autonomous ships, are surely going to present new challenges for the insurer's risk assessment. At the same time, these new vessels could possibly reduce the number of events giving rise to an insurance claim since human error has been recognised as a contributing cause to the majority of marine casualties.[6] In order to accommodate this league of ships which promise safer operations, the insurance industry will have to look towards its present practices in treatment of cyber risks. This paper aims to look at the current exposures of the shipping industry to cyber risks. Finally, the paper envisages a situation where a cyber risk and an insured peril will play parallel parts and examines the treatment of such a situation under the doctrine of proximate cause in English Law.

II
CYBER TECHNOLOGY IN SHIPPING

According to Lloyd's Register, it is more likely that we will see the use of autonomous vessels on the high seas before we see autonomous on roads.[7] It is true that unmanned or crewless small

---

[3]H Boyes and R Isbell, Code of Practice: Cyber security for ships, Institution of Engineering and Technology, 13 (2017), http://www.gov.uk/government/publications/ship-security-cyber-security-code- of-practice.

[4] Judy Greenwald, Insurers still wary of taking on cyber risk, Business Insurance, (2017), http://www.businessinsurance.com/article/20170223/NEWS06/912312057/Insurers-still-wary-of-taking-on-cyber risk-Deloitte-report.

[5] International Maritime Organization, Autonomous Shipping, http://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx.

[6] Allianz Global Corporate and Speciality AG, Safety and Shipping 1912–2012, 41 (2012), https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2012.pdf.

[7] GMTT2030 Team, Global Marine Technology Trends 2030 — Autonomous Maritime Systems, Lloyd's Register Group Ltd, QinetiQ and University of Southampton, 6 (2017), https://cdn.southampton.ac.uk/assets/imported/transforms/

craft are already in use with many navies and other entities.[8] Globally, governmental and non-governmental organisations such as the European Union's 'Maritime Unmanned Navigation through Intelligence in Networks (MUNIN),' China's 'Uncrewed Multifunctional Maritime Ships Research and Development Project,' Sweden's 'Safety and Regulations for European Unmanned Maritime Systems (SARUMS)' and United Kingdom's 'Maritime Autonomous Systems Regulatory Working Group (MASRWG)' are looking into different facets of autonomous shipping. The consequent findings reflect a fierce competition between various organisations to place the first commercially viable autonomous vessel onto the sea.[9] Acknowledging the above findings leads us to the invariable conclusion that the shipping industry has seen great technological development in the recent past through the combination of computer, mobile, satellite and software technology. Systems such as dynamic positioning systems developed by Rolls Royce and their Unified Bridge design technology are already in use and point to the cyber compatibility of the shipping sector.[10]

This is not to say that the shipping sector has lived in isolation from information technology advances and the most basic of computer technologies such as, thin film transistor/liquid crystal display screen radar (TFT/LCD)/ARPA, voyage management systems (VMS), electronic chart display and information systems (ECDIS), duplicated GPS and DGPS, doppler logs, gyrocompasses, steering consoles with adaptive autopilot, echo sounders with playback memory, magnetic compasses, wind sensors, voyage data recorders (VDR) and automatic identification systems (AIS), have all been in use for quite a while.[11]

---

content block/UsefulDownloads_Download/F9AFACCCB8B444559D4212E140D886AF/68481%20Global%20Marine%20Technology%20Trends%20Autonomous%20Systems_FINAL_SINGLE_PAGE.pdf.

[8]Helen Jackson, Unmanned Warrior 2016 success in numbers, Qinetiq, (2016), https://www.qinetiq.com/en-gb/unmanned-warrior-2016-success-in-numbers.

[9]Jon Walker, Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More, Emerj, (2019) https://emerj.com/ai-adoption-timelines/autonomous-ships-timeline/.

[10]Rolls-Royce, Unified Bridge wins Ergonomics Design Award, (2015), https://www.rolls-royce.com/media/press-releases/yr-2015/pr-28-10-2015-rr-unified-bridge-wins-ergonomics-design- award.aspx.

[11]Editor, Computerisation of bridges and engine rooms-Progress or regression?, Gard, (2002), http://www.gard.no/web/updates/content/52458/computerisation-of-bridges-and-engine-rooms-progress-or regression.

A. International Maritime Organisation (IMO) Recommendations

The IMO, through the workings of its Maritime Safety Committee ("MSC"), incorporated cyber risk management as one of the requirements under the International Safety Management ("ISM") Code.[12] That resolution aims to emphasize the risks emanating from cyber technologies in shipping by directing member states to verify that cyber safety forms part of the safety management system of the ship and ensure compliance by the first annual verification of the company's Document of Compliance after 1 January 2021.[13] Acknowledging that traditional risk management in shipping has been focused on 'operations in the physical domain' and the rise in cyber risk facing new age ships which employ various technological tools, the IMO has proposed a set of *Guidelines on Maritime Cyber Risk Management.*[14] It recognises the risks posed by hacking, malware, outdated software, and ineffective firewalls. It also points out more importantly that a distinction must be made between information technology ("IT") and operational technology ("OT"); bringing to light the contrast between risks emanating purely from use of data as information and risks arising from the use of data to control or monitor physical processes. This seems to be a result of identifying how the human element plays a part in amplifying vulnerabilities in the cyber network by using external devices such as mobile phones or third party services such as emails, social networks, etc. on board ships.[15]

B. The Guidelines on Cyber Security Onboard Ships ("The BIMCO guidelines")

The BIMCO guidelines are being touted as the most comprehensive guidance on cyber security issues in the shipping

---

[12]International Maritime Organization, Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems, www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/Resolution%20MSC.428(98).pdf.

[13]Id.

[14]International Maritime Organization, MSC-FAL.1/Circ.3 Guidelines On Maritime Cyber Risk Management, http://www.gard.no/Content/23896593/MSC-FAL.1-Circ.3.pdf.

[15]Phishing attacks and compromising ship safety through connection of personal devices are becoming an accepted risk causing activity. See, the various reports published by 'Be Cyber Aware at Sea,' a pan industry effort to promote awareness of the increasing maritime cyber threats, accessible at: https://www.becyberawareatsea.com/awareness.

industry. [16] In an industry which is highly reliant on creating standard customary practices across the breadth of entities involved, these guidelines may be an effective way of testing whether a ship-owner has taken reasonable care in managing cyber risks to ensure seaworthiness of the ship.[17] This might be an important issue for ship-owners to look at because of the implied warranty of seaworthiness in marine insurance contracts.[18] The strength of these guidelines comes from the fact that they provide obvious inclusions to the globally accepted International Code for The Security of Ships and of Port Facilities ("ISPS").[19] According to the ISPS code, every ship should maintain a ship security plan which shall inter-alia mention different security levels and the steps to be taken during the subsistence of each level. In effect, the BIMCO guidelines intrude into the traditional definitions of ship security, functions of security personnel and steps for ensuring ship safety, by infusing ingredients of cyber security to be read into these. To afford clarity, ship security should include the security of the computer systems on-board by employing correct firewalls, updated software and constant monitoring of 'the ship to shore' internet connection path.

It also expresses the current state of affairs by pointing to the gap between technological advancement in shipping and the cyber resilience of these technologies. It also adds clarity on how to incorporate cyber safety into the safety management system as stipulated under the ISM. The guidelines range from simple suggestions such as maintaining segregation between secured and unsecured networks, to more in depth approaches that cover various levels of the company management on and off board. True to the evolving nature of cyber technologies and to keep a fair view

---

[16]Editors, The Guidelines On Cyber Security Onboard Ships, International Chamber of Shipping, (2017), http://www.ics-shipping.org/docs/default-source/resources/safety-security-and-operations/guidelines-on-cyber-security-onboard-ships.pdf?sfvrsn=14.

[17]Mathew Montgomery, New Bimco Cyber Security Guidelines, HFW, (2017), http://www.hfw.com/New-BIMCO-Guidelines-July-2017.

[18]As Prof. Soyer puts it "the implied warranty of seaworthiness . . . does not just cover the structure of the vessel, but extends to the smallest detail on board, such as the adequacy of stores and accuracy of charts." See, B. Soyer, Warranties in Marine Insurance, Routledge, 65 (3d ed. 2017).

[19]According to IMO "In essence, the Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case." http://www.imo.org/blast/mainframe.asp?topic_ id=897#what.

of the issues ahead, these guidelines have undergone a process of revision and the latest version was released in December 2018.[20]

C. Lloyd's Register's 'Cyber (AL-Safe)' – ShipRight Procedure Guidance

Lloyd's Register ("LR") is pioneering classification practices that accommodate cyber technologies with marine.[21] According to its 'Cyber (AL-Safe) classification', each different automated function is granted an AL-Safe certification depending on its level of autonomy. However, more pertinent to our study, is the safety of these systems from cyber risks. To this end, the classification process takes into consideration the integrity of the systems; meaning whether data is correct, true and unaltered; maintaining that data can be protected from unauthorised or unintentional change; and, recognising when such changes occur and responding appropriately.[22] More specifically, the following targeted and untargeted threats have been mentioned as being important while considering cyber security of ship systems:

- Social Engineering
- Phishing
- Water holing
- Ransomware
- Scanning
- Spear-phishing
- Deploying a botnet
- Subverting the supply chain.[23]

What is interesting is that the procedure identifies cyber risks in an assessment principle that recognises both benign and malicious threats. Furthermore, it targets four avenues of vulnerabilities: access; hardware; software; and, interconnection of systems.

---

[20]Rasmus Nord Jorgensen, Industry Publishes Improved Cyber Guidelines, BIMCO, (2018), https://www.bimco.org/news/priority-news/20181207-industry-publishes-improved-cyber-guidelines.

[21]Lloyd's Register, First ships in the world to be certified Cyber SAFE delivered, (2017), www.lr.org/en/news-and-insight/news/first-ships-in-the-world-to-be-certified-cyber-safedelivered.aspx.

[22]Lloyd's Register, Cyber-enabled ships: ShipRight procedure – autonomous ships, July, 2016, at 14.

[23]Id. at 18.

Finally, emphasis has been laid on the 'Framework for improving Critical Infrastructure Cyber Security' developed by the National Institute of Standard and Technology ("NIST") which provides that any cyber security framework should be able to execute five essential functions, namely: identify, protect, detect, respond and recover.

D. ABS CyberSafety (CS classification)

Like Lloyd's Register, ABS is another classification society that has introduced a classification for cyber systems on board ships. Called the 'CS series,' these notations, as ABS argues, can be a useful tool for ship owners to prove that they applied due diligence in preparing for cybersecurity concerns and countering cybersecurity threats.[24] The ABS guidelines go into great detail of the practical steps a ship-owner would have to take to meet the different class requirements. These seem to go hand in hand with the scale of operations of each entity and are proportional to their capital infrastructure.

III
CURRENT CYBER RISKS – THE ATTACKS

A. Petya

The cyber-attack on Maersk in June of 2017, was a ransomware known as 'Petya'.[25] It is a virus that restricts access to a computer or its data and demands ransom in order to free the computer for use. Once inside a network of computers, the ransomware can spread rapidly across each computer on the network.[26] Significantly, the attack is said to have targeted the Ukrainian government and entities.[27] Even though researchers have touted it as an amateur attack, its impact is underscored by Maersk releasing a statement on Twitter stating that "Global cyber-attack Petya is

---

[24]American Bureau of Shipping, Guide for cybersecurity implementation for the marine & offshore industries, 2d ed. 2016, at ii.

[25]Olivia Solon & Alex Hern, 'Petya' ransomware attack: what is it and how can it be stopped?, The Guardian, (2017), https://www.theguardian.com/technology/2017/jun/27/petya-ransomware- cyber-attack-who-what-why-how.

[26]Id.

[27]Id.

affecting multiple businesses."[28] Pointing to the pervasive nature of cyber-attacks, this attack singularly had the capacity to affect 17 APM terminals around the world.[29]

B. Port of Antwerp

The attack on the port of Antwerp showcases the professional and organised manner in which cyber criminals can execute attacks. It lasted over a two year period beginning in June 2011.[30] Drug traffickers in conjunction with hackers systematically hacked the container management systems and then proceeded to physically extort containers from the port compound by using information retrieved from initial hacks.[31] This is a case where IT was subsequently used to manipulate OT.[32] The case of Mediterranean Shipping Company SA v Glencore International AG arises from this incident.[33] The carrier, MSC, was held liable for mis-delivery when hackers retrieved the pin code required by the port's Electronic Release System ("ERS"), which was communicated by the carrier to the receiver's agents via email, and then used to enter the container park and leave with the container. The facts point towards a growing trend by large ports of adopting computer codes rather than relying on physical inspection of documents.[34] Resultantly, the court's decision transfers the risk of theft from the receiver to the carrier in such cases.[35] The recoil from such a ruling could make carriers resort back to traditional methods of delivering goods through the exchange of physical documents, which would undoubtedly lead to longer waiting times at container parks and hence, more strain on already over supplied ports. Thus, the efficiency that the ERS provided to reducing the time between

---

[28]Jacob Gronholt-Pedersen, Maersk says global IT breakdown caused by cyber-attack, Reuters (2017), http://www.reuters.com/article/us-cyber-attack-maersk/maersk-says-global-it-breakdown-caused-by-cyber-attack-idUSKBN19I1NO.

[29]Id.

[30]Tom Bateman, Police warning after drug traffickers' cyber-attack, BBC News (2013), https://www.bbc.co.uk/news/world-europe-24539417.

[31]Magal, New Cyber Frontiers (Antwerp Port Case Study), Magal-S3, http://www.magal-s3.com/contentManagment/uploadedFiles/White_Papers/Cyber_For_ICS_Antwerp_Case_web.pdf.

[32] Bateman, supra note 30.

[33] Mediterranean Shipping Company SA v. Glencore International AG, [2017] EWCA Civ 365.

[34] Id.

[35]Id.

container arrival to departure (1 day in this case) was let down by the commensurate risk of clandestine theft exposed by cyber-attacks.

C. Hacks of Navigational Systems

Another aspect of cyber-crime surfaces in the pleasure craft industry which is symbolic of high net worth individuals and relatively less secure luxury.[36] In an interesting demonstration at the 2017 Superyacht Investor Conference, a Blackberry IT engineer showcased how easy it was to hack into a super yacht's Wi-Fi networks, thereby taking control of the yacht's satellite communications, telephone system and navigation.[37] Concurrently, there is a growing awareness of the lack of anti-virus software on ship systems around the globe. Commonly used navigation technologies such as Electronic Chart Display ("ECDIS") and Automatic Identification System ("AIS") are susceptible to cyber manipulation.[38] These systems are critical to shipping today as they facilitate the exchange of data such as position, name, and cargo.[39]

AIS is particularly used by port authorities to inform ships of hazards such as low tides, rocky outcroppings and shoals.[40] AIS can even be used to locate men who have fallen over board.[41] Researchers have found that AIS is particularly susceptible through two paths: software and radio frequency.[42] These can be used by possible hackers to broadcast fake weather forecasts, to fake distress signals, to impersonate maritime authorities and to create a virtual ship (a concept known as ship spoofing).[43] This can

---

[36]Unreported ransomware attacks have held yacht navigation systems to ransom. See Rupert Neate, Cybercrime on the high seas: the new threat facing billionaire superyacht owners, The Guardian (2017), https://www.theguardian.com/world/2017/may/05/cybercrime-billionaires-superyacht-owners- hacking.

[37]Ian Prasad Philbrick, It took a specialist less than half an hour to hack into a superyacht, Slate (2017), http://www.slate.com/blogs/future_tense/2017/05/16/it_specialist_hacks_into_superyacht_in_less_than_ 30_minutes.html.

[38]Chris Baranuik, How hackers are targeting the shipping industry, BBC (2017), http://www.bbc.co.uk/news/technology-40685821.

[39]M. Balduzzi, K. Wilholt & A. Pasta, A security evaluation of AIS, Trend Micro (2014) https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-a-security- evaluation-of-ais.pdf.

[40]Id.

[41]Id.

[42]Id.

[43]Id. at 8.

influence navigators on board vessels to deviate their path leading them to piracy prone zones or, in case of a poor bridge-watch, to collide into vessels whose signals have been spoofed so as to make them virtually invisible. What makes these systems even more vulnerable is the free availability of a ship's data online on open source platforms.[44] This information gives real time update of a ship's status, such as which direction it moves in, whether it is anchored, what kind of vessel it is and at what speed it is traveling.[45]

D. Cyber Concerns for Vessels of the Future

As pointed out in the 'Introduction' to this paper, the shipping industry is looking at making unmanned vessels a reality.[46] These ships are already in the stage of testing and the IMO has already issued guidelines for their testing.[47] With the incorporation of processes such as on shore remote operating centres which will communicate and control ships at sea, the pool of possible cyber-attacks and vulnerabilities will increase as a consequence of exponential technological integration.[48] This conclusion is obvious because the technologies to remotely control vessels would already be in place and hackers would only need to take control of the on shore operations.[49] Also, it has been pointed out that the linking of on board computer systems to navigational functions may provide the required scope for causing harm through cyber-attack.[50]

---

[44]Cf. www.marinetraffic.com, www.shipais.co.uk, and, www.vesselfinder.com (for examples).

[45]Id.

[46]GMTT2030, supra note 7.

[47]https://www.register-iri.com/wp-content/uploads/MSC.1-Circ.1604.pdf.

[48]Oskar Levander, Forget Autonomous Cars—Autonomous Ships Are Almost Here, IEEE Spectrum (2017), https://spectrum.ieee.org/transportation/marine/forget-autonomous-cars-autonomous- ships-are-almost-here.

[49]Such considerations have already been discussed with regard to more visible technologies such as drones. See David Kennedy, A former Marine cyber warrior explains how hackers will transform the face of modern combat, Business Insider UK (2017), http://uk.businessinsider.com/marine-cyber-warrior-hackers-transforming-modern-combat-2017-8?r=US&IR=T.

[50]Stephenson Harwood & Joint Hull Committee, Cyber Risks, Lloyd's Maritime Academy (2015), http://www.lmalloyds.com/LMA/News/whats_hot/JHC_Cyber_Info_Paper.aspx.

IV
PRESENT STANCE OF THE INSURER – THE ROMANCE WITH CL380

A. The Institute Cyber Attack Exclusion Clause – Cl. 380 – What and why?

> The risk of a loss to a ship as a result of cyber disruption is foreseeable, but is not yet a reality. A systemic threat which could conceivably result in multiple losses on a scale which might impact the solvency of the world's insurers and reinsurers does not yet exist.[51]

It would not be wholly faulty to conceive that such a view has shielded the insurers from any strong pressure from the ship owners; and hence, in the marine insurance industry it is common practice to exclude losses arising from cyber risks.[52] One of the common clauses used by insurers to exclude cyber liability is CL 380, which states as follows:

> Institute Cyber Attack Exclusion Clause CL380:
>
> 1.1 Subject only to clause 1.2 below, in no case shall this insurance cover loss, damage, liability, or expense directly or indirectly caused by, or contributed to by, or arising from, the use or operation, as a means for inflicting harm, of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system.
> 1.2 Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, Clause 1.1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software programme or any other electronic system in the

---

[51]Id.

[52]Willis, Energy Market Review 2014 (Cyber-Attacks: Can The Market Respond?), Willis (2014), http://www.willis.com/documents/publications/industries/energy/20140404_Willis_Energy_Market_Re view_2014.pdf.

launch and/or guidance system and/or firing mechanism of any weapon or missile.

The clause states that the insurer will not be liable in any case where the use or operation of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system has directly or indirectly caused, contributed or given rise to loss, damage, liability or expense. The only relief that the clause seems to afford the insured is that it activates in the case where such cyber risk has been employed 'as a means for inflicting harm', in layman terms this would seem to mean where a 'cyber-attack' has taken place. Other than break down of the computer software itself due to purely technical reasons, it is hard to fathom a scenario where a cyber risk would not be activated by a cyber-attack. There has been debate on whether the phrase begs for subjectivity or, as is generally the case in the realm of cyber activity, an attack may be untargeted. To not mince words any further, the crux of the issue is whether 'infliction of harm' should be dependent on whether the 'hacker' wanted to inflict harm on the insured's insurable interest specifically.[53]

It is important to acknowledge here the nuances of the internet which bring to the fore the following conclusions: (a) the identity of the hacker may never come to light; (b) even if the identity does come to light, there is no surety that the hacker will be in a jurisdiction where enforcement might be possible because the world of internet does not require the perpetrator to be in physical proximity of his target; and (c) hackers working without political or personal vendetta do so to gain financial wealth without debating whose money it is that they are getting.[54]

Or on the contrary, while acting with a political motive, hackers may end up harming others in a broader collateral damage sense. An example of this are the recent 'NotPetya' attacks that affected Maersk. It is believed the attacks were carried out by Russian hackers motivated to harm Ukraine's interests. Often, attacks are not targeted at anyone specific but are sent out *en-masse*, hoping to affect the most vulnerable and/or unsecured. Hence, for the

---

[53]Also, pointed out by Mr. Simon Cooper, Partner Ince & Co LLP in his paper 'Cyber risk, liabilities and insurance in the marine sector' presented at the 13th Annual International Colloquium, 'Maritime liabilities in a regional and global context', The Institute of Shipping and Trade Law, Swansea University.

[54]See, Judgment of Buxton LJ in Tektrol Ltd v. International Insurance Co. of Hanover Ltd & Anor. [2005] EWCA Civ 845.

purposes of this paper this question of intent shall not be discussed further. It may suffice to say that where a cyber-attack is not involved, the insurance industry may push for stringent classification procedures, as pointed out in chapters above, to be adopted by ship owners in anticipation of receiving the right cover. Unfortunately, throughout human history errors have been made and it would only be a fool's errand to believe that with stringent classification the possibility of computer technology breaking down or malfunctioning will become nil.

The more frustrating conundrum that this clause brings to light is that it aims to abolish the liability of the insurer in case of even the faintest contribution of a cyber-attack to the '*loss or damage or liability or expense*' suffered by the insured. To put it simply, insurers have tried to steer clear from the subject of marine cyber-attacks.[55] In a legal setting, this clause aims to override the question of causation when construing how the insured's loss took place. In an insurance context, it is of fundamental importance to see whether the indemnity being asked for was caused by an insured peril.[56] As Professor Bennett puts it, this is so because parties to the contract have chosen to formulate the extent of cover in terms that include causal expression.[57] In insurance law, this principle of causation achieves its distinct identity as the '*doctrine of proximate cause*'.[58] This has been codified in English Law through Section 55(1) of the Marine Insurance Act 1906, which remains unaffected by the Insurance Act 2015.[59] There has been considerable jurisprudence on what is a proximate cause. It will be relevant to bring some of the salient features of this area of jurisprudence into our discussion.

---

[55]However, keeping in mind the wishes of the market, the industry has come out with variables such as 'CL380 Hull amended' clauses which seek to cover the traditional marine perils even where computers or related systems are involved; see supra note 52.

[56]HOWARD BENNETT, LAW OF MARINE INSURANCE 301 (2d ed. 2006).

[57]Id. at 302.

[58]James Davey, All risks insurance and computer data – "policy" considerations in the Court of Appeal: Tektrol v. International Insurance, COMMUNICATIONS LAW, 2005, at 175–177.

[59]Section 55 (1), Marine Insurance Act 1906 ("Subject to the provisions of this Act, and unless the policy otherwise provides, the insurer is liable for any loss proximately caused by a peril insured against, but, subject as aforesaid, he is not liable for any loss which is not proximately caused by a peril insured against.").

B. The Proximate Cause Doctrine

Early judicial precedent for the doctrine can be in found the court of appeal judgment of *Reischer v. Borwick*, where a ship was covered against collision with any object but not against perils of the sea.[60] The ship first encountered a collision and then subsequently sank when one of the plugs was forced out while encountering extra water pressure during towage. The court, while holding in favour of the insured, concluded that, (a) proximate cause need not be the exclusive cause; (b) due consideration should be paid to the intent of the parties;[61] and (c) regard should be given to whether the final eventuality was a foregone conclusion. In taking the cause further, an insurer favoured judgment pronounced by Lord Shaw held that "the cause which is truly proximate is that which is proximate in *efficiency.*"[62] Although he chose to not elaborate on what would constitute an 'efficient cause,' he disproved the argument of looking at the cause last in time.

It is also important to note here that in the *Leyland case*, Lord Shaw further elaborated that where various causes have contributed to the loss, the matter should be determined based on facts and the dominant, real and efficient cause should be chosen.[63] To take refuge from a long list of cases on the subject, reference is made to the work of Malcolm Clarke who puts forward a curious test to check whether the cause in question is the proximate cause.[64] He says "loss of the kind covered must be inevitable, but the extent of the loss need only be such as would have been within reasonable contemplation or not unlikely to occur."[65] While an on-board cyber systems hack would by itself not lead to ingress of water and/or damage to ship, it may be a contributing factor where a collision has taken place due to manipulation of ECDIS, or where pirates have used on board navigation systems to make a successful piracy attempt. Would then cyber-risk be considered a proximate cause of the insured peril? In fact such a controversy, relating to the

---

[60][1894] 2 QB 548.

[61]The insurers had agreed to make partial payment for the collision damages.

[62]Leyland Shipping Co. Ltd. v. Norwich Union Fire Insurance Society Ltd., at 369, [1918] AC 350.

[63]Bennett, supra note 55, at 370.

[64]Malcolm Clarke, Insurance: The Proximate Cause in English Law, CLJ, 40(2), Nov 1981.

[65]Id. at 288.

sufficiency of electronic maps, has been the subject of litigation in at least one recent case from 2019.[66]

Now, there are 2 other rules that can influence this doctrine, namely:

> *3. Novus actus interveniens* – This rule dictates that if there is an intervening act that substantially alters the chain of causation i.e. the events leading up to the loss being claimed for, then that act should be considered the proximate cause. In the *Leyland* case the repeated grounding of the vessel after being torpedoed was held not to be an intervening act and thus not activating this rule.
>
> *4. Verba chartarum fortius accipuntur contra proferentem – Or 'contra proferentum',* is a rule of interpretation which dictates that an ambiguous clause shall be interpreted as against the party responsible for drafting it.[67] However, this rule is to be resorted to only after other remedies, such as reading of the contract in context with the intent of the parties or identifying the purpose of the document, have been exhausted.[68]

C. Multiple Proximate Causes

However, the doctrine itself has suffered variation in recent judicial interpretation due to the inclination of judges to identify multiple proximate causes. This line of cases may be divided into two categories, one being a case where one proximate cause of loss is covered by the policy while the other is not covered neither excepted, and the second being where one of the causes is covered while the other is excepted. For the first category of cases, the Court of Appeal has decreed that where the ship had been lost as the result of the combination of two causes and the policy did not provide an exclusion or warranty against the cause not covered the insured will be entitled to claim on proof of the covered peril.[69] It may therefore

---

[66]Linda McKeever v. Northernreef Insurance Co S.A., [2019] 2 Lloyd's Rep. 161 (where the claimant's statement as to purchase of updated chips for an otherwise out-of-date electronic map system was accepted as to their sufficiency).

[67]Youell v. Bland Walch & Co Ltd., at 134, [1992] 2 Lloyd's Rep 127.

[68]Dirett Travel Insurance v. McGeown, [2003] EWCA Civ 1606. See also Lindley LJ in Cornish v. Accident Insurance Co., at 456, (1889) LR 23 QBD 453, where he stipulates that the rule must be used only 'in a case of real doubt'.

[69]JJ Lloyd Instruments Ltd v. Northern Star Insurance Co. Ltd., at 37, [1987] 1 Lloyd's Rep 32.

suffice to say that where a cyber-exclusion of any kind has not been incorporated into the contractual terms of the policy, a claimant shall be indemnified on proving that the damage happened due to one of the insured perils.

In the second category of cases, which is more relatable to CL380, the courts have relied on reading carefully the exception clause to see whether it allowed for room to accommodate the covered peril[70] or pleaded for freedom by exemption of liability altogether.[71]

In *Isitt v Railway Passengers Assurance Co*, the assured suffered an injury caused by an accident within the scope of the policy, and thereby subsequently died due to pneumonia.[72] The policy wording was 'if the assured shall sustain any injury caused by accident... and shall die from the effects of such injury.' The court therein held that the death resulted 'from the effects of such injury.' This led to the accident underwriters incorporating a more elaborate exclusion clause which read 'where the direct or proximate cause [of death] is disease or other intervening cause, even though the disease or other intervening cause may itself have been aggravated by such accident, or have been due to weakness or exhaustion consequent thereon, or the death accelerated thereby.' Even this wording failed the underwriters in their subsequent endeavours to claim exclusion.[73]

However, as impeccably noted by *J. Lowry and P. Rawlings*, the sanctity of English insurance contract law lies in the notion of freedom of contract and there is no denying that a suitably worded clause would achieve the aim of exclusion as sought by insurers.[74]

D. IUA Scenario

Consequent to the above, it becomes imperative to evaluate a marine policy that incorporates the CL380. The chosen scenario has been taken verbatim from a paper of the International

---

[70]Midland Mainline v. Eagle Star Insurance Co. Ltd., [2004] EWCA Civ 1042.

[71]Wayne Tank and Pump Co. Ltd v. Employers Liability Assurance Corp. Ltd., at 69, [1974] QB 57.

[72]Isitt v. Railway Passengers Assurance Co., (1889) 22 QBD 504.

[73]In the matter of an arbitration between Etherington and the Lancashire and Yorkshire Accident Insurance Co., at 598, [1909] 1 KB 591.

[74]John Lowry; Phillip Rawlings, Proximate Causation in Insurance Law, 68 MOD. L. REV. 310, 319 (2005).

Underwriting Association (IUA) and hence, is a valuable insight into what the insurer's stance on cyber marine insurance is.[75]

> Two vessels are insured against marine risks in the London market under English law policies incorporating ITC-Hulls (01/10/83) and the Institute Cyber Attack Exclusion clause (10/11/03–CL380). Vessel A is trading and uses ECDIS (Electronic Chart Display & Information System), which is updated via the internet. Vessel B is laid up in a recognised anchorage and complies with applicable lay-up requirements. Vessel A sails into the anchorage and strikes Vessel B. On investigation, it transpires that the anchorage had been shown on the ECDIS chart until updated via the internet, two weeks prior to the collision. The update had deleted the reference on the chart to the anchorage by reason of a malicious code or software programme inadvertently loaded with the update. The officer on watch had not sailed in that area previously and had not been keeping a proper lookout. Subsequent investigation reveals the presence of the malicious code or software programme but is unable to identify the source of the code/programme or its author. There is no evidence to suggest that the author of the code/programme was a terrorist or acting from a political motive (see clause 24.2 of ITC-Hulls).

V
ANALYSIS

It is deemed that the most probable contentions put forward by the assured to claim indemnification under the policy would be, (a) collision as a peril of the sea,[76] or (b) negligent navigation.[77] This is in consonance with the IUA view as well. The burden of proving that the loss occurred from either of these perils falls on the assured

---

[75]International Underwriting Association, Cyber Risks and Insurance – An Introduction to Cross Class Cyber Liabilities, http://www.maritimelondon.com/wp-content/uploads/2016/01/005_Cyber_Risks_Combined_110116.pdf, (2016).

[76]See Clause 6.1.1 – perils of the seas rivers lakes or other navigable waters. See, House of Lords Judgment in Thomas Wilson, Sons & Co v Owners of the Cargo per the Xantho (The Xantho), (1887) 12 App Cas 503.

[77]See Clause 6.2.3 – negligence of master officer crew or pilots. This clause is referred to generally as part of the Inchmaree Clause which expressly includes perils that may not fall within the fortuitous requirement of the traditional perils. See, judgment of Hodson J, as he then was, in Baxendale v Fane (The Lapwing), [1940] P 112.

and would entail the assured identifying a fortuitous ingress of water.

However, it would be open to the insurers to argue against indemnification based on the broad wording of the cyber-attack exclusion clause. In the view of the IUA, it is mentioned succinctly that the opening words of the clause are very broad and would back such an argument. Specific attention must be given to the words 'contributed to by', at the very least the removal of the anchorage from the ECDIS could be said to have contributed to the collision and subsequent damage to the vessel. Furthermore, the facts point towards the use of the internet and updating of the ECDIS which would have inadvertently made use of the computers and/or electronic systems on board. It is submitted that going by the closing words of sub-clause 1 of CL380, this situation stands covered under the instruments, tangible and intangible, mentioned therein.[78]

Considering the Court of Appeal holding in *Reischer v. Borwick* it is tenable that a court would see the malicious code resulting in the ECDIS anomaly as one of the probable causes of collision. This, according to IUA, would be enough to activate the exclusion in CL380. However, giving full credence to the ECDIS issue would amount to turning a blind eye to the fact it may as well have been possible to avert the collision had the deck officer been keeping a proper watch. This might constitute an intervening act under the *novus actus interveniens* exception to the proximate cause theory.[79] Which cause was more efficient in causing the damage would be determined from the facts by taking into account other factors. In the *Mckeever* case, the court, while considering the adequacy of electronic charts, did accept the witness's statements of employing paper charts in conjunction with the electronic charts,[80] thereby decreasing the value of an argument that the electronic charts could have been the efficient cause of damage.

IUA have also put forth the argument, albeit doubtfully, that 'malicious' in CL380 must be construed as a reference to the intent of the hacker and not to the code. Quite rightly, in this regard they

---

[78]"Of any computer, computer system, computer software programme, malicious code, computer virus or process or any other electronic system."

[79]Leyland Shipping Co. Ltd. v. Norwich Union Fire Insurance Society Ltd., [1918] AC 350 (reference should be made to Lord Dunedin's statements where he points out that that there was direct damage from the torpedo to the vessel and this fact was not mere part of the background that resulted in the subsequent sinking of the vessel).

[80]Linda McKeever v. Northernreef Insurance Co. S.A., [2019] 2 Lloyd's Rep. 161.

refer to the House of Lords judgments in *Grecia Express,*[81] *North Star*[82] and *B Atlantic*[83] cases to establish that 'malicious' can be a reference to random, non-specific intent that may or may not have been targeting the assured and which did not require to be proved.[84] The IUA then refers to the case of *Tektrol Ltd.*, where the controversy surrounded effect of a similar clause to CL380, although the IUA erred in noting that the exclusion only applied when the assured was 'specifically targeted'. In this case of an all risk business loss policy, the principle of *contra proferentum* plays a major role and brings out rather dramatically the importance of clear policy wording.[85]

A. Tektrol Ltd v International Insurance Co of Hanover Ltd & Anor.

The claimant, Tektrol, suffered a cyber-theft and a burglary which had the consequence of depriving the owners of the source code for their product. Tektrol claimed under the business interruption head of their policy and the insurers denied on both accounts, of cyber-theft and burglary. The exclusion clause in contention was as follows:

> Sections 1 & 2 do not cover:
>
> > 7. DAMAGE caused by or consisting of or CONSEQUENTIAL LOSS arising directly or indirectly from
> > (a) disappearance, unexplained or inventory shortage, misfiling or misplacing of information;
> > (b) in respect of Section 2:
> >
> > (i) Erasure loss distortion or corruption of information on computer systems or other records programmes or software

---

[81]Strive Shipping Corp v. Hellenic Mutual War Risks Association (Bermuda) Ltd., [2002] EWHC 203.

[82]North Star Shipping Ltd. v. Sphere Drake Insurance Plc., [2005] EWHC 665.

[83]Atlasnavios Navegacao Lda v. Navigators Insurance Co. Ltd., [2014] EWHC 4133.

[84]Referring to the court's reliance on the criminal law statute, Malicious Damage Act, 1861.

[85]Tektrol Ltd. v. International Insurance Co. of Hanover Ltd., [2005] EWCA Civ 845. See also Davey supra note 58, "..it demonstrated the difficulties that insureds face when seeking effective insurance cover."

> caused deliberately by rioters strikers locked-out workers persons taking part in labour disturbances or civil commotion or malicious persons;
> (ii) other erasure loss distortion or corruption of information on computer systems or other records programmes or software unless resulting from a Defined Peril in so far as it is not otherwise excluded.

At first instance, Langley J, as he then was, accepted the insurer's contentions that the computer virus placed by malicious persons fell within the exclusionary clause 7(b)(i).

He further held that the theft of computers resulted in loss of information which fell within the exclusion in 7(b)(ii). Although, Langley J was right in referencing the Court of Appeal judgment of *Wayne Tank and Pump Co Ltd v Employers Liability Assurance Corp. Ltd., [1974] QB 57* to hold that, "if the insurer could bring either of the incidents within an exclusion in the policy he was in any event not liable in respect of the other incident.

His findings were reversed by the Court of Appeal utilising the *contra proferentum* rule, the need of which was put efficaciously by Carnworth LJ as follows: "Although it is described as an 'all risks' policy, one has to search long and hard, through a bewildering and apparently comprehensive list of exclusions, to discover the extent to which any risks are in fact covered."

It was an accepted fact between the parties that the author of the virus was unknown.[86] However, the controversy, according to the Court of Appeal, was, (a) whether the attack was caused 'deliberately' and, (b) whether 'malicious persons' as written in the clause covered the hacker as well. In holding positively on the issue of whether the act was deliberate, the court said that there was no doubt that the intent of the hacker was to cause injury to a category of persons and such injury was caused deliberately because it was the aim and object of the hacker's actions, not just a random

---

[86]The court relied on the following assumption of facts: "The virus author had no knowledge of or connection to (Tektrol) or its source code. Although he did not intend to erase the ... source code, he intended the virus program to spread around the world and knew that whenever the virus program was activated by the opening of the "Christmas Card" attachment, computer data could be erased on the computer concerned."

event.[87] Additionally, the court said it matters not that Tektrol was one of his intended victims.

However, the *contra proferentum* rule was put into motion when the insurers argued that 'malicious persons' as mentioned at the end of the sentence that includes 'rioters strikers locked-out workers....' had the effect of bringing the hacker within its scope. This argument was unanimously rejected by the court who said that the hacker fell into a wholly different category, one which could not sit in conjunction with rioters or locked-out workers. This category pointed to the inference that the excluded damage envisioned by the draftsman was of the kind that could be effected by malicious persons in physical proximity to the insured's premises and not that of a remote hacker.

It was then argued whether the burglary was covered under the second exclusion. This time the onus of interpreting the word 'loss' fell on the court. In having to disagree with Langley J's interpretation that 'loss' covered the theft of the computers, the court pointed out that the court of first instance had reached this erring interpretation due to the draftsman's use of overlapping phrases. This was a case of linguistic overkill and redundancies in drafting.[88] It could not be fathomed that the draftsman would have intended to refer to a physical loss of hardware (i.e. a computer) by merely using a single vague word in the middle of a clause that refers to software/electronic means. These findings suggest that the *contra proferentum* rule may play an important part in determining the meaning of specific cyber exclusions.

In dissent, Carnwath LJ took the view that, on the burglary issue, the emphasis of the exclusion is on the nature of the thing lost and not on the mechanism by which the loss arises.[89] In fact in a very recent case of a public liability insurance, the *contra proferentum* rule was again used to come to a finding against the insurer where the liability under the policy was sought to be excluded on the basis of an exclusion that incorporated the words 'deliberate acts' of the

---

[87]The hacker's actions were contrasted to those of someone causing accidental harm in the event of simply using the system.

[88]The court refers to Lord Hoffman's observations in Tea Trade Properties Ltd. v. CIN Properties Ltd., [1990] 1 EGLR 155 and in Arbuthnutt v. Fagan, [1995] CLC 1396.

[89]He wished to dismiss the appeal on the second issue even though he noted that the wording used was not clear.

insured.[90] In interpreting that the 'deliberate act' contemplated by the exclusion meant an act which is done to create liability for losses covered by the policy, the court declined to accept a general-broader meaning of the term that would work against the insured.[91]

VI
CONCLUSION

These differing views depict the difficulty in ascertaining the precise limits of insurance cover when it comes to dealing with cyber risks.[92] It would be interesting to see how insurers draft new policy and exclusion clause wordings.

As for the insurer, it is believed that CL380 aims to escape the proximate clause principles. However, it will have to be seen how far courts are ready to go with this understanding. Emphasis will be laid on whether a clause such as CL380 is paramount in nature and whether the wording is clear enough to encapsulate the kind of cyber-attack that has taken place. Debate could arise whether the words of the present clause are meant to refer to both externally brought on cyber risks (such as via the internet) that cause harm to IT, or internally brought on cyber risks (such as via personal devices) that cause harm by manipulating the OT. Would aspects of cyber risk start reflecting in covered perils such as negligence by crew (in using personal devices on-board that lead to virus infection)? We can see from the case of *McKeever* that this has already been put to the legal test through the lens of determining the vessel's navigational adequacy.[93]

A question that still needs answering emanates from the intentions of the parties while entering the contract. It is to be seen whether the acceptance of the cyber classification of a vessel results in a tacit acceptance by the insurer of the standard of cybersecurity on board. Because if it is so, then why should a court of law be disinclined to apply the *contra proferentum* rule to read the CL380 clause as not being applicable to cyber elements that have received

---

[90]Burnett v. International Insurance Co. of Hanover Ltd., [2019] CSIH 9 (as per author's last check as of time of writing, an application for permission to direct appeal had been granted by the Supreme Court).

[91]Id.

[92]See James Davey supra note 58.

[93]Linda McKeever v. Northernreef Insurance Co. S.A., [2019] 2 Lloyd's Rep. 161.

the required classification? It seems highly unlikely that a ship-owner would not bank upon such accepted classification procedures that are a key check point for shipping vessels. Additionally, it can be easily argued through the lens of the *Burnett* case that the CL 380 wording "as a means for inflicting harm" should be construed narrowly so as to exclude only a targeted attack on the insured and not an attack which can't be identified as having a specific intent to harm the insured.[94]

[94]Burnett v. International Insurance Co. of Hanover Ltd., [2019] CSIH 9 (as per author's last check as of time of writing, an application for permission to direct appeal had been granted by the Supreme Court).