UNIVERSITY OF PIRAEUS

DEPARTMENT OF MARITIME STUDIES

MARITIME STUDIES PROGRAM IN SHIPPING

SHIPPING MANAGEMENT

Assignment:

"CYBER ATTACK AS A COVERED DANGER IN MARINE INSURANCE"

Diplomatic Thesis

submitted to the Department of Maritime Studies of the University of Piraeus

to cover the requirements for the completion of

the MSc in Shipping management graduate program

PIRAEUS, DECEMBER 2022

DECLARATION OF AUTHENTICITY

The person who carries out the thesis bears the entire responsibility of determining the fair use of the material, which is defined on the basis of the following factors of the purpose and character of the use (commercial, non-profit or educational), the nature of the material used (exctract, part of text, drafts, figures, images or maps), the proportion and importance of the part it uses in relation to the whole copyrighted text and the possible consequences of such use on the market or the general value of the copyrighted text.

EXAMINATION COMMITTEE

The members of the Committee:

Professor Mr. Georgios Daniel
Professor Mr. Dionysios Polemis
Professor Mr. Ioannis Lagoudis

The potential approval of the thesis by the Department of Maritime Studies of the University of Piraeus does not indicate acceptance of the positions and opinions of its author.

ACKNOWLEDGEMENTS

The subject of this work initially motivated my curiosity to undertake the study, analysis and subsequent structuring and synthesis of the three main factors and concepts that structure it, i.e. insurance risk coverage, cyberattack and all this in the field of marine insurance. The problem of the subject is not only topical, but it is an issue that has already concerned the field of marine insurance, jurisprudence, legal science and the modern way of life, where everything now revolves around the concept of information. Based on the occasion and the stimulus to deal in depth with this burning and contemporary issue, I thank my supervisor for entrusting me with the topic in question and the president of the Department, Mr. Angelos Pantouvakis, who suggested my collaboration with Mr. Daniel.

With respect

Theofanis Michalopoulos

Dedicated to Marianthi…

CONTENTS

Introduction

According to Aristotle 2,500 years ago, the question of "(the first) moving immovable" was raised. Many philosophical theories have been developed on this topic. After all, does the property move other bodies or not? Speed is an element of our time, everything moves at such speeds that motionlessness is observed. In my opinion, the application of the above theme raised by the great natural philosopher Aristotle fits almost perfectly the current era we are going through, which is characterized by science and theory as the era of the digital revolution. Indeed, we live in an era where with a press of a button we can find ourselves in zero time, and without moving, to the other end of the universe and receive the "gold" of our time, information.

The digital revolution as a human invention or discovery has penetrated into all productive sectors, primary, secondary and tertiary, thus also in maritime transport. Basic elements of digitization in rough lines are what is called as cyberspace, which as a definition prevailed of cyberspace, denotes the environment created by communication networks using computers, local area connections (LANs) and/or wide area networks (WANs) such as the Internet. From the 2010s onwards, the replacement of traditional practices of the past by the modern way of life with the use of the internet and cyberspace in general was realized with speeds like those of the internet itself. Maritime transport, a critical sector for globalisation, on which human societies, state structures, giant enterprises depend, could not but be part of this digital dependence as cyberspace provides the two key elements of the modern era, speed and information, very important things that the shipping industry needs, namely accuracy, proper operation and delivery and receipt of goods at the desired time. The benefits of this revolution in the productive sector are of enormous dimensions as they cover with the above elements the needs of man from the most basic, such as feeding, to the comfort of the "well life", while the global economy develops further as it has been defined in different ways with the positives and the negatives, depending on the point of view that everyone benefits from it or not, but in any case the quantitative and qualitative size of it is constantly increasing and indeed in this case with with great acceleration. Examples of the positive penetration of cyberspace in maritime transport are the security of navigation, the security of cargo, the security of transactions, the organization of business and the dissemination of information in

times completely different from the previous twenty years. Electronic systems have entered everywhere and everything now depends on the computer.

Aristotle's ancestor, another great philosopher, Socrates, mentioned another great trait, which has also received a multitude of approaches and analyzes from theory and science over the centuries, having, and it is none other than the well-known phrase "I know one thing that I don't know anything". The "simple" Socrates within a sentence of five words in the Greek pronunciation of his style managed to integrate to an almost absolute degree the concepts of humility, objective perspective of things and what people call truth, revealing at the same time the vanity of human desire. This phrase at the particular point of the introduction is used as an antithesis to the phrase of the later philosopher Socrates mentioned above, to express in the best possible way that no human creation is understood that does not also bring its negative effect, despite his great desire of man to progress towards evolution. In this way, that great philosopher, Socrates, even today answers in the same way that he answered when he was alive, that is, with enough sarcasm, that cyberspace also has its pathogenesis, which appeared almost at the same time with the territory of this (cyberspace) in the making, and in this case in the making of maritime transport. Cyber-attack as a term used for the negative action of third parties or persons operating within shipping companies, with the purpose of its economic destruction or their economic benefit using the very elements of the operation of cyberspace, created the concern first in the companies and organizations themselves and by extension the competent shipping agencies, which already belatedly in the year 2016 and onwards started to set a legal, technical and more generally framework of disciplined practice to ensure the protection of companies and organizations. Vigilance and discipline are essential elements of safety at the preventive level. This article analyzes both the types of cyberattack and the practices followed to extinguish them. But what happens in the event that despite vigilance and discipline, the cyberattack will create damage or loss to the business, as cyber security to exist, is in a constant competition of speed and knowledge at the software level so as to bend what is called cyberattack.

As is easily understood, prevention does not constitute the complete security and restoration of companies and organizations, creating the need to cover the damage or loss that they will suffer in the event of such a risk. So the need for cyberattack insurance as an insurance risk in maritime transport is felt especially since the cyber risk has touched large sums of millions of dollars, creating damage and loss to big

giants like Moller Maersk and Cosco. The huge issue of the delimitation of the insurance risk is therefore transferred to the insurers, who, as analyzed in this paper, are called upon to solve the Platonic riddle of whether politicians should philosophize or philosophers should administer, as the specific of the grammatical interpretation of the terms of the insurance convention and the definition of risk is in stark contrast to the general and specific characterization of the abstract risk emanating from cyberspace, the elements of which are the illegality, the unclear mode of action of the cracker and the great surprise of his action due to the immediacy and speed that characterize the actions of the crackers. Below is analyzed the degree of willingness and reluctance of insurers to carry out cyber risk insurance and at what points they use exclusion clauses of the traditional type, clause 380, or its mutations, or replacing it with new innovative clauses that formulate the conditions of their application more precisely and better performance of the described elements relating to cyberspace and cyber risk. The marine transport insurance sector, especially since the implementation of the ISM code by the Maritime Transport Commission from 1-1-2021, is in a continuous process of assimilating the new situation in the insurance market, namely the pressure of the continuous and continuous demand for insurance of the cyber risk from companies that are characterized as major players in the global purchasing public. Cyber risk has not yet become autonomous as an insurance product in the marine market, distinguishing the reluctance of insurers to enter unknown paths that are difficult to assimilate. At the moment, an attempt is being made to integrate cyber risk insurance into traditional insurance products, i.e. the risks of piracy, war and others, with the predominant use of piracy insurance risk, but this practice does not fully cover what we mean by cyber risk, creating the need for cyber threat autonomy, something everyone hopes to see in the near future. The placements of major insurance groups, such as P&I Clubs, Lloyd's, are listed.

Finally, concerns are raised regarding the application of the basic principles governing the Act 1906 and 2015 that apply to marine insurance, namely the principle of utmost good faith, the proximate cause and that of guarantees, in which (principles) the data in relation to traditional practice, theory and jurisprudence change in the case of cyber risk, unfortunately, until today we do not have from the above three bodies decisions of English courts, institution and authority catalytic for there to be a well-trodden path to be followed by the private bodies, the latter trying and in the sense of, in many cases of forced agreement between insurers and insured, so that within the

framework of the common interests between the parties to the insurance there is the demand for insurance coverage of the cyber risk, in order to satisfy by extension the insurance in the cyber space.

Chapter 1. Cases of cyberattacks, The threat of the new age

1.1 Important Case Studies Related to Cyber Attacks and Cyber Security in Shipping

1.- MSC MEDITERRANEAN SHIPPING CO SA V GLENCORE INTERNATIONAL AG [2017] EWCA Civ 365, Court of Appeal (Civil Division), Lord Justice Lewison, Lord Justice Henderson and Sir Christopher Clarke, 24 May 2017.twoof three containers containing cobalt briquettes shipped under a bill of lading dated 21 May 2012werelost.Thiswas the 70th similar shipment, but the first to go missing. The shipper, Glencore, filed a claim against the carrier, MSC, for damages for breach of contract, deposition, and conversion. The cargo was transported from Fremantle to Antwerp on MSC Eugenia and transshipped to MSC Katrina. The bill of lading is ted Glencore as shipper and Steinweg of Antwerp as agent. The bill of lading was negotiable and the consignee field was filled in" to order". The bill of lading contained the following clause: "If this bill of lading is a negotiable (To order/of)bill of lading, one duly end or sed original copy of the bill of lading must be delivered by the merchant to the shipping company in exchange for the goods or delivery order" .In Antwerp, an electronic release system was introduced and used by the MSC. Under this system, no paper delivery order or release note was issued against the bill of lading; an "import pin code" was issued. Steinweg was familiar with the operation of this system and billed Glencore under the item "delivery note. "The judge ruled for Glencore ([2015] 2 Lloyd's Rep 508), holding that (1) the issuance of the PIN code amounted to constructive delivery, (2) the PIN code was a delivery order, (3) the release note was a delivery order, and (4) Glencore, by delivery of the69cargobeforeMSC also sought to amend its appeal to show that the cybersecurity issue caused a break in the chain of causation.

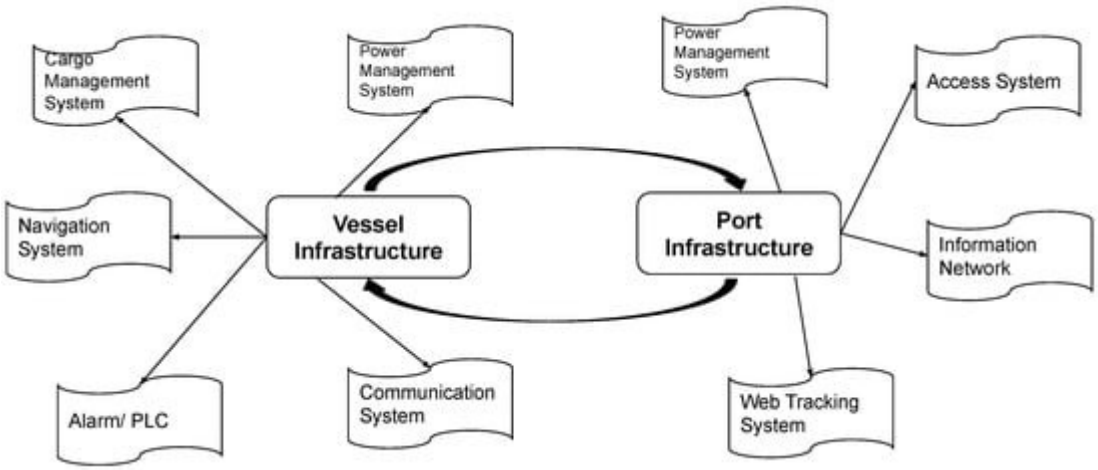
According to the view of theory and science, the case may not have resulted in the economic ruin of the affected parties, but it is rightly held to have raised several issues of general importance in connection with(a) electronic bills of lading and delivery orders, and (b) waiver and estoppel. In 2005, the Antwerp Port Authority introduced a new procedure called the Electronic Release System (ERS). Under this procedure, upon presentation of a bill of lading, the carrier provides a computer-

generated electronic number to the relevant consignee or its agent and the port terminal. These numbers are given in lieu of Delivery Orders or Release Notes, which are created through the port authority and are not visible to the carrier. The owner of the bill then presents the pin code to the terminal for delivery of the cargo. Usually, the pickup driver enters the pin code at the terminal. This system is not mandatory and is not used by all carriers using the port, but it was used in all 69 previous shipments of cobalt by MSC and Glencore's port agent, Steinweg. MSC will present the bill of lading (and payment of all outstanding charges) by means of a system of emailed release notes with pin codes. The trial court found that Glencore did not know at the time of shipping that Steinweg and MSC were using the ERS. He also found that the port agent did not have the authority to modify the contract of carriage. These two conclusions were not challenged on appeal. It held that MSC was liable for the mis delivery and that the release note, with or without the pin code, did not constitute a delivery order as required by the bill of lading, nor did it constitute a vessel delivery order within the meaning of Article 1.4 of the Carriage of Goods by Sea Act 1992. It also held that Glencore was not bar red from asserting strict performance for the 70th time by the actions of its agents who had accepted the modified procedure for the 69th time in the past. From the above, we conclude that the judge's decision, although correct as to the issues, did not resolve the issue of the safety of transactions using the ERS trading system, perhaps because he did not seek liability from those who violated that system.

2.- According to an article published on October 16, 2017 in the World Maritime News Staff, shortly after the major attack on the Colossus of the loan company A.P. Moller Maersk, hackers managed to gain access to computer systems of BW Group, and the latter confirmed this to World Maritime News. As disclosed, the cyber attack occurred in July 2017. They referred "*We had an unauthorized access some time back in July and actions have been taken to rectify the matter,"* as a spokesperson from BW Group said. "*Internal and external communications to customers and stakeholders were not impacted and it was business as usual with some inconveniences as we worked around planned system downtimes as our IT department, with the assistance of external consultants, reinforced our cybersecurity infrastructure,"* the spokesperson explained. The incident followed a large-scale cyber attack on Danish A.P. Moller-Maersk on June 27, which shut down IT systems across multiple sites and business units owned by the company. The

attack has cost the company up to USD 300 million. Julian Clark, Global Head of Shipping at Hill Dickinson, a commercial international law firm headquartered in Liverpool, UK, **clearly** explained that *"if a company as sophisticated as Maersk could be affected in such a dramatic way, requiring them to take two weeks to get all their systems back online, anyone and everyone is exposed."*Mr. Clark also said in an interview with World Maritime News that although cost is an important factor for shipping companies, the time has come where there needs to be a significant investment in cybersecurity measures**, thereby approaching the issue of internet security with more care and a sense of responsibility**.[1]

Figure 1. Vessel/port infrastructure.[2]



3.- Shipping firm Clarksons braces for data leak after refusing to pay hacker World's largest shipbroker follows large corporations including Deloitte, Yahoo and Equifax in falling victim to cyber-attack Shipping company Clarksons is bracing for a tranche of private data to be released, after refusing to pay a ransom to a hacker who staged a "criminal attack" on its computer systems. In a statement to the stock market, the world's largest shipbroker said it was working with specialist police and contacting customers who may have been affected after a "cybersecurity incident". "As soon as it was discovered, Clarksons took immediate steps to respond to and manage the incident," the company said. "Our initial investigations have shown the unauthorised access was gained via a single and isolated user account which has now been disabled." "Today, the person or persons behind the incident may release some data." Shares in Clarksons fell by more than 2% after the announcement, despite the company's insistence that the hack would not affect its ability to do business. The

[1] https://www.offshore-energy.biz/hackers-access-bw-groups-it-systems-countermeasures-undertaken/
[2] https://www.mdpi.com/2078-2489/13/1/22

shipbroker arranges charter ships to transport goods, as well as helping shipping companies raise finance and providing services such as logistics and equipment. Andi Case, the Clarksons chief executive, **after the result of the cyberattack, which is characterized as not insignificant, despite the initial indifference of the company**, said: "Issues of cybersecurity are at the forefront of many business agendas in today's digital and commercial landscape, and despite our extensive efforts we have suffered this criminal attack. "As you would rightly expect, we're working closely with specialist police teams and data security experts to do all we can to best understand the incident and what we can do to protect our clients now and in the future. "We hope that, in time, we can share the lessons learned with our clients to help stop them from becoming victims themselves. "In the meantime, I hope our clients understand that we would not be held to ransom by criminals, and I would like to sincerely apologise for any concern this incident may have understandably raised." Clarksons is just the latest company to be hit a major cyber-attack, joining a list that includes Uber, Deloitte, Yahoo, Equifax and extramarital affairs website Ashley Madison. "Clarksons would like to apologise to shareholders, clients and staff for any concerns this incident may raise," the company said. Since being hacked, Clarksons said it has consulted data security experts and is investing "heavily" to shore up its defences, amid a broader cybersecurity review. the cyber-attack comes a year after the company issued a profit warning, blaming a drop-off in global trade. **It is therefore another example of a cyberattack, which was initially judged to be insignificant or otherwise of small scope, but which ultimately led the company to take drastic measures of maximum security.**

4.- **According to another article[3] published on July 25, 2018 in the World Maritime News Staff, COSCO Shipping lines falls victim as it was hit to its internet connection within its offices in America.** As such, local email and network telephone were not working properly and the company decided to shut down the connections with other regions for further investigation. Based on the information released so far, the incident that took place on Tuesday, July 24, was described as a ransomware attack. The Chinese shipping and logistics company said that its vessels were not impacted and that its main business operation systems were performing stably. However, COSCO's terminal at the Port of Long Beach was affected. *"We are glad to inform you that we have taken effective measures. Except for above regions*

[3] https://www.offshore-energy.biz/cosco-shipping-lines-falls-victim-to-cyber-attack/

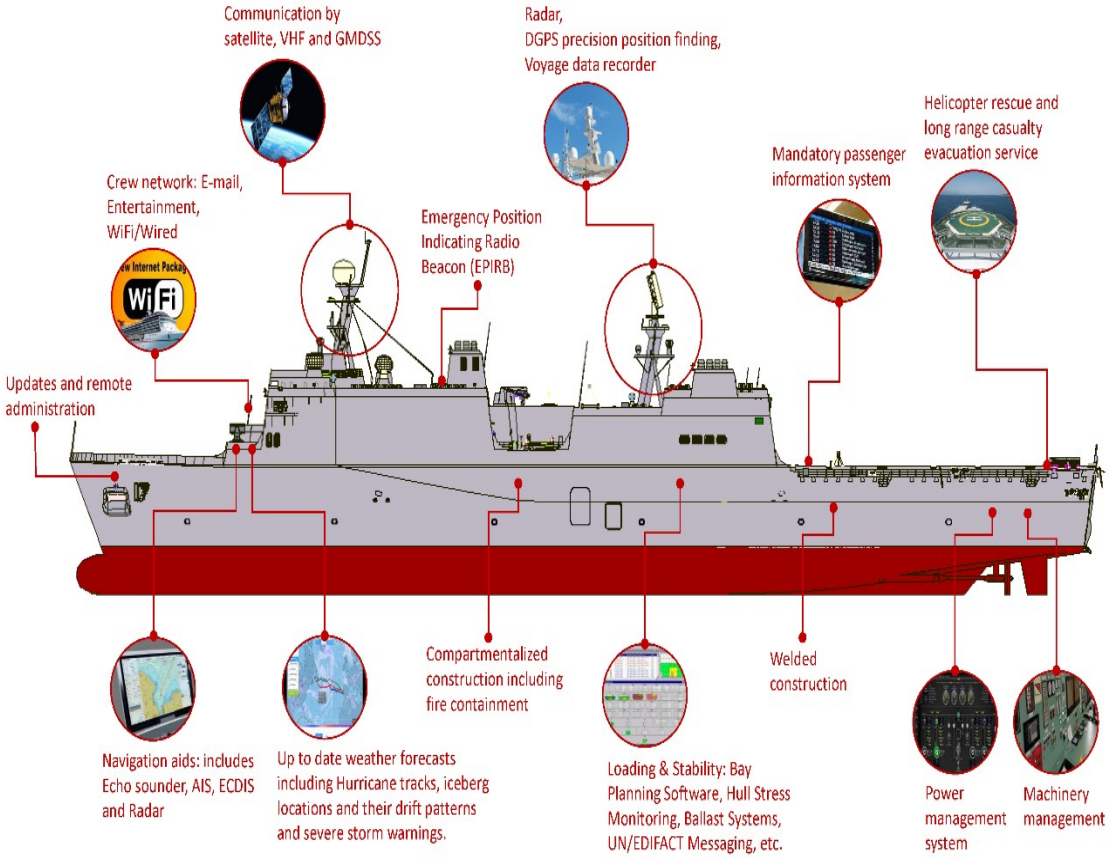
affected by the network problem, the business operation within all other regions will be recovered very soon. The business operations in the affected regions are still being carried out, and we are trying best to make a full and quick recovery. We will keep you updated of the latest progress through various channels," the company said. The latest attack is a stark reminder of the ever-growing threat from cyberattacks in the maritime world which is becoming increasingly dependent on digital technology. Even though the impact was not as severe as the one experienced by Maersk Group in June 2017, companies are encouraged to boost their cyber security if they want to avoid the scenario that cost Maersk around USD 300 million, **and all this because the risk of a cyberattack is now felt at an unsuspected time and every company can become a victim at any moment, a risk that no company wants to take**.

5.- **Throwback Attack: How NotPetya accidentally took down global shipping giant Maersk** DANIEL E. CAPANO SEPTEMBER 30, 2021. One of the most widespread and devastating cyberattacks of 2017 took place against global shipping giant Maersk. It began on a quiet afternoon in June, when a staff member began seeing messages informing him that the filesystem was being repaired, while others received messages that critical files had been encrypted.The encryption key required $300 in bit coins. The Maersk headquarters panicked. The entry system and phone network had been rendered useless by malware that was spreading rapidly within and outside the company network. By the end of the day, the network was so deeply disrupted that the company simply shut down. Maersk is a global shipping company that transports all kinds of goods in 76 ports and more than 800 vessels worldwide, and is responsible for about one-fifth of global trade. This entire company was brought to its knees by a mysterious malware that spread to all Maersk locations around the world. **The example of this company is now a landmark for every movement of companies, governments and groups of people that are related to cyber security, not only at a real and legal level but also at the level of coverage of cyberattacks as a risk by insurance companies.**

Figure 2. Automation systems for modern and autonomous ship

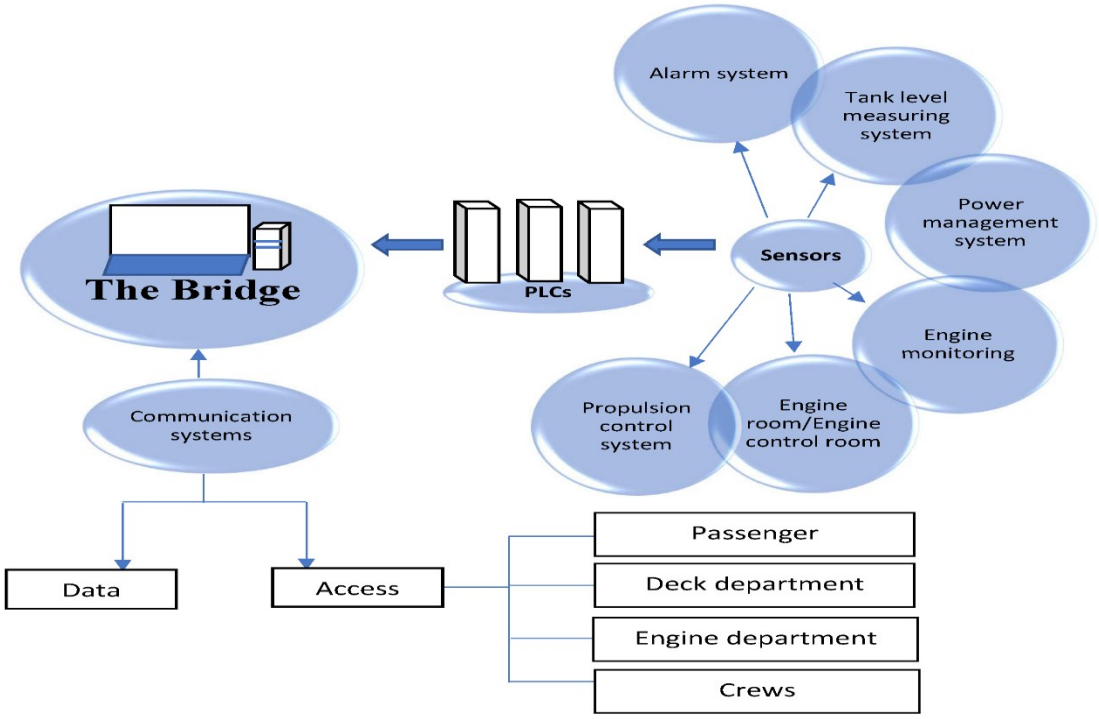
s

4



[4] https://www.mdpi.com/2673-8732/2/1/9

Figure 3. Vessel elements interaction.



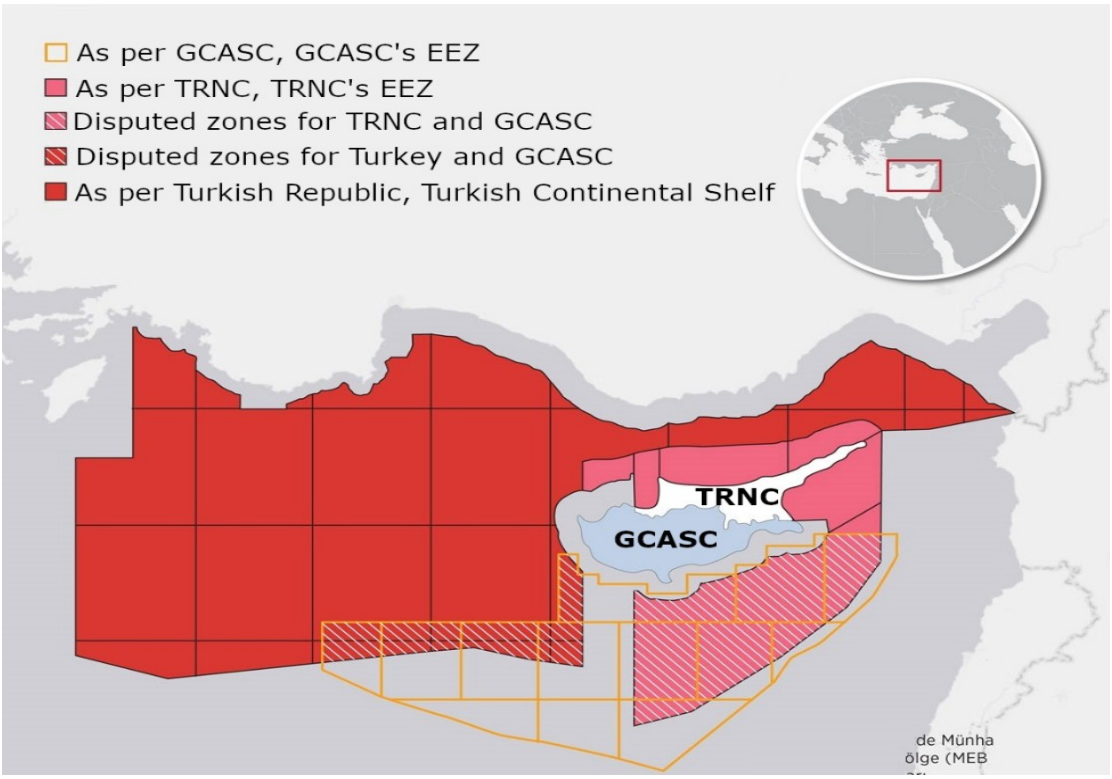
1.2 Cases of State Involvement in a Cyber Attack [5]

[5] Allegations of State-sponsored Cyberattacks There are five countries suspected of state-sponsored cyberattacks against the maritime industry. The suspects are China, Iran, North Korea, Russia, and Turkey.3.1. China In April 2012, the Danish Maritime Administration suffered a significant cyberattack, but the cyberattack was not publicly announced until September 2014 (Cyber Keel 2014). This targeted attack demonstrates spear phishing techniques. After this event, and after the 2017cyberattack that caused significant damage to Maersk, one of the world's leading shipping companies, the Danish government took note and took steps to create an official cyber security department. Thus, in June 2018, the Danish Maritime Authority established the Danish Maritime Cybersecurity Unit. The unit, which provides services to players in the Danish maritime sector, also organizes specialized workshops and conferences on cybersecurity, especially for the maritime sector.3.2. Iran The Port of San Diego in the United States suffered a cyberattack on September 25, 2018 (I Mar EST 2018); the incident, identified as a ransomware attack named SamSam, affectedmorethan200 victims, including hospitals, municipalities, and public institutions, as well as the port itself,causing$30 million in economic damage (U.S. Department of Justice 2018).The attack was orchestrated by two Iranians who demanded a ransom in Bitcoin.3.3. North Korea In April 2016, South Korea announced thatapproximately280 vessels had been hit by a GPS jamming attack, forcing the affected ships to return to port (Graham 2017). South Korea claimed that the attack was orchestrated by North Korea. However, North Korea denied this claim (Saul 2017). (Cozzens 2020).3.4. Russia

Five countries, China, Iran, North Korea, Russia and Turkey have so far been named as suspects in cyberattacks on the shipping industry. Very briefly it is stated that a) in April 2012 the influence of Danish companies was detected through malware from a pdf with which confidential information of shipping companies was obtained, which later in September 2014 was revealed to come from China b) on 25-9-2018 , a cyberattack using the ransomware attack method, named samsam, affected more than 200 companies and organizations in the port of San Diego in America, which attack was discovered by the FBI c) in April 2016 South Korea announced the GPS attack to approximately 280 ships affected by the GPS jamming method and forced to return all to port d) the an incident that was later attributed to a Russian ship in the Gulf of Novorossiysk affected the movement of 20 ships and e) the well-known case of continuous and multiple cyber-attacks on GPS in the area of the Cyprus-Israel EEZ which the state of Turkey does not recognize until today. **Finally, the reference to cyber-attacks has been used as a weapon to claim land rights, sea "plots", like that of Leviathan, concerning countries.**

OnJune22,2017, a vessel off the Novorossiysk-Russian coaster ported to the U.S. Coast Guard Navigation Center about a GPS malfunction. According to the report, the vessel's GPS was showing an incorrect position, and the issue affected more than 20 other vessels in the area. (Humphreys 2017; Goward 2017).3.5. Turkey According to studies, numerous hydrocarbon reserves may exist in the Mediterranean Sea around the island of Cyprus (Faustmann et al.) In this sense, onJanuary26,2007, the Greek Cypriot Southern Administration (GCASC) separated the area identified as its Exclusive Economic Zone(EEZ) into 13 zones and began licensing these zones to oil exploration companies(Arıdemir and Allı 2019). These companies thus gained the privilege of exploring for hydrocarbons in the licensed areas. However, some of the identified areas overlap with the Turkish continental shelf and the EEZ of the Turkish Republic of Northern Cyprus (TRNC). (Yilmaz 2019).

Figure 4. The case of the Cyprus-Israel EEZ and the Turkish position



Chapter 2. The way cyberattack functions

2.1 Types of Cyber Attack

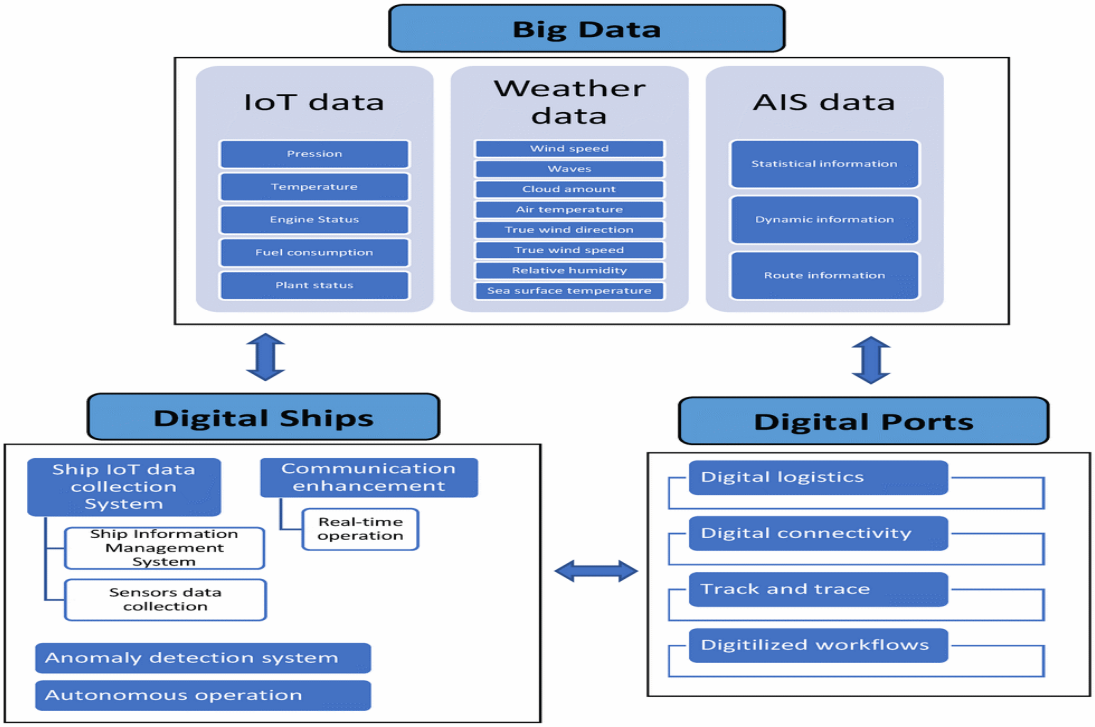
The most common forms of cyber-attacks are: a) Ransomware, i.e. a type of malicious software according to which the natural person is blackmailed whose sensitive personal data is either withheld against their will or there is a threat of their publication in order to obtain a financial benefit from on the part of the perpetrator, b) Phishing, i.e. a way of extracting information ("fishing") from the target - the victim of sensitive personal information, common in the cases of bank account details for the financial benefit of the perpetrator either by using threats or directly "emptying" accounts, c) Wi-Fi, i.e. attacking data held and maintained on devices connected to a Wi-Fi network, with the perpetrator extracting sensitive personal information of the

user of these devices or by introducing malicious software into them with the aim of either financial gain or creating defamation of that person, d) DDoS (Distributive Denial of Service), i.e. an attack with the aim of creating a form of electronic system source, the aim of which is to crash a website temporarily or permanently.

A cyber-attack is any malicious and premeditated action by means of the use of the computer and the internet either by an individual action of a natural person or by a collective action of persons, organized or not, in a legal entity, with the aim of violating software systems with the aim of destroying data or extracting information that exists and is kept in this software system and is the property of another natural or legal person. The cyberattack is usually characterized by a) the suddenness of the action of the perpetrator of the attack as the speeds that develop are high, b) the lack of borders as we think of them in their traditional form, borders of states, continents, administrative entities, as the the internet is a separate world that operates with different rules and having different borders, c) the inadequacy of monitoring cyberattacks in their entirety as not all are recorded, d) the immediacy of every action via computer as the attack can take place in unsuspecting time and at the push of a button, e) the difficulty of finding the identity of the person attacking. As a result of the characteristics of a cyberattack, it is very difficult to identify both the cyberattacks and the persons who commit them, while in this way the core of the right of personality of the affected persons is laid, and at the same time they are violated depending on the country of origin of the natural or legal person , constitutionally guaranteed human rights, rights recorded and guaranteed in the European Convention on Human Rights, in the Charter of Fundamental Rights of the European Union. Bearing in mind that the internet space and what is defined as cyberspace in the modern era is an essential element for the modern man to be able to develop socially, economically and exist as an entity, as we live in the age of information which moves the economy on a global level , the state and transnational initiatives, organizations of all kinds and ultimately affects the development of the personality of each person, who is communal as a unit with the whole, as it is characterized by the word and concept of globalization. By extension, the need for the existence of a secure cyberspace is being perceived day by day. Everything points to the intention of companies, especially those with large financial interests at stake, to insure it (cyberspace) with classic marine insurance contracts, having as the insurable risk that of cyberattacks.

The need for accuracy and speed as necessary features to achieve the goals of a shipping company or business in the modern era creates further and by extension the need for the ever-increasing use of the computer and the internet. The information that used to be transmitted by telephone, telegraph, traditional mail, at this moment has been replaced by the use of e-mail, the search of Google and other websites, the data clouds (Dropbox, Microsoft etc.), the use of browsers, and generally of the internet as it functions and acts in the so-called cyberspace. As in all industries but also in

Figure 5. Digitalisation of maritime industry.[6]



general as it happens to all internet users, so in shipping companies are victims and sometimes perpetrators of what we call cyber security in the modern era. Some examples of devices using the internet are AIS, which according to SOLAS Regulation 19 Chapter 5 is required to be used mainly for broadcasting SOS and for receiving or transmitting data relating to any ship of tonnage equal to or greater than 300 tons operating on international routes, for any bulk cargo ship of 500 tons or more, and for passenger ships regardless of size. The fact that this device was not designed in such a way as to be protected from crackers, and its operating error rate created and creates fertile ground for the aforementioned crackers to breach the data and information they were transmitting, as a result of which the safe international or

[6] https://www.mdpi.com/2078-2489/13/1/22

non-navigability creating great financial burdens and even disasters for shipping companies.

Figure 6. Ship Information System architecture[7]

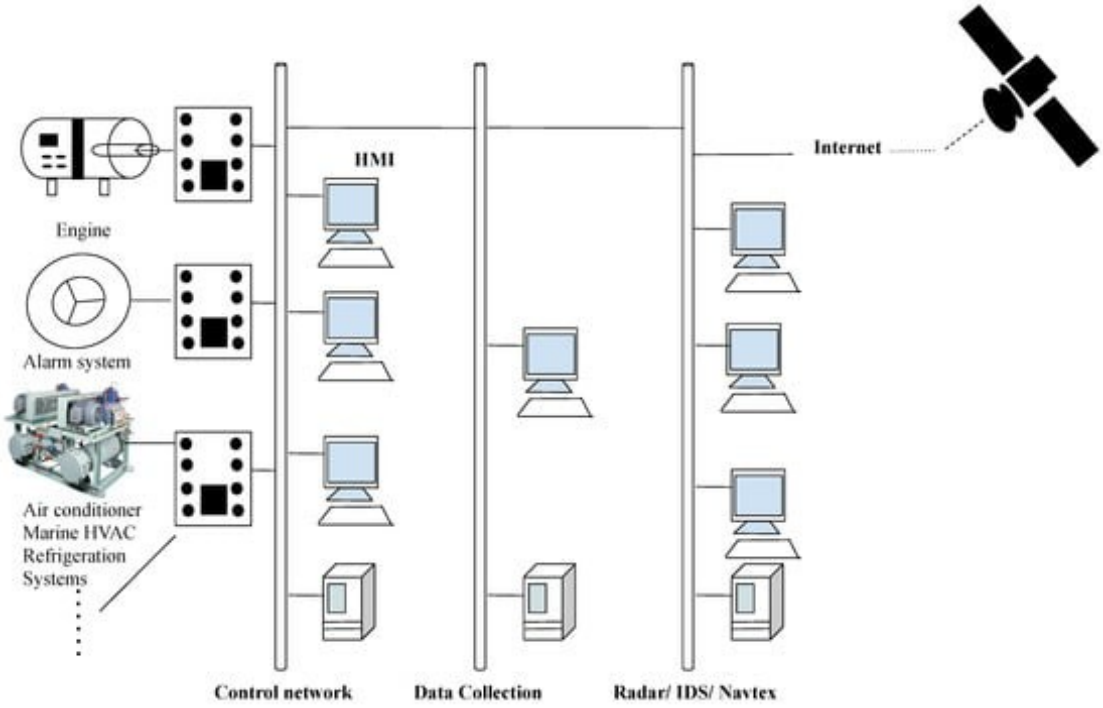
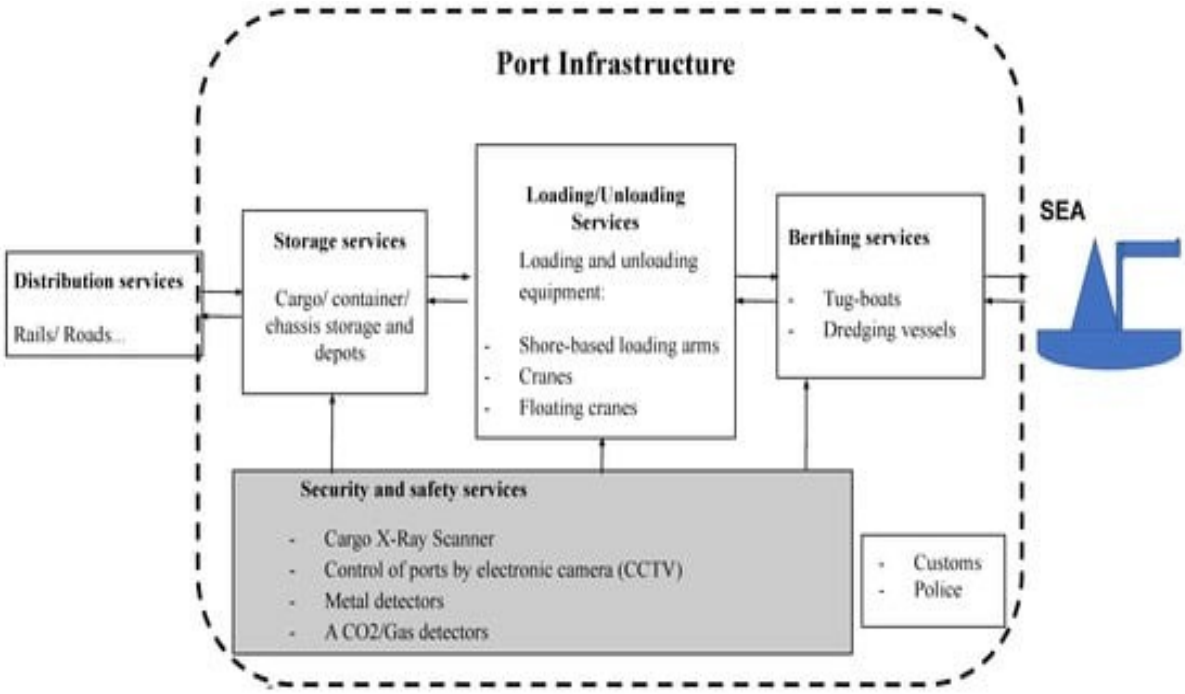


Figure 7. Port architecture[8]

[7] https://www.mdpi.com/2078-2489/13/1/22
[8] https://www.mdpi.com/2078-2489/13/1/22



Some of the basic and common types of cyberattacks concerning shipping, whether it targets the shipping company or any ship owned or owned by a shipping company or company, are: a) Brute Force, i.e. the use of different combinations of passwords with the aim of "breaking" user passwords, b) Social Engineering, i.e. the attempt to erode the security protocol used by the company which is achieved by manipulating its human resources, c) Denial of Service, i.e. the bombardment of a network by many users with aimed at removing legitimate and authorized users from using it, d) Subverting the supply chain, i.e. the damage to the supply chain of the company or the ship as a result of the attack on equipment, software or supporting services, e) Spear Phising, i.e. the Inflow of malware via email messages when the target persons are specific, while with the use of tools such as scanning, water holing, malware and phising, companies are attacked when the perpetrator does not have a specific goal but in fact by using them they discover the pathogenic characteristics or elements of this (company) which he tries then to exploit them. The ingenuity of the perpetrators of the cyberattack has caused a great problem, which is assisted by the continuous technological evolution and development.

Typical characteristics of cyber threats (Bodeau et al. 2010) Level Typical threat actor Typical threat actor intent 1) Cyber vandalism, hackers, taggers, "script kiddies,"small disgruntled group of above Small disgruntled group of organizations or types of organizations affected (e.g., specific departments or entire federal

government) to disrupt and embarrass. Individuals or small loosely affiliated groups, political or ideological activists, terrorists, domestic insiders, industrial spies, spammers Obtaining vital information and/or usurping or interfering with the business or mission functions of an organization for profit or ideology Surveillance National government agencies, patriotic hacker groups, advanced terrorist groups, professional organized crime firms. Increase knowledge of general infrastructure, plant seeds for future attacks, obtain or modify specific information, and/or disrupt cyber resources, especially those related to mission or intelligence types 4) Cyber sabotage, espionage Specialized intelligence or military service operatives Obtain specific high-value information to undermine or sabotage critical aspects of a mission, program, or enterprise, or to put the mina position to do so in the future 5) Cyberconflict, warfare 5) Cyber Conflict, War Significantly undermine or disrupt the mission, intelligence and/or infrastructure of a national military (possibly with intelligence services support), highly sophisticated and capable in surgent or terrorist group organization.

2.2 The position of the agencies on the issue of the threat of cyberattacks

The international concern caused by the headache of cyber-attacks in the shipping sector has triggered the adoption of legislative measures by the competent bodies responsible for the smooth operation of transport and the security of international trade. In this way, the uniform treatment of the problem described above and the effectiveness of limiting it to tolerable frameworks by the companies are achieved. Critical are the actions taken by the International Maritime Organization, the Maritime Safety Committee, as well as a collective cooperation of a large part of the shipping agencies, consisting among others of international shipping organizations, which moved and continue to move within the accepted frameworks and the spirit of the legislative directives of the International Maritime Organization.

2.2.1 IMO's contribution to addressing cybersecurity risk

As early as June 2016, the International Maritime Organization, recognizing that cyber-attacks are now a threat to the shipping industry, publishes “Interim Guidelines on Maritime Cyber Risk Management”[9] creating, on the one hand, the early stage for the development of a single strategy to deal with the risk in order to ensure of cyber security in maritime transport and trade, on the one hand, this action marked the departure of the institutional bodies and shipping itself from the lax response to cyberattack in the practice of the past. Then, on July 5 2017, a full

[9] MSC.1/Circ.1526

planning text for dealing with relevant situations and threats follows from the same organization, "Guidelines on Maritime Cyber Risk'"[10], which is influenced both by the above-mentioned " Interim Guidelines on Maritime Cyber Risk Management" and by a legislative text of the 98th session of Maritime Safety Commission in the United States of America of April 4, 2017, "'Measures to Enhance Maritime Security "[11], focused on the theme of the necessity of technology for the proper functioning of systems, which will provide safety to navigation and the marine environment, highlighting the great importance for the existence of an adequate and effective framework for the management of cyberattacks, the so-called "cyber risk management"[12], keeping its position as an institution of international shipping, not entering into the creation of a list of case studies, but providing only general directions. It should be noted that the latest applicable Magna Carta, after pointing out that insufficient cyber security endangers the safety of the ship itself, i.e. human resources and property, proceeds with the proposal of risk management at a global level, which includes risks in cyberspace, dealing with the problem of cyberattacks with a holistic approach[13], as cyberspace is not a detached part of the company, but is taken into account as an integral part of the whole. As such, the International Maritime Organization took the initiative to lay the foundations for the protection of companies and shipping from cyber-attacks, which other bodies have imitated productively.

2.2.2 The position of the Maritime Security Committee

The pioneering and innovative body of the International Maritime Organization in the context of cooperation to deal with cyberattacks is followed by the Maritime Security Committee, which, guided by the "Interim Guidelines on

[10] MSC-FAL.1/Circ.3

[11] MSC-FAL.1/Circ.3

[12] Cyber risk management: the process of identifying, analyzing, assessing, communicating, and accepting, transferring, or mitigating cyber-related risks to an acceptable level by considering the costs and benefits of actions taken by stakeholders (see "Guidelines for Shipboard Cyber Security "Version 3-Annex 4: Glossary).(See also: Guidelines for Shipboard Cyber Security,Version3-Annex4: Glossary).See also: Guidelines for Cyber Security of Ships,4th Edition. Since ship sand shipping are vulnerable to cyberattacks, the industry has joined forces to develop the "Guidelines for Cyber Security on Ships "based on high-level principles: establishing awareness of the safety, security, and commercial risks arising from a lack of cyber security measures, protecting ships' Protection of IT infrastructure and connected equipment, systems of user authentication and authorization to ensure proper access to necessary information, protection of data used in the ship environment, ensuring proper protection of information based on its confidentiality, control of IT users to ensure they have only authorized access and rights to information Control of IT users to ensure that they only have access to and rights to authorized information; control of communications between ship and shore; development and implementation of cyber incident response plans based on risk assessments.

[13] https://safety4sea.com/wp-content/uploads/ISM-Code/ISM&20Code%202015%20with%20cover.pdf

Maritime Cyber Risk Management" and the "Guidelines on Maritime Cyber Risk" mentioned above adopts on June 16, 2017 the resolution "Maritime Cyber Risk Management in Safety Management Systems"[14]. Accordingly, cyber risk management is linked to the objectives and requirements of the International Safety Management Code (ISM code) and in this way the former is integrated into the already existing safety management system (Safety Management Systems - SMS). By choosing this indirect way, cyber security risk management has become mandatory for all shipping companies at a universal level. Consequently, cyber security is addressed at a holistic level of overall security management, which companies also owe and are obliged to initially comply with said resolution by verifying it with a special document of compliance (DOC), which is implemented from 1-1-2021 onwards. As of this date, the companies face sanctions at an administrative and criminal level. This means that each company must cumulatively implement: a) the definition of a specific duty code with specific responsibilities and obligations of the staff[15], whether they operate on land or at sea. This means that the company, in the context of familiarizing the staff with the risks inherent in cyberspace, must provide for their training in cases of cyberthreats, which are now an everyday occurrence. According to the above-mentioned responsibilities, the company must carry out proper planning to cover the needs of preparedness in cases of dealing with and managing any crisis, while at the same time the staff should also follow the specific planning, determining exactly what to do in such cases. The goal is a safe sailing ship, the safety of the ship and of the company itself, including all members of the company from the top to the bottom. Unfortunately, a survey carried out in the year 2018 had the result of sampling that approximately 50% of the participants in the survey have the guarantees to respond in cases of cyber threats. b) The identification of the gaps in the operation of the ship and the company, as well as the determination of the pathogenic elements of the operation system of the above as vulnerable points to be attacked with the far-reaching consequence of disrupting their operation. c) The assessment and evaluation of the type and size of each risk, based on which the above-mentioned emergency planning exists to mitigate and shrink the potential attack, or prevent the potential attack attempt. The purpose of this element is to enable the company to operate without having to stop any of its operations.

[14] MSC.428{98)

[15] see the 8th section of the ISM code “EMERGENCY PREPAREDNESS”

From the application of the said ISM code, further questions arise such as: whether an insurance company will take notice of the cyberattack for the insurance of a ship or company with an insurance risk, the application of the above code , if in this case the staff's familiarity with dealing with these risks will be taken into account and in general if the company's readiness to deal with the insured cyberattack will be taken into account.

2.2.3 The coordination with the IMO of the international shipping bodies

Simultaneously with the movement of the International Maritime Organization, which was followed by the Maritime Safety Committee in the above-mentioned resolution “Maritime Cyber Risk Management in Safety Management Systems”, against in the year 2017 the main international shipping organizations reissue the third edition of “The Guidelines on Cyber Security Onboard Ships”, which is a further in-depth look at the issue of cybersecurity providing detailed analytical risk management guidelines. It is also one of the key references of the fourth section of “Guidelines on Maritime Cyber Risk Management”, to find the detailed management instructions mentioned above cyber threat. This guide is of an advisory nature without having the mandatory nature as mentioned in the “Interim Guidelines on Maritime Cyber Risk Management” and the “Maritime Cyber Risk Management in Safety Management Systems”. Although it is not mandatory to follow these guidelines almost all involved with the Shipping Industry follow it universally and fully accept it. As well the usefulness of this guide lies in the fact that it is the core of the most current issue for the implementation and maintenance of cyber risk management which is used for the first time by shipping operators who are engaged at a professional level.

The comprehensive steps in this guide are identifying risks, identifying vulnerabilities, assessing risk exposure, developing protection and mitigation measures, creating plans to minimize cyber risks to a potential threat, and finally planning response and remediation from potential shock incidents cyber security. In addition, this guide leads the user to a deeper understanding of the multifaceted dimension of a cyberattack, as using it as a tool and means, he can easily determine the type of each attack, the type of the perpetrator, his possible motives, while also understanding the vulnerabilities points of the system that his company operates, and finally through this he can determine the damage and loss, positive, reserve and lost profits, in case the risk in question is covered by marine insurance.

Since the digital revolution has already been introduced in the maritime industry, the need for cyber security creates the further need for the continuous updating, supplementing, correcting and generally evolving of risk management guides. In October 2020, the International Chamber of Shipping and BIMCO together with the publishing house Witherby issue the “Cyber Security Workbook for On Board Ship Use”, which is an updated handbook to previous editions of cyber risk management guides. Thus, from the senior management of the ship to the junior members of the crew, they are trained in the management of the risks that may occur with the basic steps of detection, response and ultimately recovery in the optimal time, developing useful practices so that the safe sailing is not suspended at all and generally the sea transport process.

2.2.4 The use of the International Organization for Standardization and International Electrotechnical Commission Directive and the EU GDPR Regulation by the IMO

Another useful tool that the International Maritime Organization refers companies to as an additional weapon in their quiver is the "ISO/IEC 27001 standard on Information technology”, which was established by International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), laying the foundation for an archetypal information security management system (Information Security Management System – ISMS). The sensitive personal data of the companies, i.e. information included in the circle of the principles of privacy and confidentiality. Companies from the moment they apply the instructions of this manual to the letter and receive the necessary certification from the competent bodies are considered to have the guarantees of the maximum standards for the security of the personal data information of the company's personnel and the ship.

In parallel with the International Maritime Organization, the European Union itself, realizing the systematic attacks in the information field and the fact that cyber security is a necessity for the protection of personal data, sensitive or not, in April 2016 establishes the Protection Regulation[16], and leaving a window of two years for businesses, companies and all public or private sector legal entities and organizations to comply with it. On May 25, 2018, this regulation came into effect. All the above legal entities had to meet the minimum standards of the Regulation regarding the

[16] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016

protection of personal data. A large portion of the compliance was occupied by the protection of those in the internet space and in general in what is called cyberspace. By extension, cyber security becomes vital under this Regulation. The Regulation in question is characterized by great rigor, as the European Union, in its effort to guarantee the protection of personal data and the right to the freedom to develop the personality, sets the model for the protection of these (personal data) which the legal authorities must follow, otherwise the fines[17] they are going to face are huge. The shipping industry is also included within the framework of compliance imposed by this Regulation.

In addition to the special compliance planning that the companies in question must follow, such as flow mapping, gap analysis, obtaining consent from natural persons is also a key element in order to observe and maintain or process the information concerning them by the company , since the latter has previously notified them of the manner in which they will be protected with the following privacy policy and the terms of use and operation of the company, which should be fully adapted to the Regulation in question.

It is also worth noting that compliance does not only concern companies that have their headquarters in EU Member States, but concerns any action by a company or not that is carried out within the territory of the EU or generally concerns a European Citizen. This element concerns shipping companies par excellence, which enter and leave the European maritime space, or not, using either European ports or European waters (waters of its Member States).

Cruise shipping companies are the ones who face the greatest risk of sanctions from the European Union as they daily enter the process of accepting personal data of the large number of passengers, i.e. natural persons, that they manage for their transportation. In the event of a cyberattack, if the company has not complied with the above European Regulation, and a cracker intercepts data, in addition to the latter, the company in question bears great responsibility for not taking the necessary measures in its security systems. The European Union has always operated and continues to operate with a view to prevention and not repression. This, as its policy, also raises

[17] According to article 83 §5 of the European Regulation 2016/679 "Violations of the following provisions attract, in accordance with paragraph 2, administrative fines of up to 20,000,000 euros or in the case of companies, up to 4% of the total global annual turnover of the previous financial year, depending on which is higher", indicating an order of magnitude of the severity of the administrative sanctions that the violation of the provisions of the said Regulation entails.

the quality of the product, which bears the origin of this (product) from the European Union, in relation to products - goods from third countries.

Despite the fact that the European Regulation pushes companies to comply for the protection of personal data, and cyber security is a prerequisite, and all this within a strict legal framework that foresees an order of magnitude of large penalties, its application in several cases it is either economically unprofitable or technologically incompatible, as the development in technology as mentioned above is a positive factor in preventing cyberattacks but at the same time increases the risk of their existence with the aim of disrupting cyber security. The result of this is the lack of a stable basis at a legal and factual level on which to base the concept of marine insurance in the event of an event corresponding to a cyber-attack risk covered by an insurance contract.

Chapter 3. The need for insurance in cases of cyber risk

Insurance companies, reinsurance companies and P&I Clubs have contributed in various ways to the understanding of the concept of cyber risk, with the aim of being able to further include it as an insurance risk in marine insurances. Examples of the meaningful approach to this risk from the point of view of the insurance companies, indicatively and not exclusively, are the following:

NORTH P&I club[18]: A cyber risk can be the failure of a GPS receiver located on the ship, due to some equipment failure, which can extend to the other systems of the ship as a result of which it cannot function properly or even be taken over by malicious third parties (hacking).

UK P&I club[19]: Cyber risk is defined as the risk of loss or damage or disruption of access to electronic systems and technological networks.

JAPAN P&I club[20]: Cyber risk is defined as a potential factor, which may cause problems or affect the IT system and which may even cause, in addition to dysfunction in the performance of tasks and financial disaster to the company. Cyber risk stems from both external and internal factors.

BIMCO, CLIA, ICS, INTERCARGO, INTERMANAGER, INTERTANKO, IUMI, OCIMF and WORLD SHIPPING COUNCIL[21]: A cyberattack is any type of offensive ploy, which targets IT and OT systems, computer networks or personal

[18] see Cyber Risks in Shipping - The North of England P&I Association (July 2017).
[19] see Cyber Risks and P&I insurance - UK P&I club Q&A document (March 2018).
[20] see P&I Loss Prevention Bulletin - Japan P&I club (Vol.42, May 2018).
[21] see The Guidelines on Cyber Security on board ships Version 3 - Annex 4: Glossary.

devices of employees and seeks to destroy or gain access to the systems and data of the company and the ship.

In rough lines, these definitions converge in that they approach the concept of cyber risk as a risk included in the insurance risk category of piracy, with the distinction that it takes place in cyberspace. Furthermore, the impact of the cyberattack constitutes a second element that needs to be determined in order to be the subject of insurance, that is the possible losses or damages that follow the event, that is for example the damage that may result from the loss of data, the temporary suspension of critical parts of the insured company, etc.

The legal framework of marine insurance is illustrated in the traditional and widely accepted marine insurance act 1906, which came into force on 01-01-1907, codifying the then existing jurisprudence that had been recorded until then in conjunction with the reformation of it by the marine insurance act 2015. This legal framework established the basic principles of marine insurance at a global level. Section one of the Marine Insurance Act 1906 defines marine insurance as "A contract of marine insurance (that) is a contract by which the insurer undertakes to indemnify the insured, in the manner and to the extent agreed upon, against marine losses, that is, of the damages that take place during the maritime adventure". Further in article 5 of the marine insurance act 1906 it is defined what the insurable interest is and specifically in article 5 paragraph 1 of this it is defined that "according to the provisions of this legislative act, anyone who has an interest in a maritime shipment has an insurable interest". And in paragraph 2 of the same article it is clarified that "a person has an interest in the maritime shipment when he is in a legal or bona fide relationship with the shipment or the insurable property at risk and therefore can benefit from the safe or due arrival of the insurable property or be harmed by its loss, damage or detention or may be held liable in relation to it".

From the combination of the above mentioned provisions it follows that in order for cyber risk insurance to be able to exist in a marine insurance contract, these provisions should be interpreted expansively, and the elements of traditional insurance should be matched with the new data of cyber risk, and specifically, the cyber risk insurance should cumulatively bring the three main characteristics of a valid contract in marine insurance, namely its economic value, the legality of the insurance contract and the real insurable interest. In particular, the financial valuation of the interest in the insurance contract should be possible, as it concerns an

indemnity contract, while at the same time this interest should not be illegal because otherwise it will suffer from invalidity, while at the same time the interest should be based on facts and facts that can be proven. All these elements when including the insurance risk of the cyberattack by interpretation should be present for the insurance contract, which insures the cyber risk, to be valid.

3.1 The three main principles govern traditional insurances and the problem of their application in cyber risk cases

Furthermore, a valid marine insurance should be inspired by the three basic principles, those of utmost good faith, the theory of proximate cause (causa proxima) and guarantees. These three principles are summarized below for a better understanding of the principles that will also apply to the insurance risk of the cyberattack so that we can refer to a valid insurance contract.

According to article 17 of the act of 1906 "A contract of marine insurance is a contract based upon the utmost good faith, and, if the utmost good faith be not observed by either party, the contract maybe avoided by the other party". Below will be the analysis of these three principles which concern the traditional insurance contract, but since the cyberattack as an insurance risk is included in marine insurance in the manner described above, their brief analysis is considered necessary in the context of the deeper understanding of the insurance risk in question.

This article, enshrining the principle of supreme good faith on which all marine insurance contracts are based, incorporates the ancient doctrine of uberrimae fidei, according to which regardless of the insured risk and the object of the insurance, this principle must exist and good faith and good morals must be observed by all contracting parties throughout the duration of this contract. In fact, this principle should also exist during the negotiations, when it is concluded, but also in the cases of its interpretation and ultimately its execution. Although this principle is observed equally and equally by both parties, the insured in most cases should prove that it is active, so that the insurer has the obligation to accept the same insurance policy, as otherwise the the latter will be able to activate his claim that he is not bound by the insurance contract, with the result that the insured guilty of the violation on his part of this principle loses the right to compensation when the proven existence of the insurance risk. The supreme good faith in rough lines gives birth to the obligation of the insured to disclose to his insurer before the validation of the insurance contract all the information which the insurer should take into account, in order to accept or not

the coverage of each insurance risk. All this based on the presumption of what reaction the average prudent insurer would have in the event that he possessed the information that the insured concealed from him regarding the conclusion of the above contract. It should be noted that according to article 21 paragraph 2 of the act 1906 after its amendment by the marine insurance act 2015, the duty of utmost good faith is modified by the introduction of the fair presentation of the risk, which nevertheless brings about the same results mentioned above. As is easily understood, the principle of supreme good faith mainly favors the insurer who, by definition, relies exclusively on the information provided by the policyholder, and on the basis of which the contract is drawn up, assuming the truth of this information in a spirit of trust. This trust is covered by the veil of the authority in question, otherwise this authority functions as a clause with the very essence of the insurance contract at stake. In the case of marine cyber risk insurance, the application of the principle of supreme good faith is considered problematic firstly because the insured cannot know himself from the start and then transfer to the insurer all the information concerning cyber security, with the result that for technical reasons the drafting of the terms of the contract to be unsafe, and in my view entering into a contract in which the insured appears to have the intention of providing any information he has about cyber security, but he himself may not provide any information to the insurer, and this should work to the benefit of the latter in the event that he activates the non-acceptance clause of the insurance contract, thus falsifying or falsifying the very principle of utmost good faith, for reasons that do not in principle concern the good faith of the insured. Despite this, today the information that the insured is required to provide to the insurer has been delimited so that it is considered that the former adheres to the principle of the highest good faith in the case of insurance against cyber-attacks, and this concerns the information of the electronic system, electronic device, communication device, navigation, etc., as well as any other information related to their operation. In this context, knowledge of how cyberspace works, cyber security and cyberattacks is a two-faceted problem. On the one hand, the insured who, based on this principle, has the obligation to convey accurate information, and in many cases of great and difficult to understand detail and composition, due to the complexity of IT issues, presuppose great and special training and familiarity in this field. On the other hand, the insurer should possess the same training and familiarity to digest this information and be able to record the complexity and detail of this

information on a piece of paper, so that the ratio of this principle, i.e. the equality of the burden of complying with the principle in question has substance. The last two-fold problem is mitigated by the above-mentioned resolution of the international code of safe management with the title "Maritime Cyber Risk Management in Safety Management System". Its implementation is expected to greatly modify the map of marine insurance with insurance risk the cyberattack. It is worth noting that the rapid increase in telecommuting due to the pandemic and the explosion of digital transformation, has decisively transformed the demand for insurance with covered insurance risk cyberattack in almost all industries. A recent study by the Security Certification Organization, ICS, shows that job vacancies for cybersecurity professionals exceeded 4 million in the year 2020.

According to section 55(1) of 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.". According to this article, the principle of the proximate cause is formulated, without specifying the way in which it is found. The cause is most often obvious, obvious and inextricably linked to the cause, but other times it is the subject of study and work to find the so-called causal link between the actual event and the risk. In this way a question arises when the marine insurance contract, covering only specific risks, which are precisely defined in it and are the object of the insurance, does not include other risks not contained in it. Thus, if the loss or damage is the consequence of a risk not included in the insurance policy, the insurer is not obliged to cover the damage suffered by the insured. Important under the terms of civil law, as in this case, is the existence of the above-mentioned causal link between the occurrence of the damage and the damaging incident that took place or otherwise as briefly stated the relationship between the cause and the causative, establishing the very theory of proximate cause analyzed in this section. In this case, the beneficiary of the compensation, i.e. the insured, as in any other case of asserting a claim of a civil nature, bears the burden of proof. Likewise, the insured must prove the existence of a causal connection between the cause of the loss and the insured risk, which is mentioned in the insurance contract.

While the definition of causation is easy to understand in theory, the case study case study develops a complexity in its practical application, as identifying the actual cause that caused the incident in a number of marine insurance examples is not

an easy task as it cannot listed in one or two causes, but by a combination of applicants, many times not demarcated among themselves, these causes creating insurance risks which are very likely not all contained in the insurance policy, putting at stake the claimed result as it is extension at stake whether the risk ultimately exists in the concluded contract or not. This is not often found in marine and marine insurance, which is why the theory of proximate cause, in my view, is the second most important principle after the principle of utmost good faith that applies to marine insurance. The liability of the insurer is therefore determined by the proximate cause, according to the terms of the principle of immediacy, for the coverage of the insurance risk for which the insurer has committed, and not for the remote one. Therefore, the fact that is judged as decisive for the final result, and not the chronological order of the events, is the criterion for covering the loss or damage of the insured, i.e. the intensity of the cause - event, and not the temporality that is the criterion the events took place. Regarding the cases of cyber risk in marine insurances, there is also a problem in the application of this principle, since as mentioned above, depending on the way in which the cracker or crackers attack, the cause is not always perceived in detail with the desired accuracy, while the surprise of cyber-attacks, the difficulty of detecting them, and the quantification of the attacks make it difficult to impossible to apply this principle.

According to section 33(1) of the 1906 act “A warranty, in the following sections relating to warranties, means a promissory warranty, that is to say, a warranty by which the assured undertakes that some particular thing shall or shall not be done, or that some condition shall be fulfilled, or whereby he affirms or negatives the existence of a particular state of facts.”. According to article 10 of the 2015 act, the breach of a guarantee only temporarily suspends the validity of the contract, which can be cured by putting the said contract back into force if the said breach ceases to exist. These provisions which refer to the existence of guarantees in the contract create common interests for both parties to the contract, as on the one hand the insurer is insured, and on the other hand the policyholder can negotiate a better premium. Therefore, in the case of a breach of any of the mentioned guarantees, the insurer renders the existing contract useless, exempting it from all responsibility towards the policyholder, but is responsible for any insurance risk coverage from events that occurred before the time of the breach. Warranties are categorized into those that are express and those that are implied. The first are set and formulated according to the

will of the contracting parties, which is why there is great diversity in their wording and do not concern anything specific, and the second operate by presumption, they are warranty of seaworthiness, warranty of port worthiness, warranty of cargo worthiness and warranty of legality.

Regarding the connection of the insurance risk of the cyber threat with the warranties set in each marine insurance contract at the level of express warranties, the diversity is approximately the same as that of the classic risks of piracy, war, etc. However, in the case of implied warranties, article 39 in paragraph 4 states that "a ship is deemed to be seaworthy when it is capable in all respects of facing the ordinary maritime risks of the insured voyage". In this case, the following problem and question arises, when is a vessel considered sufficient for its seaworthiness in the case of a cyberattack? What are the standards with which it must be equipped so that in the event of an attack, the lack of seaworthiness constitutes the insurance risk and not the breach of the seaworthiness warranties? Also, how can the insured prove the lack of seaworthiness or unseaworthiness of his ship before the cyberattack?

So from the moment that, as mentioned throughout this work, that the shipping industry has been digitized for the most part, or vice versa, digitalization has taken over most of the operation of the shipping industry, the presumptive existence of the vessel's seaworthiness is inextricably intertwined with its electronic systems and government machinery, which are the target of a cyberattack. This means that the coverage of the insurance risk of the cyberattack negates the warranties of seaworthiness, not so much in its legal part, namely the formulation of adequacy of seaworthiness, but in the technical difficulty of proving the existence of adequacy for it (seaworthiness).

3.2 The damage caused by a cyber attack

In the decade of the 2020s, in which the great spread of digital dependence is observed not only of companies, but also of government structures and organizations around the world, referring to the fact that we are living in the era of the digital revolution, the incidents of cyberattacks have not yet been counted and there is no clear picture of this phenomenon. But as it happens in the field of medicine with diseases, the result of the disease, i.e. in this case by matching the damage, creates the basis and the motivation to lead the theory and science of medicine precisely to the desired opposite result, i.e. the restoration of the health of the human organism, through the close monitoring of the action of each microbe or virus. In the same way,

theory and science deal with the cyberattack in the same way, that is, they perceive its existence from the moment there is "the pain", the damage to the company. But who exactly is she? In what forms is it perceived by companies?

There are numerous examples in the 2020s of such loss and damage, such as the cases of cyberattack victims of Facebook, Apple, Microsoft in the year 2013, the International Maritime Organization in September 2020, during which it was unavailable for two months its website despite the intensive efforts of specialists in the field of information technology to restore its online services to a normality, and in the same month of 2020 the cyberattack on the French Company CMA CGM, a global power player in maritime and air transport, but also in land and logistics, operating and operating in 160 countries and with 755 different services and many branches, falls victim to a cyberattack forcing it to cut off all external contact in its network in order to deal with malware introduction, container shipping and logistics giant, A.P. Moller-Maersk, falls victim to an attack in October 2017, in Greece on 20-03-2022 the letter transport services of the company Elta Courier face a cyberattack. The last example is one of the few where the reaction was immediate and in an article it is characteristically stated that "the immediate reaction and the actions of the competent service functions limited and prevented the extension of the attack. We immediately informed and are cooperating closely with all the competent state authorities as well as with IT companies specializing in cyber security". The above examples also demonstrate two factors, firstly, the giant companies will announce the cyberattack when there is a big problem for their operation resulting in the loss of millions of dollars, which means that cyberattacks are now a frequent phenomenon and are faced at any time, but the cyberattack that succeeds in paralyzing the structures of large organizations or companies also demonstrate the degree of organization of the malicious user-cracker. big of all companies so that the companies are in a framework of readiness to face organized or non-organized attacks of this type.

Returning to the issue of loss and damage, i.e. the result of a cyber-attack, in a shipping company, the answer is that first of all, the most common context of this is the financial and property impact, which the company suffers either for the withdrawal of sums of money, positive damage, either to create a negative atmosphere for the company or organization, in an attempt to discredit it through the disclosure of confidential data and information, or to paralyze its operating system by suspending

its functions for as long as the cyberattack is active, in competitive frameworks. But in the interim of positively or negatively damaging the target of the cyberattack, millions of dollars are lost. Unfortunately, however, the damage is not limited only to the property impact or destruction, as it has been observed that cyber-attacks also affect the navigation systems or those of the GPS, which lead to ship collisions with consequential consequences, including the loss of life, injuries, piracy, shipwreck, environmental disaster.

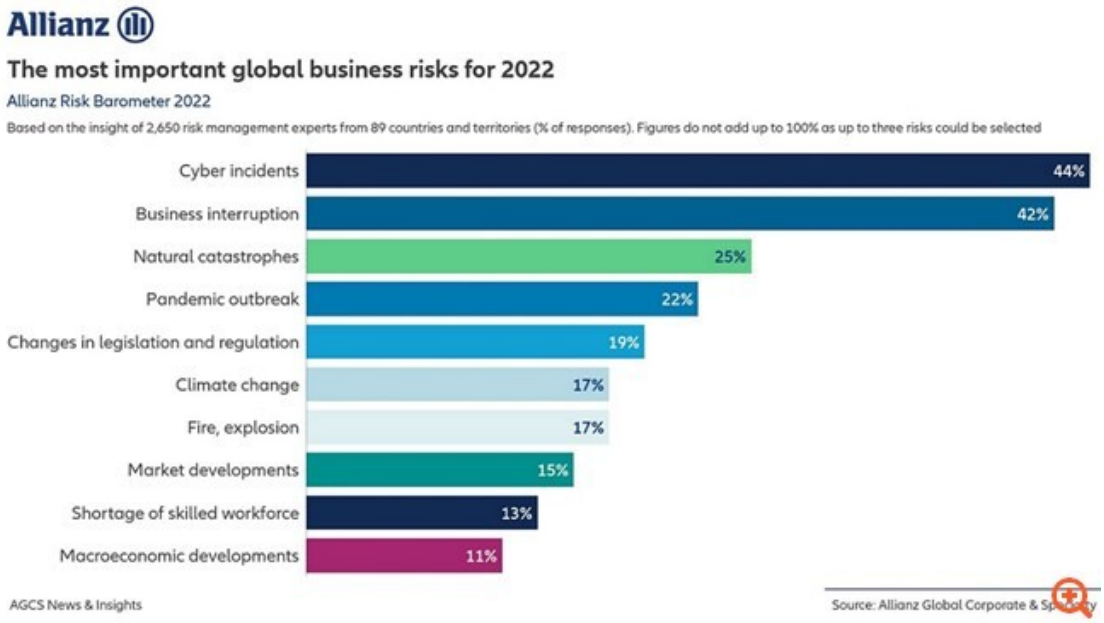
A serious example of piracy resulting from a cyberattack is the one in which Somali pirates with the help of a cracker managed to affect the tracking systems of a shipping company's ships passing through the Gulf of Aden, while ships are a frequent target when crossing the Singapore straits, which account for 25% of piracy incidents. Despite this October 2022 figures from the International Maritime Bureau show that by the end of September 2022 piracy and armed robbery against ships are at levels last seen in 1992. The latest global piracy report includes 58 incidents of piracy and armed robbery against ships – the lowest since 1994 – from 68 incidents during the same period last year. Which means that the actions described in this paper and concerning cyber security, as well as the constant vigilance of the companies have a positive result at a statistical level, as the level of maritime piracy of the last 30 years is at the lowest levels.[22]

Figure 9.

[22] https://www.newmoney.gr/roh/palmos-oikonomias/nautilia/i-piratikes-epithesis-miothikan-sta-chamilotera-epipeda-ton-telefteon-30-eton/

However, despite this positive development in which other factors, such as the quarantine period due to covid and the Ukrainian War, may be advocating, according to the Allianz Risk Barometer the incidents of cyberattacks are ranked at the top for the second time in the history of the survey (44% of responses). , increased by 5% from the corresponding measurement of the year 2021 and by 7% from that of 2019, while the second place is occupied by the Interruption of business activity (42%) and the third by Natural disasters (25%).[23]

Figure 10.



In conclusion, the question that arises from the above showing of the loss and damage faced by the victims of cyberattacks is whether they will be able to have the

[23] https://www.capital.gr/epixeiriseis/3608769/allianz-risk-barometer-2022-oi-kuberno-kindunoi-apoteloun-ton-korufaio-epixeirisiako-kinduno-pagkosmios

assistance of the risk insurance companies, or not! The world is evolving into a new era of gears. This has the result that, on the one hand, traditional insurance risks are reduced, with the indirect consequence of decreasing the interest of the buying public in insuring these risks, but on the other hand, it seems that insurers are not always willing to insure the cyber-attacks to enable companies to deal with the production line more than with cyber security, which is growing into a standalone business.

In cyber risk insurance, a very important factor is the responsibility of the person involved, which should be of such a nature that it is not confused with a malfunction of the system due to an innocent error or a random event, but is the result of a premeditated action. Therefore, within the above-described general context of the complexity of the cyber risk, it is often considered difficult to find not only the entity responsible, but also whether the attack is a product of criminal activity or not. The difficulty of identifying and verifying the attack lies in the fact that it is not recognized as a criminal act in principle, as according to the terms of the criminal law, the cyber threat begins with actions that are considered legal, i.e. using a computer and the Internet, entering websites, using a Universal Serial Bus or simply usb-stick on computers. The criminal act begins from the moment the defenses of an electronic system are breached, the unauthorized entry into the cyberspace of a company, etc. Most of the time the criminal act is judged directly by the result it brings about as the speeds that develop from the breach to the damage or loss are realized at times not noticeable. This problematic is also transferred to the issue of marine insurance for cyber risk, since on the one hand, as mentioned, the subject who violates is imperceptible, the insurer in this case having to face the general phenomenon-rule of the anonymization of the perpetrator who acts in cyberspace, from on the other hand, the culpability and its gradation are not always perceived, as described by civil law in the elements of civil liability, i.e. a cyberattack from a random event and for reasons of force majeure, or emergency, existence of slight or gross negligence and contributory fault (on the other hand), the existence of intent, while when criminally infernal acts are investigated there is also the question of the gradation of malice, intentional, necessary or contingent. All of the above constitute another additional difficulty in terms of insurance law in order to cover and to what extent the realization of the insurance risk of the cyberattack.

In the above report on finding responsibility, the contribution and connection of the cyber risk with issues related to the civil liability of the company or the ship in

the event of an accident, for example, a ship collision event, a loading or unloading of cargo, is indirectly born in a negligent manner resulting in its destruction, a collision of a ship with a port platform and all this happening because the electronic navigation systems of the ship, or the handling of the cranes that are present either on the ship or in the port, do not work properly due to a cyberattack. According to the theory and jurisprudence the responsibility in such cases of civil liability incidents if the incident originates due to a cyberattack then the participation of the victim in the context of cyber security will depend on whether or not he had complied with the appropriate protection measures in ship involved or agent of the company that created the incident. The ISM code mentioned above is the criterion for the measures with which each company must comply. The same case includes the ship that is characterized as insufficient in terms of the safe management system (SMS). Consequently, when the company or ship takes all the appropriate measures mentioned above with this work and follows a proper cyberattack management plan, in cases of civil liability as described above in the event of a collision, it will not bear any responsibility if it has been a victim cyberattack. And the insurance company which insures the cyber risk for this company will have every right to assert the claim of the culprit in the context of civil liability if it is proven that there is complicity on the part of another ship or object.

3.3 How is cyber risk handled by insurance and reinsurance companies

Private law is the one that preeminently governs marine insurances, as marine insurance presupposes a contract in the context of indemnity law with the participation of the contracting parties who, after negotiating the terms of the future agreement between them, by signing it mutually secure the rights and are bound by the obligations they assume for each other, and specifically the insurer undertakes to cover the damage or loss of the insured in the event of activation of the insurance risk accurately described in the contract, on the other hand the insured is obliged to pays the agreed premium. To date, marine insurance includes the vessel, its equipment (Hull and Machinery Insurance), cargo, civil liability of third parties (P & I Insurance). Further according to article 3 of act 1906 “Maritime “perils" means the perils consequent on, or incidental to, the navigation of the sea, that is lo say, perils of the seas, fire, war perils, pirates, rovers, thieves, captures, seisures, restraints, and detainments of princes and peoples, jettisons, barratry, and any other perils, either of the like kind or which may be designated by the policy.” This article in the reference

of insurance risks does not include the cyberattack, therefore as it was briefly mentioned in some points of the present pain to have the cyberattack in the legal world of the insurance of law, the concept of cyberattack is incorporated into traditional insurance risks, otherwise known traditional insurance products. In addition, it should be noted that the risks mentioned above are categorized into those that come from the sea, and mainly concern weather phenomena and natural disasters, and those that occur at sea, such as theft, war and piracy. It is clear that cyberattack is one of the dangers that occur at sea, and under no circumstances can they come from the sea, as cyberattack clearly requires human action either by intention or by mistake. In addition to the coverage of the cyber risk, an uninsurable product that has not yet received its final form as an insurance product for all the reasons mentioned in this work, it is observed that the insurance of the ship and its equipment are excluded from marine insurance coverage. And the need to cover the gaps that cannot be covered by traditional insurance products, with which, as we mentioned above, a hesitant effort is realized on the part of insurers in order to appease the number of insured people, who either have, or do not have, the cyberattack experience.

Summarizing the problematic implementation of cyber risk insurance, insurers to insure this risk must overcome a) the complexity of cyber security aspects combined with the unprecedented cyber insurance, b) the lack of liability of shipping companies until now to take measures for cyber security (now this is to be seen after two years of the mandatory measures being in force), c) the lack of purpose of the insurance coverage from the insurers' side, d) the lack of possibility of predicting the risks themselves, the valuation of the damage , the prediction of the extent of the damage caused but also of the cyberattack itself and the lack of specialized knowledge and the parallel need to use experienced and specialized in the field of cyber security and e) the fact of the non-existence of jurisprudence to date, creating by extension a lack of "fixed variables" that could serve as tools in a insurers to be able to complete the "function" of the insurance.

The obstacles to insurance coverage of cyber risk do not concern only the side of the insurer, as the insured in many cases finds himself helpless in the abyss of the often costly and complex nature of the process to prove the existence of the loss or damage suffered due to an attack on his cyber space. In addition, the insured should always prove that he had taken the necessary ISM Code measures to prove his preparedness for dealing with cyberattacks. IHS Fairplay together with BIMCO,

according to columnist[24] Mrs. Eleana Houtea after the explosion created by the examples of cyberattacks by Moller Maersk (2017) and Cosco (2018), carried out a survey in 2016 on cyber security in shipping with the results to show that cyber-attacks were common, with the use of malware and phishing being the most common. The following statistical results were derived from this research, namely that 11.7% were confirmed attacks, while in 3% of cases the loss was covered by the insurance companies. Of this percentage, Hull & Machinery insurance did not cover a single claim, while P&I club insurance covered less than 1% and 1.9% of cases were covered because the company had dedicated cyber insurance.[25]

3.3.1 The position of P&I clubs in cyber risk insurance

The P&I clubs, the mutual insurance organizations of protection and indemnity, as non-profit companies, which were created by the shipowners themselves, are strong players in the field of marine insurance. Their placement in insurance matters, and in fact in the area of coverage they undertake, namely civil liability towards third parties for shipowners, or and ship managers or and charterers, is of great importance. In addition, the International Group of P&I clubs or otherwise the International Group of Protection and Indemnity Associations which is made up of 13 different clubs around the world was created in 1889 and functions as a reinsurer of the mutual insurance organizations for the above insurance risk coverage of the individual partnerships and it owns his own position on insurance matters which is also characterized as of weighty importance. It should be noted that the 13 P&I clubs that make up the said International Group are 1) American P&I Club, 2) The Britannia P&I Club, 3) Gard P&I Club, 4) The Japan P&I Club , 5) The London P&I Club, 6) The North of England P&I Club, 7)The Shipowners' P&I Club, 8) Skuld P&I Club, 9) The Standard Club, 10) The Steamship P&I Club,11) The Swedish Club, 12) UK P&I Club, 13) The West of England P&I Club.

Therefore, the position of the above mutual insurance organizations and the above-mentioned International Group, although it is not expressly rejected in cyber

[24] https://nautilia.gr/eidiseis/nautilia-prostasia-apenanti-kyvernoapeiles/

[25] https://polynoe.lib.uniwa.gr/xmlui/bitstream/handle/11400/3040/%CE%9D%CE%B1%CF%85%CF%84%CE%B9%CE%BA%CE%AC%20%CE%91%CF%84%CF%85%CF%87%CE%AE%CE%BC%CE%B1%CF%84%CE%B1%20%CE%BA%CE%B1%CE%B9%20%CE%98%CE%B1%CE%BB%CE%AC%CF%83%CF%83%CE%B9%CE%B1%20%CE%91%CF%83%CF%86%CE%AC%CE%BB%CE%B9%CF%83%CE%B7%20.pdf?sequence=1&isAllowed=y
And https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/13670/%ce%9a%cf%85%ce%b2%ce%b5%cf%81%ce%bd%ce%bf%ce%b1%cf%83%cf%86%ce%ac%ce%bb%ce%b5%ce%b9%ce%b1%20%26%20%ce%b8%ce%b1%ce%bb%ce%ac%cf%83%cf%83%ce%b9%ce%b1%20%ce%91%cf%83%cf%86%ce%ac%ce%bb%ce%b9%cf%83%ce%b7.pdf?sequence=1&isAllowed=y

risk insurance, but as a result they exclude the largest part of cyberattack cases, as according to traditional insurance practice these organizations are the subject of only specific risks, something that cannot be delineated to date in the case of cyberattack. Non-coverage also includes losses, such as financial loss caused by malware or the cost of restoring damaged or lost information.

In fact, these organizations within the framework of their common policy, with minor differences between them, use an exemption clause from cyberattack (CL380/10-11-2003), according to which the insurer is excluded from covering any damage or loss from which it came indirectly, directly or indirectly from the use or operation of a computer and its software programs, and specifically mentions “in no case shall this agreement cover loss damage liability or expense directly caused by or contributed to or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus or process or any electronic system." (Institute Cyber Attack Exclusion Clause - CL380). The clause in question, although it is firmly accepted by everyone, parts of its wording create practical problems, as today in the era of digital revolution and cyberspace organizations use an anachronistic clause, as in the year 2003 when it was drafted there was not even a need for cyber risk insurance as cyberspace had not entered maritime transport in the way it does today. In particular, the wording "As a means of causing harm" the use of a computer becomes problematic, while the issue of whether the policyholder, who seeks to insure the cyber risk, should be the target of the cracker or is covered remains unclear. and by the fact that he eventually became a victim without being the original target of the cracker. In other words, this clause, due to the lack of decisions by the English Courts on cyber-attack insurance issues, in relation to the burning issue of its activation or not, is currently a result of interpretation in terms of theory and interpretation and acceptance of the parties to the insurance contract. It was also noted that the faulty wording for causing the damage or (loss) creates practical issues of interpretation regarding the use of the computer, which may not lie in the established operation of the computer and its software, as an object that carries weight, countryside, any sharp corners to be used as an object to commit the crime. Unfortunately, the exclusion clause in the method of grammatical interpretation used mostly by insurance law creates problems of interpretation, which may seem simple, but in cases of civil liability large sums of money are at stake. These issues remain outstanding and create

problems which in my view are to be resolved when the English Courts are taken up even incidentally with such related issues. Therefore, since the English Courts and in general the Judicial Authority that binds the insurers have not expressed their informed opinion, the 13 organizations mentioned above, depending on the special position of interest of each one, differ in the placement and interpretation of the exemption clause mentioned above. Briefly presenting the case study of the positions of the 13 above-mentioned organizations, in particular we mention 1) American P&I Club does not incorporate clause 380, but sets its own clause which mentions the exclusion of insurance from any obligation that originates and stems from the electronic transaction systems such as for example the electronic bill of lading, which it does not accept 2) The Britannia P&I Club it does not incorporate clause 380, nor does it include any exception related to the use of a computer 3) Gard P&I Club incorporates clause 380 and specifically refers to the exclusion of coverage for damage caused by a computer, software program, malicious virus or any other electronic system 4) The Japan P&I Club it does not refer to the existence or not of clause 380 and carries out its own categorization of risks in cyberspace, i.e. external and internal, of which it covers only the external 5) The London P&I Club it incorporates the clause 380 and additionally following the common policy of most of the 13 clubs excludes liabilities, losses and expenses arising from the electronic trading system 6) The North of England P&I Club does not use clause 380 but by its own wording excludes from the coverage only that it originates from the use of a computer, while similarly it excludes liability coverage from electronic trading systems 7) The Shipowners' P&I Club it follows the usual practice of clubs and incorporates clause 380, which it completes in the case of damages that come from computer use of the wording "chemical, biochemical or electromagnetic weapon", to which the opinion of Nicholas Gooding, representative of the International Marine Insurance Association at the International Maritime Organization, was contributed. This club also excludes its liability for loss or damage arising from the electronic transaction system 8) Skuld P&I Club excludes any coverage related to cyberspace, does not accept liability and expenses arising from the electronic trading system with a sole exception if the latter has been approved by IGPANDI 9) The Standard Club incorporates exemption clause 380 and at the same time excludes the liabilities associated with the electronic trading system 10) The Steamship P&I Club incorporates exemption clause 380 and at the same time excludes liabilities connected

with the electronic transaction system 11) The Swedish Club incorporates exemption clause 380 and at the same time excludes liabilities connected with connected to the electronic transaction system, while expressly excluding liability, costs and expenses caused by the use of a computer or computer system 12) UK P&I Club incorporates exclusion clause 380 and at the same time excludes liability connected to the electronic transaction system 13) The West of England P&I Club incorporates exemption clause 380 and at the same time excludes liabilities associated with the electronic transaction system.

In conclusion, the positioning of P&I Clubs, with few exceptions, is common, and the reluctance to insure cyber risk is a constant. Like the rest of the insurers, the P&I Clubs are awaiting the implementation of the measures of the resolution of the International Maritime Organization (IMO) which came into force on 01-01-2021, as well as the results of said implementation with the passage of time in order to implement the approach between the abstract of the cyberattack to the concrete of cyber risk insurance.

3.3.2 The innovative position of Lloyd's of London

The innovative position of Lloyd's of London the traditional hesitant position of the P&I clubs in matters of cyber risk insurance is coming to disrupt the largest insurance market in London, Lloyd's, who are rightly characterized as pioneers today in covering this risk. In particular, the innovation they are introducing is a new cyberattack exemption clause, LMA 5403[26], which replaces clause 380, which became mandatory from 01-01-2020 for every insurance policy or its renewal for the risk of war or ship insurance and its equipment. So, this initiative demonstrates that the practice followed with the use of traditional insurance products must be changed, and an independent insurance product that concerns cyberspace must be created. Of

[26] MARINE CYBER ENDORSEMENT. **1** Subject only to paragraph 3 below, in no case shall this insurance cover loss, damage, liability or expense directly or indirectly caused by or contributed to by or arising from the use or operation, as a means for inflicting harm, of any computer, computer system, computer software program, malicious code, computer virus, computer process or any other electronic system. **2** Subject to the conditions, limitations and exclusions of the policy to which this clause attaches, the indemnity otherwise recoverable hereunder shall not be prejudiced by the use or operation of any computer, computer system, computer software program, computer process or any other electronic system, if such use or operation is not as a means for inflicting harm. **3** Where this clause is endorsed on policies covering risks of war, civil war, revolution, rebellion, insurrection, or civil strife arising therefrom, or any hostile act by or against a belligerent power, or terrorism or any person acting from a political motive, paragraph 1 shall not operate to exclude losses (which would otherwise be covered) arising from the use of any computer, computer system or computer software program or any other electronic system in the launch and/or guidance system and/or firing mechanism of any weapon or missile. LMA5403 11 November 2019**.** **https://www.lmalloyds.com/LMA/News/LMA_bulletins/LMA_Bulletins/LMA19-031-PD.aspx**

course, this move is the start of work on the issue of maritime cyber risk insurance and presupposes further fermentation to reach a level of complete autonomy, while the formulation of a separate exception clause is a step forward, but it does not mean that the big issue of cyber risk insurance as analyzed above.

3.3.3 International Association of Insurers Introduces Two New Cyber Exclusion Clauses

The International Association of Insurers, representing international insurance and reinsurance companies, which act independently of Lloyd's, aims to strengthen the business environment of its members. It is clear that the issue of cyber risk insurance has also concerned it, and in fact it, like Lloyd's of London, published two new cyber exclusion clauses in 2019, IUA 09-081 and IUA 09-082 replacing the updated clause 380 mentioned and analyzed above for the sake of clarity in the wording of the aforementioned exclusion clause, reinforcing the principle of supreme good faith that in this particular case should be observed by the insurer towards the insured. The first clause concerns the absolute exclusion of the insurer's liability for loss of the insured in cyberspace. According to it, the liability of the insurer is excluded in a more extended context any loss arising from the use of computers, internet or data. The second exclusion clause concerns the limitation of exclusion from cyber loss, referring only to losses arising directly from actual cyber incidents. The clarity provided by these new clauses comes to fill the gap that existed in the past for the delineation of what is insured against cyberspace and what not, covering the need of the insurers to have a ready form for the formulation of an exemption clause, which does not include in its bosom the above-mentioned pathogens of clause 380.

Conclusion

This work was concerned with the following essential elements concerning the coverage of the insurance risk deriving from the cyber-attack on maritime transport. In particular, cyberspace, as it has drastically penetrated the shipping industry, its lack or malfunction creates damage and losses to shipping giants with the biggest examples being Moller Maersk and Cosco, and many other examples worth millions of dollars each (company). The types of cyberattack, such as Ransomware, Phising, Wi-fi, DDos, used by different types of actors (crackers) such as activists, criminals, opportunists, terrorists, are sometimes detected, sometimes not, and the need to delineate the elements of the cyberattack, i.e. the illegitimacy, the mode of action, the motive of action and the eventual result of damage or loss in extent, temporal and

financial, has firstly mobilized the companies themselves to secure themselves within their own structures by using IT departments as internal or external partners, but further from 2016 onwards, with the pioneer once again, the International Maritime Organization is the start of engaging maritime organizations and bodies to combat cyberattacks, with the aim of restoring the safe use and operation of cyberspace, which was followed by the Security Committee in 2017, the international shipping organizations in the same year, while the International Organization for Standardization and the European General Data Protection Regulation (GDPR) assisted in this move.

In June 2016, the “Interim Guidelines on Maritime Cyber Risk” is published by the International Maritime Organization as a guide that provides recommendations for cyber risk management at a proactive cyber security level. On 5 July 2017, these recommendations are being replaced by a full set of guidelines with the same objective as above ``Guidelines on Maritime Cyber Risk Management", which was heavily influenced by the document published two months ago ``Measures to Enhance Maritime Security" " which was presented at the 98th Meeting of the Marine Safety Commission in the United States of America. All of the above promoted the adoption of the resolution "Maritime Cyber Risk Management in Safety Management Systems" of June 16, 2017, which was integrated into the then already existing safety management systems (SMS), which began to be implemented in the form of compliance by shipping companies for cyber security from 1-1-2021. Alongside these moves, in 2017 international shipping organizations jointly reissued the third edition of the International Shipping Organization's guidelines, "The Guidelines on Cyber Security Onboard Ships", which assists companies in developing appropriate cyber risk management. Finally, in all these mobilizations carried out for cyber security, the use of the ISO/IEC27001 standard on Information technology and the European Organization for the protection of personal data, which were used and are used for prevention purposes in the event of a cyberattack, had a very important contribution.

In any case, however, the protection against damage or loss of each company or organization is a continuous and permanent request in the risk insurance market, calling on underwriters to do what managers are called to do in cases of difficult choices, to think out of the box, in order to be able to respond to the new development of the market in general and of the buying public of insurance today. From the research data, which were presented and analyzed in this paper, the conclusion of an

internal desire of insurers to insure cyber risk and an external reluctance to document and formulate in a concrete way the cyber risk they insure, having covered the extent of the possible damage or loss of the companies as well as the period of time that it will be active. In my view it must be recognized that the work of underwriters is not easy, as the cyber risk, to be covered in its entirety, will create a risk financially unprofitable for insurers, which from measurements and statistics is the reason why there is the aforementioned external reluctance of insurers to insure it. The extent of the risk, the uncertainty and the non-existence of stable variables that characterize the cyber risk and its effects, prevent insurers from satisfying this insurance risk in its entirety. So the reservations that justifiably exist on the part of insurers are a case study, which we notice is being resolved gradually and methodically. The thirteen (13) P&I Clubs and their group, which are responsible for civil liability in cases of conflict, take a conservative stance both in insuring the risks arising from maritime cyber-attacks and in the use of clause 380, the opt-out clause, which they slightly complement in some cases, especially in cases of specifically excluding cyber risk insurance from electronic freight transactions. Lloyd's of London insurance market is introducing a new maritime cyberattack exclusion clause at the end of 2019, replacing the above, making it mandatory for any new war risk or Hull & Engine ship and engine insurance contract. Machinery, while they created several new insurance products which are now available on the market. Finally, the International Insurers Association (IUA) publishes two new clauses, the Cyber Loss Absolute Exclusion and the Limited Cyber Loss Exclusion, which were published in June 2019, offering a clear wording in relation to Clause 380 mentioned above.

From the above it is observed that the insurance markets in the new era requests for cyber insurance move conservatively using the already existing insurance risks mentioned in the Act 1906 and 2015, while introducing innovations mainly in the exclusion clause for the insurance of the said risk, the cyber risk. In my view, all this fluidity that has arisen on the question of insurance cover for cyber risk in maritime transport, is to be delineated when the English courts take up their position on this issue. However, in order for this to be implemented, first there should be in the world of contracts the coverage of the insurance risk of the cyberattack, which until now in practice the reluctance of the insurers creates an obstacle for things to evolve and the situations to be consolidated. Of course, this does not mean that the insurers are obliged to do so, as the risk insurance is a contract in which the parties to the

insurance contract have rights and obligations after it is signed, as before the signature the right of freedom of contract or not applies. No one is forcing them to do so, and the insurers themselves are placing their financial benefit on a future and uncertain future.

As a result, the use of cyberspace gives companies the speed of information and the accuracy of the company's movements in the market, increasing quantitatively the property benefit and qualitatively the supply and demand of the buying public. A price is the antithesis of the positive use of cyberspace, the cyber risk of a cyberattack, which at the punitive level, in which there is damage or loss to the company, which insurers are asked to cover. However, their only pressure, as it has always been and continues to be, is the constant and continuous demand for insurance risk coverage from the market, justifying them in my view, as there is the great risk of the future and uncertain coverage of the cyber risk they will receive, if the latter has not been defined and specified first, something which also needs its time to complete its cycle like all the elements in nature which are under the natural process of “metabolism”.

Abbreviations

The following abbreviations are useful in this manuscript:

AI Artificial Intelligence

AIS Automatic Identification System

CE Certificate Authority

ECDIS Electronic Chart Display and Information System

GMDS Global Maritime Distress System

GPS Global Positioning System

IBS Integrated Bridge System

ICS Industrial Control System

ICT Information and Communications Technology

IMO International Maritime Organization

IT Information Technology

NNSS Global Navigation Satellite System

NMA Navigation Message Authentication

OT Operational Technology

PKI Public Key Infrastructure

Radar Radio Detection and Ranging

VSAT Very Small Aperture Terminal

VSS Video Surveillance System

Dictionary

Access control is selective limiting of the ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains or to control system components and functions.

Cyberattack is any type of offensive manoeuvre that targets IT and OT systems, computer networks, and/or personal computer devices and attempts to compromise, destroy or access company and ship systems and data. Cyber incident is an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or to the information that they process, store or transmit, and which may require a response action to mitigate the consequences.

Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level by taking into consideration the costs and benefits of actions taken by stakeholders.

Cyber system is any combination of facilities, equipment, personnel, procedures and communications integrated to provide cyber services; examples include business systems, control systems and access control systems

Digitalisation is how the digital world impacts people and work.

Executable software includes instructions for a computer to perform specified tasks according to encoded instructions. Firewall is a logical or physical break designed to prevent unauthorised access to IT infrastructure and information.

Firmware is software imbedded in electronic devices that provides control, monitoring and data manipulation of engineered products and systems. These are normally self-contained and not THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS V4 Glossary 59 accessible to user manipulation.

Flaw is unintended functionality in software.

Information Technology (IT) covers the spectrum of technologies for data storing and processing, including software, hardware, and communication technologies.

Intrusion Detection System (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.

Intrusion Prevention System (IPS), also known as Intrusion Detection and Prevention Systems (IDPSs), are network security appliances that monitor network and/or system activities for malicious activity.

Local Area Network (LAN) is a computer network that interconnects computers within a limited area such as a home, ship or office building, using network media.

Malware is a generic term for a variety of malicious software, which can infect computer systems and impact on their performance.

Virus is a hidden, self-replicating section of computer software that maliciously infects and manipulates the operation of a computer program or system.

Wi-Fi is all short-range communications that use some type of electromagnetic spectrum to send and/ or receive information without wires.

ABS, 2020. IMO 2021 cyber risk management guidelines - What to know and how to comply [PowerPoint presentation].

Arıdemir, H., and Allı, C., 2019. An analysis of the exclusive economic zone debates in Eastern Mediterranean region. Journal of Economics Business and Political Researches, 4 (10), 188–202. Available from: https://dergipark.org.tr/en/download/article-file/829290 [Accessed 4 May 2020].

Aselsan, 2017. KORAL mobil radar EH (elektronik harp) sistemi [online]. Available from: https://www.aselsan.com.tr/1a8b7437-1ca0-4652-bd30-d71640c857b2.pdf [Accessed 22 July 2020].

Bateman, T., 2013. Police warn over drugs cyber-attack [online]. Available from: https://www.bbc.com/news/world-europe-24539417 [Accessed 25 March 2020].

Belmont, K.B., 2016. Cyber Cases in the Maritime Environment.

BIMCO, 2018. The guidelines on cyber security onboard ships. 3rd ed.

Blake, T., 2017. Hackers took ‘full control’ of container ship’s navigation systems for 10 hours - IHS Fairplay | RNTF [online]. Available from: https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-shipsnavigation-systems-for-10-hours-ihs-fairplay/ [Accessed 25 March 2020].

Bodeau, D.J., Graubart, R., and Fabius-Greene, J., 2010. Improving cyber security and mission assurance via cyber preparedness (Cyber Prep) levels. International conference on social computing, 20-22 August 2010 Minneapolis.

Brekke, E.F., et al., 2019. The Autosea project: Developing closed-loop target tracking and collision avoidance systems. Journal of Physics: Conference Series.

C4ADS, 2019. Above us only stars. Exposing GPS spoofing in Russia and Syria.

C4Defence, 2019. KORAL’a REDET-II desteği [online]. Available from: https://www.c4defence.com/Arsiv/korala-redetii-destegi/8940/1 [Accessed 22 July 2020].

Chambers, S., 2020. London Offshore Consultants suffers ransomware attack [online]. Available from: https://splash247.com/london-offshore-consultants-suffers-ransomware-attack/ [Accessed 25 March 2020].

Coble, S., 2020. Carnival Cruise Lines hacked [online]. Available from: https://www.infosecuritymagazine.com/news/carnival-cruise-lines-hacked/ [Accessed 25 March 2020].

CORDIS, 2020. ERA Chair in Maritime Cyber Security at Tallinn University of Technology [online]. Available from: https://cordis.europa.eu/project/id/952360 [Accessed 21 August 2020].

Cozzens, T., 2020. UrsaNav installs eLoran testbed in South Korea [online]. Available from: https://www.gpsworld.com/ursanav-installs-eloran-testbed-in-south-korea/ [Accessed 23 July 2020].

CRISTIN, 2020. Maritime Cyber Resilience [online]. Available from: https://app.cristin.no/projects/show.jsf?id=2057306 [Accessed 30 July 2020].

Cyber Keel, 2014. Maritime cyber-risks.

Cyber-MAR, 2019. About [online]. Available from: https://www.cyber-mar.eu/about/ [Accessed 25 April 2020].

Danish Maritime Cybersecurity Unit, 2019. Cyber and information strategy for the maritime sector 2019 - 2022 [online]. Available from: https://www.dma.dk/Documents/Publikationer/Cyber%20and%20Information %20Security%20Strategy%20f or%20the%20Maritime%20Sector.pdf [Accessed 4 January 2020].

Denizcilik Bilgileri, 2018. Türkiye GPS jammer ile Yunan araştırma gemilerini engelliyor mu? [online]. Available from: https://www.denizcilikbilgileri.com/turkiye-gps-jammer-ile-yunan-arastirma-gemileriniengelliyor-mu/ [Accessed 4 February 2020].

Eastern Mediterranean Sea-GPS Interference, 2018 [online]. U.S. Maritime Administration. Available from: https://www.maritime.dot.gov/content/2018-014-eastern-mediterranean-sea-gps-interference [Accessed 8 April 2020]. Electronic interferences assesment, 2018 [online]. NATO Shipping Center. Available from: https://shipping.nato.int/nsc/page10303037.aspx [Accessed 8 April 2020].

Esage, A., 2018. British shipping company Clarksons hacked [online]. Available from: https://www.securitynewspaper.com/2018/08/02/british-shipping-company-clarksons-hacked/ [Accessed 26 March 2020].

European Cybercrime Centre, 2013. Hackers deployed to facilitate drugs smuggling [online]. EC3. Available from: https://www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf [Accessed 8 May 2020].

Fadilpašić, S., 2017. Shipping giant Maersk reveals $300 million cyber-attack loss [online]. Available from: https://www.itproportal.com/news/maersk-lost-300-million-due-to-notpetya/ [Accessed 25 April 2020].

Faustmann, H., Gurel, A., and Reichberg, G.M., eds., 2012. Cyprus Offshore Hydrocarbons: Regional Politics and Wealth Distribution. Peace Research Institute.

Goward, D., 2017. Mass GPS Spoofing Attack in Black Sea? [online]. Available from: https://www.maritimeexecutive.com/editorials/mass-gps-spoofing-attack-in-black-sea [Accessed 25 April 2020].

Graham, L., 2017. Shipping industry vulnerable to cyberattacks and GPS jamming [online]. Available from: https://www.cnbc.com/2017/02/01/shipping-industry-vulnerable-to-cyber-attacks-and-gps-jamming.html [Accessed 23 March 2020].

Humphreys, T., 2017. Ships fooled in GPS spoofing attack suggest Russian cyberweapon [online]. Available from:

https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russiancyberweapon/ [Accessed 23 March 2020].

Humphreys, T.E., et al., 2008. Assessing the spoofing threat: Development of a portable GPS civilian spoofer. International technical meeting of the satellite division of the institute of navigation, 16-19 September 2008 Savannah.

IMarEST, 2018. Ports of Barcelona and San Diego hit by cyberattacks [online]. Available from: https://www.imarest.org/themarineprofessional/item/4473-ports-of-barcelona-and-san-diego-hit-by-cyberattacks [Accessed 13 April 2020].

IMO, 2017. Resolution MSC.428(98).

ISO, 2018. ISO/IEC 27000:2018(en) Information technology - security techniques - information security management systems.

Kochetkova, K., 2015. Maritime industry is easy meat for cyber criminals [online]. Available from: https://www.kaspersky.com/blog/maritime-cyber-security/8796/ [Accessed 25 March 2020].

Leyden, J., 2018. Holy ship! UK shipping biz Clarksons blames megahack on single point of pwnage [online]. Available from: https://www.theregister.co.uk/2018/08/01/clarksons_breach_update/ [Accessed 26 March 2020].

Lund, M.S., et al., 2018. Integrity of integrated navigation systems. Conference on communications and network security (CNS), 30 May - 1 June 2018 Beijing.

Maersk, 2017. Cyberattack update.

Maritime and Port Authority of Singapore, 2019. New 24/7 Maritime Cybersecurity Operations Centre to Boost Cyber Defence Readiness [online]. Available from: https://www.mpa.gov.sg/web/portal/home/mediacentre/news-releases/mpa-news-releases/detail/8a5114cf-8214-4b46-8999-2c6c42433b1e [Accessed 25 April 2020].

Maritime Executive, 2017. Ferry builder Austal hit by cyberattack [online]. Available from: https://www.maritime-executive.com/article/ferry-builder-austal-hit-by-cyberattack [Accessed 25 March 2020].

Mohindru, S.C., 2017. Shipping: BW Group's computer systems hacked; steps up cyber security [online]. Available from: https://www.spglobal.com/platts/en/market-insights/latest-news/shipping/101317-shippingbw-groups-computer-systems-hacked-steps-up-cyber-security [Accessed 25 March 2020].

MUNIN, 2012. About MUNIN [online]. Available from: http://www.unmanned-ship.org/munin/ [Accessed 24 April 2020].

Ngai, S., 2017. BW Group steps up cyber security after IT infringement – IHS Markit Safety at Sea [online]. Available from: https://safetyatsea.net/news/2017/bw-group-steps-up-cyber-security-after-it-infringement/ [Accessed 25 March 2020].

Oruc, A., 2019. Tanker industry is more ready against cyber threats. International conference on marine engineering and technology, 5-7 November 2019 Muscat.

Ozkaya, S., 2018. Doğu Akdeniz'de ısınan sular ve Kıbrıs denklemi [online]. Anadolu Agency. Available from: https://www.aa.com.tr/tr/analiz-haber/dogu-akdeniz-de-isinan-sular-ve-kibris-denklemi/1278755 [Accessed 8 May 2020].

Sabah, 2016. KORAL TSK'ya teslim edildi [online]. Available from: https://www.sabah.com.tr/galeri/turkiye/koral-tskya-teslim-edildi [Accessed 22 July 2020].

Safety4Sea, 2019. UK marine services company hit by cyberattack [online]. Available from: https://safety4sea.com/uk-marine-services-company-hit-by-cyber-attack/ [Accessed 22 March 2020].

Safety4Sea, 2020. Data breach at UK yachting recruitment agency exposes 17,000 personal data [online]. Available from: https://safety4sea.com/data-breach-at-uk-yachting-recruitment-agency-exposes-17000- personal-data/ [Accessed 22 March 2020].

Saul, J., 2017. Cyber threats prompt return of radio for ship navigation [online]. Available from: https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-shipnavigation-idUSKBN1AN0HT [Accessed 23 March 2020].

Senzee, T., 2019. What happened in ransomware attack on Port of San Diego [online]. Available from: https://www.sandiegoreader.com/news/2019/apr/10/city-lights-happened-ransomware-port-san-diego/ [Accessed 13 April 2020].

Shauk, Z., 2013. Malware on oil rig computers raises security fears [online]. Available from: https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-securityfears-4301773.php [Accessed 25 March 2020].

Sophos, 2013. The A-Z of computer and data security threats.

The Local, 2014. State-sponsored hackers spied on Denmark [online]. Available from: https://www.thelocal.dk/20140922/denmark-was-hacked-by-state-sponsored-spies [Accessed 23 March 2020].

Torbati, Y., and Saul, J., 2012. Iran's top cargo shipping line says sanctions damage mounting [online]. Available from: https://www.reuters.com/article/us-iran-sanctions-shipping-idUSBRE89L10X20121022 [Accessed 26 March 2020].

Trend Micro, 2017. Ransomware [online]. Available from: https://www.trendmicro.com/vinfo/us/security/definition/ransomware [Accessed 25 April 2020].

Tung, L., 2018. Maersk took just 10 days to replace 45,000 PCs wiped by NotPetya attack [online]. Available from: https://www.csoonline.com/article/3514914/maersk-took-just-10-days-to-replace-45-000-pcs-wipedby-notpetya-attack.html [Accessed 26 March 2020].

U.S. Department of Justice, 2018. Two Iranian men indicted for deploying ransomware to extort hospitals, municipalities, and public institutions, causing over $30 million in losses [online]. Available from: https://www.justice.gov/opa/pr/two-

iranian-men-indicted-deploying-ransomware-extort-hospitalsmunicipalities-and-public [Accessed 13 April 2020].

University of Rijeka, 2019. Cyber Security of Maritime ICT-Based Systems. Available from: https://www.pfri.uniri.hr/web/en/projekti/aktivni/10-2019/2019-Svilicic-eng.pdf [Accessed 30 July 2020].

USCG NAVCEN, 2020. GPS problem reports status [online]. Available from: https://navcen.uscg.gov/?Do=GPSReportStatus [Accessed 4 April 2020].

Vistiaho, P., 2017. Maritime cyber security incident data reporting for autonomous ships. Thesis (M.Sc.). Tampere University of Technology.

WMN, 2018a. COSCO Shipping Lines falls victim to cyberattack [online]. Available from: https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/ [Accessed 25 March 2020]

WMN, 2018b. Data theft affects hundreds of Svitzer Australia's employees [online]. Available from: https://worldmaritimenews.com/archives/247526/data-theft-affects-hundreds-of-svitzer-australiasemployees/ [Accessed 25 March 2020].

Yara International, 2018. Yara Birkeland [online]. Available from: https://www.yara.com/knowledgegrows/game-changer-for-the-environment/ [Accessed 24 April 2020].

Yilmaz, T., 2019. Doğu Akdeniz'de GKRY için en akılcı seçenek iş birliği [online]. Anadolu Agency. Available from: https://www.aa.com.tr/tr/turkiye/dogu-akdenizde-gkry-icin-en-akilci-secenek-is-birligi-/1488040 [Accessed 4 May 2020].

Additional important websites to see

https://www.westpandi.com/products/cyber-security/

https://www.mdpi.com/2077-1312/9/12/1384

https://www.steamshipmutual.com/publications/articles/insuranceact2015

https://www.clydeco.com/clyde/media/fileslibrary/Admin/

CC010256_Insurance_Act_2015_26-07-16-web.pdf

http://www.villagranlara.com/the-uk-insurance-act-2015-the-shift-in-marine-insurance-warranties-regime/

https://www.duo.uio.no/bitstream/handle/10852/50059/5070.pdf?sequence=1

https://www.amazon.com/Warranties-Marine-Insurance-Baris-Soyer/dp/1859419437

https://www.amazon.com/Warranties-Marine-Insurance-Baris-Soyer/dp/1138613967

https://www.westpandi.com/publications/news/archive/p-i-cover-and-cyber-risk/

https://www.allianz.com.tr/content/dam/onemarketing/aztr/allianz/pdf/diger/Tekne-Kloz-Metinleri-04022020.pdf

https://kennedyslaw.com/thought-leadership/article/cyber-exclusion-clauses-are-they-fit-for-purpose/

Read other items in the Marine Brief - June 2018

https://alphamrn.com/2021/03/08/questions-answers-from-the-webinar-cyber-security-in-the-maritime-environment/

https://alphamrn.com/wp-content/uploads/2010/10/Webinar-Cyber-Security-in-the-Maritime-Environment-QA-1.pdf

https://www.netsquare.gr/maritime-cyber-resilience-webinar-2021/

https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EL.pdf

Additional bibliography

1. DiRenzo, J.; Goward, D.A.; Roberts, F.S. The little-known challenge of maritime cybersecurity. In Proceedings of the 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA), Corfu, Greece, 6–8 July 2015; pp. 1–5.
2. Jensen, L. Challenges in maritime cyber-resilience. Technol. Innov. Manag. Rev. 2015, 5, 35. [CrossRef]
3. Alcaide, J.I.; Llave, R.G. Critical infrastructures cybersecurity and the maritime sector. Transp. Res. Procedia 2020, 45, 547–554. [CrossRef]
4. Fell, J. Mayflower tribute set to sail unmanned [automated marine transport]. Eng. Technol. 2015, 10, 42–44. [CrossRef]
5. Foundation, N. Demonstration Test of World's First Unmanned Operation of Small Tourism Boat Successfully Completed at Sarushima, Yokosuka. Available online: https://www.nippon-foundation.or.jp/en/news/articles/2022/20220111-67000.html (accessed on 14 January 2022).
6. Gu, Y.; Goez, J.C.; Guajardo, M.;Wallace, S.W. Autonomous vessels: State of the art and potential opportunities in logistics. Int. Trans. Oper. Res. 2021, 28, 1706–1739. [CrossRef]
7. Gu, Y.; Wallace, S.W. Operational benefits of autonomous vessels in logistics—A case of autonomous water-taxis in Bergen. Transp. Res. Part E Logist. Transp. Rev. 2021, 154, 102456. [CrossRef]
8. Werle, D.; Boudreau, P.R.; Brooks, M.R.; Butler, M.J.; Charles, A.; Coffen-Smout, S.; Griffiths, D.; McAllister, I.; McConnell, M.L.; Porter, I.; et al. The Future of Ocean Governance and Capacity Development. In The Future of Ocean Governance and Capacity Development; Brill Nijhoff: Leiden, The Netherlands, 2019; pp. 1–4.
9. Kavallieratos, G.; Katsikas, S.; Gkioulos, V. Cyberattacks against the autonomous ship. In Computer Security; Springer: Berlin/Heidelberg, Germany, 2018; pp. 20–36.
10. Tam, K.; Jones, K. Cyber-risk assessment for autonomous ships. In Proceedings of the 2018 International Conference on Cybersecurity and Protection of Digital Services (Cybersecurity), Scotland, UK, 11–12 June 2018; pp. 1–8.
11. Balduzzi, M.; Pasta, A.; Wilhoit, K. A security evaluation of AIS automated identification system. In Proceedings of the 30th Annual Computer Security Applications Conference, New Orleans, LA, USA, 8–12 December 2014; pp. 436–445.

12. LR. Cyber Enabled Systems. Available online: https://unece.org/fileadmin/DAM/trans/doc/2018/sc3wp3/07. LR.pdf (accessed on 31 January 2022).
13. CruisMapper. Cruise Ship Safety. Available online: https://www.cruisemapper.com/wiki/751-cruise-ship-safety (accessed on 3 February 2022). Network 2022, 2 136
14. Yastrebova, A.; H¨oyhty¨a, M.; Boumard, S.; Ometov, A. Comparative study on GNSS positioning systems for autonomous vessels in the arctic region. In Proceedings of the WiP Proceedings of the International Conference on Localization and GNSS (ICL-GNSS 2020), Tampere, Finland, 1–3 June 2020.
15. Kessler, G.C.; Craiger, J.P.; Haass, J.C. A taxonomy framework for maritime cybersecurity: A demonstration using the automatic identification system. Int. J. Mar. Navig. Saf. Sea Transp. 2018, 12, 429. [CrossRef]
16. Bhutani, A.; G¨ ottel, B.; Van, N.T.P.; Mukhopadhyay, S.; Demir, V. Advances in Radar Technology; Scientific Research Publishing: Wuhan, China, 2021; p. 245.
17. Kuzmichev, A.P.; Smirnov, V.G.; Zakhvatkina, N.Y.; Bychkova, I.A. Use of Satellite Communication Systems for Collecting and Transmitting Data on the State of the Arctic Sea Ice Cover. In Proceedings of the 2021 IEEE International Geoscience and Remote Sensing Symposium IGARSS, Brussels, Belgium, 11–16 July 2021; pp. 5732–5734.
18. FORSCOUT. Securing Ship Automation & Control Systems. Available online: https://www.forescout.com/resources/securingship- automation-control-systems/ (accessed on 31 January 2022).
19. Stouffer, K.; Falco, J.; Scarfone, K. Guide to industrial control systems (ICS) security. NIST Spec. Publ. 2011, 800, 16.
20. Ilcev, M. New Aspects for Modernization Global Maritime Distress and Safety System (GMDSS). Int. J. Mar. Navig. Saf. Sea Transp. 2020, 14, 519–530. [CrossRef]
21. S´aiz, V.M.M.; L´opez, A.P. Future trends in electric propulsion systems for commercial vessels. J. Marit. Res. 2007, 4, 81–100.
22. Scherer, T.; Cohen, J. The evolution of machinery control systems support at the naval ship systems engineering station. Nav. Eng. J. 2011, 123, 85–109. [CrossRef]
23. Kazak, N.; Frolova, S. Ship Automation and Control Systems. In Proceedings of the IX All-Russian Science-Practical Conference of Students, Postgraduates and Young Scientists, Kerch, Crimea, 6 May 2020; p. 46.
24. Ben Farah, M.A.; Ukwandu, E.; Hindy, H.; Brosset, D.; Bures, M.; Andonovic, I.; Bellekens, X. Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. Information 2022, 13, 22. [CrossRef]
25. Menhat, M.N.; Zaideen, I.M.M.; Yusuf, Y.; Salleh, N.H.M.; Zamri, M.A.; Jeevan, J. The impact of Covid-19 pandemic: A review on maritime sectors in Malaysia. Ocean. Coast. Manag. 2021, 105638. [CrossRef] [PubMed]
26. Chang, C.; Wenming, S.; Wei, Z.; Changki, P.; Kontovas, C. Evaluating cybersecurity risks in the maritime industry: A literature review. In Proceedings of the International Association of Maritime Universities (IAMU) Conference, Tokyo, Japan, 30 October–1 November 2019.
27. Larsen, M.H.; Lund, M.S. A Maritime Perspective on Cyber Risk Perception: A Systematic Literature Review. IEEE Access 2021, 9, 144895–144905. [CrossRef]

28. Marine Traffic. Available online: https://www.marinetraffic.com/en/ais/home/centerx:-12.0/centery:25.0/zoom:4 (accessed on 14 January 2022).
29. Androjna, A.; Brcko, T.; Pavic, I.; Greidanus, H. Assessing cyber challenges of maritime navigation. J. Mar. Sci. Eng. 2020, 8, 776. [CrossRef]
30. Lisa, V. $80 Million Yacht Hijacked by Students Spoofing GPS Signals. 31 July, Naked Security (Sophos). Available online: https://nakedsecurity.sophos.com/2013/07/31/80-million-yachthijacked-by-students-spoofing-gps-signals (accessed on 31 January 2022).
31. GPS World. State Department Issues Notice on North Korean Jamming. 2016. Available online: http://gpsworld.com/statedepartment-issues-notice-on-north-korean-jamming (accessed on 31 January 2022).
32. John, R. GPS fLaw Could Let Terrorists Hijack Ships, Planes. Fox News Tech. Available online: http://www.foxnews.com/tech/2013/07/26/exclusive-gps-flaw-could-let-terroristshijack-ships-planes.html (accessed on 31 January 2022).
33. Meland, P.; Bernsmed, K.; Wille, E.; Rødseth, Ø.; Nesheim, D. A retrospective analysis of maritime cybersecurity incidents. Int. J. Mar. Navig. Saf. Sea Transp. 2021, 15, 4. [CrossRef]
34. Analytica, O. Global maritime security risks rise with GNSS use. In Emerald Expert Briefings; Oxford Analytica: Oxford, UK, 2019; Volume 1.
35. Coffed, J. The Threat of GPS Jamming: The Risk to an Information Utility; Report of EXELIS: Herndon, VA, USA, 2014; pp. 6–10.
36. Schmidt, D.; Radke, K.; Camtepe, S.; Foo, E.; Ren, M. A survey and analysis of the GNSS spoofing threat and countermeasures. ACM Comput. Surv. 2016, 48, 1–31. [CrossRef]
37. Svilicic, B.; Brcˇic´, D.; Zˇ usˇkin, S.; Kalebic´, D. Raising awareness on cybersecurity of ECDIS. Int. J. Mar. Navig. Saf. Sea Transp. 2019, 13, 231–236.
38. Svilicic, B.; Kamahara, J.; Celic, J.; Bolmsten, J. Assessing ship cyber risks: A framework and case study of ECDIS security. WMU J. Marit. Aff. 2019, 18, 509–520. [CrossRef]
39. Kavallieratos, G.; Diamantopoulou, V.; Katsikas, S.K. Shipping 4.0: Security requirements for the cyber-enabled ship. IEEE Trans. Ind. Inform. 2020, 16, 6617–6625. [CrossRef]
40. Dyryavyy, Y. Preparing for Cyber Battleships—Electronic Chart Display and Information System Security; NCC Group: Manchester, UK, 2014.
41. Wu, Z.; Pan, Q.; Yue, M.; Ma, S. An Approach of Security Protection for VSAT Network. In Proceedings of the 2018 17th IEEE International Conference On Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1511–1516.
42. Santamarta, R. Maritime Security: Hacking into a Voyage Data Recorder (VDR). 2015. Available online: https://ioactive.com/maritime-security-hacking-into-a-voyage-data-recorder-vdr/ (accessed on 10 January 2022). Network 2022, 2 137
43. Pavur, J.; Moser, D.; Strohmeier, M.; Lenders, V.; Martinovic, I. A tale of sea and sky on the security of maritime VSAT communications. In Proceedings of the 2020 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 18–21 May 2020. Available online: https://ieeexplore.ieee.org/abstract/document/9152624?casatoken=WNlJxkEBkiMAAAAA:

M7VuGUYSWSjse0C9DUqJuH9gjFl9lWUO9MvFuZoCpEwuAX3BmKg57M9w2Z SfDfKM sTvYrwwgQ6P (accessed on 10 January 2021).

44. Tam, K.; Jones, K. MaCRA: A model-based framework for maritime cyber-risk assessment. WMU J. Marit. Aff. 2019, 18, 129–163. [CrossRef]

45. Heffner, C. Exploiting Surveillance Cameras Like a Hollywood Hacker. Available online: https://privacy-pc.com/articles/exploiting-network-surveillance-cameras-like-a-hollywood-hacker.html (accessed on 10 January 2021).

46. Bugeja, J.; J ¨onsson, D.; Jacobsson, A. An investigation of vulnerabilities in smart connected cameras. In Proceedings of the 2018 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Athens, Greece, 19–23 March 2018; pp. 537–542.

47. Shoultz, D. Securely Connected Vessels: Vessel Communications and Maritime Cybersecurity. Technical Report. 2017. Available online: https://www.maritimeprofessional.com/blogs/post/securely-connected-vessels-vessel-communicationsand-maritime-15176 (accessed on 9 July 2021).

48. Healey, J. Beyond Data Breaches: Global Interconnections of Cyber Risk; Atlantic Council: Washington, DC, USA, 2014.

49. Caprolu, M.; Di Pietro, R.; Raponi, S.; Sciancalepore, S.; Tedeschi, P. Vessels cybersecurity: Issues, challenges, and the road ahead. IEEE Commun. Mag. 2020, 58, 90–96. [CrossRef]

50. Al-Mhiqani, M.N.; Ahmad, R.; Yassin,W.; Hassan, A.; Abidin, Z.Z.; Ali, N.S.; Abdulkareem, K.H. Cyber-security incidents: A review cases in cyber-physical systems. Int. J. Adv. Comput. Sci. Appl. 2018, 1, 499–508.

51. Forscout. Spoofing in the Black Sea: What Really Happened? Available online: https://www.gpsworld.com/spoofing-in-theblack-sea-what-really-happened/ (accessed on 31 January 2022).

52. Borger, J. Pentagon Orders Temporary Halt to US Navy Operations after Second Collision. Available online: https://www.theguardian.com/us-news/2017/aug/21/us-destroyer-uss-john-s-mccain-damaged-after-collision-with-oil-tanker (accessed on 31 January 2022).

53. Cohen, Z. US Navy Ship Collides with South Korean Fishing Boat. Available online: https://edition.cnn.com/2017/05/09/politics/fishing-vessel-hits-us-navy-ship-south-korea/index.html (accessed on 31 January 2022).

54. Roberts, F.S.; Egan, D.; Nelson, C.; Whytlaw, R. Combined cyber and physical attacks on the maritime transportation system. NMIOTC Marit. Interdiction Oper. J. 2019, 18, 22.

55. Oruc, A.; MIMarEST, M.S.M. Claims of State-Sponsored Cyberattack in the Maritime Industry. In Proceedings of the 15th International Naval Engineering Conference & Exhibition, Delft, The Netherlands, 6–8 October 2020.

56. Winder, D. U.S. Coast Guard Issues Alert after Ship Heading into Port of New York Hit By Cyberattack. Available online: https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-portof-new-york-hit-by-cyberattack/?sh=61b920e741aa (accessed on 31 January 2022).

57. Cooper, H. Chinese Hackers Steal Unclassified Data from Navy Contractor. 2018. Available online: https://www.nytimes.com/2018/06/08/us/politics/china-hack-navy-contractor-.html (accessed on 31 January 2022).

58. Maritime-Executive. Cyberattack Hits Multiple Greek Shipping Firms. Available online: https://www.maritime-executive.com/article/cyberattack-hits-multiple-greek-shipping-firms (accessed on 3 February 2022).
59. Bebbington, T. Cyberattack or Coincidence? Available online: https://www.seatrade-maritime.com/opinions-analysis/cyberattack-or-coincidence (accessed on 3 February 2022).
60. The Guidelines on Cybersecurity Onboard Ships. Available online: https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018 12.pdf (accessed on 3 February 2022).
61. Nicaise, V. Cybermar´etique: A Short History of Cyberattacks against Ports. Available online: https://www.stormshield.com/news/cybermaretique-a-short-history-of-cyberattacks-against-ports/ (accessed on 3 February 2022).
62. Team, E. Maersk Line: Surviving from a Cyber Attack. Available online: https://safety4sea.com/cm-maersk-line-survivingfrom-a-cyberattack/ (accessed on 3 February 2022).
63. Rosehana Amin, R.D.; Jones, D. Part 1: A Very Modern Form of Piracy: Cybercrime against the Shipping Industry—Rapidly DevelopingRisks. Available online: https://www.clydeco.com/en/insights/2021/03/a-very-modern-form-of-piracy-cybercrimeagainst-th (accessed on 3 February 2022).
64. Elliott, L. Port of Houston Target of Suspected Nation-State Hack. Available online: https://www.nbcnews.com/tech/security/port-houston-target-suspected-nation-state-hack-rcna2249 (accessed on 3 February 2022).
65. Silverajan, B.; Ocak, M.; Nagel, B. Cybersecurity attacks and defences for unmanned smart ships. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 15–20.
66. Bothur, D.; Zheng, G.; Valli, C. A critical analysis of security vulnerabilities and countermeasures in a smart ship system. In Proceedings of the 15th Australian Information Security Management Conference, Perth, Australia, 5–6 December 2017.
67. Zhou, X.; Liu, Z.;Wu, Z.;Wang, F. Quantitative processing of situation awareness for autonomous ships navigation. Int. J. Mar. Navig. Saf. Sea Transp. 2019, 13, 25–31. [CrossRef] Network 2022, 2 138
68. Reddy, G.N.; Reddy, G. A study of cybersecurity challenges and its emerging trends on latest technologies. arXiv 2014, arXiv:1402.1842.
69. Petkovi´c, M.; Vujovi´c, I. Blockchain security of autonomous maritime transport. J. Appl. Eng. Sci. 2019, 17, 333–337. [CrossRef]
70. Bechtsis, D.; Tsolakis, N.; Bizakis, A.; Vlachos, D. A blockchain framework for containerized food supply chains. In Computer Aided Chemical Engineering; Elsevier: Amsterdam, The Netherlands, 2019; Volume 46, pp. 1369–1374.
71. Ahmad, R.W.; Hasan, H.; Jayaraman, R.; Salah, K.; Omar, M. Blockchain applications and architectures for port operations and logistics management. Res. Transp. Bus. Manag. 2021, 41, 100620. [CrossRef]
72. Wullems, C.; Pozzobon, O.; Kubik, K. Signal authentication and integrity schemes for next generation global navigation satellite systems. Eur. J. Navig. 2005, 3, 4.
73. Caparra, G.; Sturaro, S.; Laurenti, N.; Wullems, C.; Ioannides, R.T. A novel navigation message authentication scheme for GNSS open service. In

Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Portland, OR, USA, 12–16 September 2016; pp. 2938–2947.

74. Brcˇic´, D.; Kos, S.; Zˇ usˇkin, S. Navigation with ECDIS: Choosing the proper secondary positioning source. Int. J. Mar. Navig. Saf. Sea Transp. 2015, 9, 317–329.

75. Bour, G.; Bernsmed, K.; Borgaonkar, R.; Meland, P.H. On the certificate revocation problem in the maritime sector. In Proceedings of the Nordic Conference on Secure IT Systems, Aalborg, Denmark, 29–30 November 2020; Springer: Berlin/Heidelberg, Germany, 2020; pp. 142–157.

76. Rødseth, Ø.J.; Frøystad, C.; Meland, P.H.; Bernsmed, K.; Nesheim, D.A. The need for a public key infrastructure for automated and autonomous ships. In Proceedings of the IOP Conference Series: Materials Science and Engineering, Ulaanbaatar, Mongolia, 10–13 September 2020; Volume 929, p. 012017.

77. Seo, S.H.; Lee, B.H.; Im, S.H.; Jee, G.I.; Kim, K.S. Efficient spoofing identification using baseline vector information of multiple receivers. GPS Solut. 2018, 22, 1–14. [CrossRef]

78. Mrakovi´c, I.; Vojinovi´c, R. Maritime cybersecurity analysis—How to reduce threats? Trans. Marit. Sci. 2019, 8, 132–139. [CrossRef]

79. Tam, K.; Jones, K.D. Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. J. Cyber Policy 2018, 3, 147–164. [CrossRef]

80. Jones, K.D.; Tam, K.; Papadaki, M. Threats and Impacts in Maritime Cybersecurity. Master’s Thesis, University of Plymouth, Plymouth, UK, 2016.

ANNEXES OF COURT DECISIONS[27]

[28][29]Case No: A3/2015/2525 Neutral Citation Number: [2017] EWCA Civ 365IN THE COURT OF APPEAL (CIVIL DIVISION) ON APPEAL FROM THE HIGH COURT QUEENS BENCH DIVISION Mr. Justice Andrew Smith 2013FOLIO424 Royal Courts of Justice Strand, London, WC2A 2LL Date: 24/05/2017 Before :LORD JUSTICELEWISON LORD JUSTICE HENDERSON and SIR CHRISTOPHER CLARKE -between: MSC Mediterranean Shipping Company S.A. Appellant - and - Glencore International AG Respondent -Michael Howard QC and Yash Kulkarni (instructed by Duval Vassiliades) for the Appellant John Passmore QC (instructed by Gateley Plc) for the Respondent Hearing dates: From January 2011toJune 2012,Glencore International AG ("Glencore")69 shipments of cobalt briquettes indrumstrans ported to Antwerpby Mediterranean Shipping Company SA ("MSC"). This case concerns the 70thsuchshipment, a cargo equivalent to three containers. Respondent Glencore was the holder of the bill of lading ("B/L") and the owner of the cargo; MSC was the carrier. After the cargo was unloaded in Antwerp, two of the three containers were misappropriated.69All oft he cargo was transported under a bill of ladingsubstantiallysimilartothetermscontainedinthebillofladinq("B/L").2.Thefollowing four companies were involved in Antwerp: (i) C Steinweg NV ("Steinweg")was Glencore's agent at that port and was the notified party to the B/L(ii) Carjo Trans BVBA ("Carjo Trans")was a carrier employed by Steinweg. The terminal was an open yard with a secure perimeter;3. The Port operated an Electronic Release System("ERS"). Under this system, based on the bill of lading, the carrier provided a computer-generated electronic number ("import pin code") that was passed to the relevant consignee or its agent and the port terminal. This was in lieu of a delivery order or release note to be presented to the terminal for acceptance of the cargo. The owner of the bill of lading had to present the pin code to the terminal in order to take delivery of the cargo. In practice, the pickup driver had to manually enter the pin code to access the terminal. Collect the containers.4.Thissystem was introduced at the beginning of 2011.Thesystem is not mandatory and has not been adopted by all carriers using the port. under the ERS, in so far as it applies to MSC, upon presentation of the bill of lading by the consignee or its local agent and payment of any outstanding freight or other charges, MSC Belgium's Import Operations Department,sentareleasenotewithpincodestothedesignatede-mailaddress. These were also sent to the port terminals via electronic data inter change. Each code corresponded to a code that was automatically generated by the systemandstoredinencryptedformintthePortAuthority'sdatabasewhentherelevantemployeeofthedepartmentclickedabuttononthecomputerscreenwiththemouse.Copiesof the emails with attached release notes containing the codes were not stored in the outboxes of the Bureau's assistants. Hard copies of the release notes were available from the MSC Belgium data base, but only with the approval of someone at a senior level in the computer department.5. Steinweg acted as Glencore's agent foreach of the 69 shipments; Steinweg presented the original bills of lading to MSC or MSC Belgium and on each occasion delivered the shipments by pin code from the MSCterminaloperatedbyMSCHomeforMSC.6. The judge described the usual

[27] https://www.quadrantchambers.com/news/mediterranean-shipping-company-sa-v-glencore-international-ag-2017-ewca-civ-365-msc-eugenia
[28] http://beta.bailii.org/ew/cases/EWCA/Civ/2017/365.rtf
[29] http://beta.bailii.org/ew/cases/EWCA/Civ/2017/365.html

sequence of events as follows:"Shortly before the vessel arrived in Antwerp, MSC sent a 'notice of arrival' to Steinweg, informing it of the estimated time of arrival ("ETA"). After the invoice was presented and the freight and charges were paid, MSC sent Steinweg an electronic document entitled "Release Note," which contained a pin code (or codes) for releasing the cargo and the period during which thecodeswere"valid"(typicallyapproximatelyonemonthfromthevessel'sdeparture).Unde rthe heading "Terms and Conditions Applicable to the Subject Receipt Note, "there lease note contained the following provisions (thesecondofwhichwasgenerally,thoughnotalways,underlined)ThepayeeoftheSubjectR eceiptNoteexpressly confirms that it knows and unconditionally accepts these terms and conditions. o *"This release note is subject to the terms and conditions contained in the Resolution by Alfaport Antwerp dated 3rd of September 2010 concerning electronic release of containers in the port of Antwerp. The text of this Resolution is available on our website …. The addressee of this release note expressly confirms to have knowledge of these terms and conditions and to accept them unconditionally.* o *"Discharge of the cargo will constitute due delivery of the cargo. After discharge the cargo will remain on the quay at risk and at the expense of the cargo, without any responsibility of the shipping agent or the shipping company/carrier".* 7. These quence of events regarding the subject cargo is as follows The bill of lading(B/L)issued onMay21,2012statesthatMSCreceivedthreecontainerscontaining drums of cobalt metal briquettes at the port of shipment (Fremantle, Australia). The port of discharge was Antwerp. ThecargowasloadedonMay20, 2012 aboard the "MSC Eugenia". The Bill was a negotiable bill, marked "To order". It provided: *"If this is a negotiable (To Order/of) Bill of Lading, one original Bill of Lading, duly endorsed must be surrendered by the Merchant to the Carrier (together with outstanding freight) in exchange for the Goods or a Delivery Order"*. The B/L expressly stated the choice of English law and conferred exclusive jurisdiction on the English High Court of Justice.9. OnMay24,2012, Glencore sent two copies of the B/L and other documents to Steinweg. OnJune20,2012, MSC sent Steinweganoticeofarrivalwithanestimatedarrivaldateof June24,2012,forthe"MSCKatrin a"withthetransshippedgoods; Steinweg submitted a copy of the B/L signed and sealed by itself and Glencoreto MSC Belgiumand paid thefee.sentareleasenotetoSteinwegviaemail.Thereleasenotecontained three pin codes(one for each container), which were validuntilJuly25,2012OnJune26,2012,thecargoarrived at the port. The container was discharged and placed at the MSC terminal; onJune26,2012, Steinweg notified the carrier, Carjo Trans, of the pin codes. [30]10. On 27 June 2012 when Carjo Trans went to collect the containers,[31] it found that two of them had already been collected. It reported this to Steinweg and the Port Authority confirmed this to Steinweg[32] as well. Exactly what happened to the two containers is unknown but it was common ground[33] that they were delivered to "unauthorized persons"; and the judge thought it most likely that the loss occurred after someone had learnt of the codes and had used them to steal the containers[34]. This appears to have been the first time that MSC had had a problem of this kind when using the ERS[35]. After the loss MSC and Steinweg adopted

[30] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[31] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[32] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[33] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[34] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[35] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf

certain measures, described at [15] of the judgment, to avoid it happening again. 11. On 25 March 2013 Glencore issued a claim against MSC claiming damages for breach of contract, bailment and conversion[36]. It also claimed against MSC Home. The claim against the latter was not pursued. On 10 July 2015, following a hearing on 6 and 7 July 2015, Andrew Smith J gave judgment in favour of Glencore. By the start of the trial title to sue had been agreed; as had damages, subject to liability, in the sum of US $ 1,109,364.78; and the live issues between the parties had been reduced to four. *The issues at trial* 12. The first issue was whether MSC's provision of the pin codes to Steinweg constituted provision of a Delivery Order within the meaning of the B/L[37]. MSC contended that, when Steinweg on behalf of Glencore tendered a copy of the B/L to MSC Belgium, MSC[38] was then obliged to exchange it either for the goods or for a Delivery Order[39]. MSC did not then contend that it delivered the containers in exchange for the B/L. Nor did it rely on the provision in the Release Note which said that discharge of the cargoes would constitute due delivery[40]; nor did it argue that it delivered the containers by putting them into storage to await collection by Carjo Trans[41]. That the B/L was exchanged for a delivery order consisting of an electronic pincode.13Thetrialjudge rejected this argument. He held that the parties must be deemed to have referred to a delivery order for a vessel as provided in section 1(4) of the Carriage of Goods by Sea Act 1992.Thesaidsection provides as follows.: *"References in this Act to a ship´s delivery order are references to any document which is neither a bill of lading nor a sea waybill but contains an undertaking which– (a) is given under or for the purposes of a contract for the carriage by sea of the goods to which the document relates, or of goods which include those goods; and (b) is an undertaking by the carrier to a person identified in the document to deliver the goods to which the document relates to that person."* The essential feature of such a document is that it contains an under taking by the carrier (or, in some cases, a person undertaken by the carrier by delegation) to deliver to the person identified in the document the goods to which he or she relates. Are lease note contain in gap in code is not a document containing such an undertaking.14Usually,thereason for agreeing that the delivery order, rather than the goods, maybe delivered is, as the judge observed, to expedite performance of the contract, particularly in the case of bulk cargo (for these purposes, one The reason for the agreement was, as the judge observed, to expedite the performance of the contract and, in particular, to allow bulk cargoes(for these purposes, one bill contains three containerized cargoes) to be divided into parcels without resorting to the dangerous practice of issuing bills in lieu of payment. The judge considered that the shipper could not possibly agree to terms under which the holder of the bill of lading might waive his rights under the bill of lading against the carrier without receiving in return the goods or the benefit of a substituted undertaking from the carrier [19]. It held that the language was not understood by the parties in abroad sense, and that the parties' previous pattern of dealing did not support a more generous interpretation of thelanguage.15. Thetrialcourtfoundthreeobstaclestoanargumentbasedonthepreviouspatternofdealing.
The firstis.: *"22 …although in principle the factual background can sometimes inform the interpretation of a negotiable document of title, there is an obvious difficulty*

[36] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[37] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[38] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[39] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[40] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf
[41] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf

about a document having "different meanings for different people according to the knowledge of the background" (to use the words of Lord Hoffmann in Mannai Ltd v Eagle Star Assurance Co Ltd, [1997] 749, 779C/D). The proper approach to using the background knowledge to inform the interpretation of bills of lading was explained by Lord Hoffmann in Homburg Houtimport BV v Agrosin Private Ltd (The "Starsin"), [2003] UKHL 12 at paras 73ff: it is to be recognised that negotiable bills of lading, being documents of title, are "addressed" to and might need to be understood by various persons other that the original parties, and therefore the original parties are taken to have intended that they should be given the meaning conveyed by their wording in light of knowledge available to the range of persons to whom they are addressed. Thus, "As it is common knowledge that a bill of lading is addressed to merchants and bankers as well as lawyers, the meaning which it would be given by such persons will usually also determine the meaning it would be given by any other reasonable person, including the court. The reasonable reader would not think that the bill of lading could have been intended to means one thing to the merchant or banker and something different to the lawyer or judge" (at para 76). The parties making the contract in the B/L would not have expected the range of addressees described by Lord Hoffmann to know of their own previous dealings, and are not to be taken to have intended that it should inform the interpretation of the B/L." 16. The second obstacle, as the judge found, is that Glencore did not know of the use of the ERS in Antwerp until the loss occurred, and therefore did not know of its use at the time it executed the B/L. Steinweg was Glencore's agent for the purpose of executing the bill of lading and the freight forwarding contract was not Glencore's agent and its knowledge was not adequate to determine Glencore's contractual intent when it entered into the B/Lagreement.17The third obstacle is that MSC failed to determine, in light of its prior pattern of transactions, that the B/L would (i) allow MSC to use ERS and deliver or deliver the goods immediately after the bill of lading was delivered, or(ii) allow MSC to use ERS to order and only allowed the goods to be delivered when the code was presented to the port authority, but also (ii) that MSC must show that when it provided the pin code for the earlier cargo, it was there by deemed to have fulfilled its responsibilities with respect to the cargo and its delivery. The earlier transaction did not support this position. Even if Glencore had agreed to use the pin code, it did notnecessarilyagreethatdeliverywouldbedeemedtohavetakenplacewhenthepincodewas sent to Steinweg, rather than when the cargo was later received.18 In [25] of the decision, the judge stated.: *"MSC does not, of course, submit that, by providing the release note containing the pin codes, it undertook to Glencore or Steinweg that it would deliver the cargo to them: had it done so, it would clearly have been in breach of its undertaking. Mr Kulkarni's primary submission is that it thereby gave no undertaking at all with regard to delivery: his alternative submission is that, if MSC gave any undertaking, it was only that the goods would be delivered to whoever presented the right codes, and it did not undertake to deliver them to Steinweg or Glencore. Thus, it accepts that it did not give in exchange for the B/L a Delivery Order of the kind that I have described and that, in my judgment, was required by the B/L. I therefore conclude that MSC did not comply with its obligations under the B/L, unless it can rely on an implied term or show that it was varied by agreement."* 19. The second issue was whether the past course of transactions between MSC and Glencore formed the basis for the provisions to be implied in the B/L that[42]: *"upon surrender of the bill of lading by a lawful holder, a carrier or its agent may provide*

[42] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf

an import pin code… (so that thereafter the recipient of the import pin code can present the import pin code to take delivery of containerised cargo, provided always that the import pin code matches the corresponding [electronic data interchange] pin code)" 20. The trial court rejected this implied condition on the ground that it was incompatible(if not inconsistent) with the express condition in the B/L that the goods be offered in exchange for the goods or the order for delivery. Although the parties relieved the carrier of its prima facie obligation to deliver the goods only against delivery of the B/L by agreeing that Glencore might deliver the goods in exchange fora delivery order, the very fact that they agreed to such a limited relief made it difficult to believe that they intended anything more than The very fact that they agreed to such a limited relaxation made it difficult to believe that they intended anything more.[43]. 21. The implications had additional difficulties. Airlines were not obligated to use the ERS, and not all airlines used the ERS. Moreover, the implication of ownership from the course of dealings between the original parties into the document faced objections, such as those expressed by Lord Hoffman in"Stasin,"that background known only to the original parties would dictate interpretation. Moreover, the implication that MSC or its agent used the ERS to provide the pin code, and that by providing it MSC fulfilled its obligations with respect to the delivery of the cargo and was relieved of its responsibilities in the contract and the deposit, would be necessary for any usefulness. There is no appropriate reason to introduce such a clause by implication. 22. The third issue was whether MSC's January 2011 letter to Steinweg modified the terms of the B/L so that it could be exchanged for a valid pin code under the ERS. The judge rejected this suggestion and no appealwasfiledonthispoint.23The fourth issue was whether Glencore was barred from claiming that the delivery of the cargo upon presentation of the pin code was a breach of contract and/or a breach of duty by MSC. In this regard, the judge found no basis to conclude that Glencore represented or acted in a manner that would lead one to understand that it would be satisfied if it delivered the cargo to the person who presented the correct pin code. The judge's finding that Glencore's knowledge of the use of ERS was limited was also an answer to the estoppel claim. 24 Reasons for Appeal Reason1: Pin Code as (Symbolic)Delivery25.Michael Howard, Esq. for MSC, Heargues that the judge erred in failing to find that the provision of the pin code to Steinweg itself amounted to a delivery of title to the goods under the law. The judge argues that here are two general rules that are relevant. One is that a carrier who makes a delivery not pursuant to a bill of lading is placing himself or herself at risk. The other is a limitation on the former. The other is that delivery maybe made by the symbolic act of a metonym of the cargo being given to the receiver.26 In this regard, here lies on a classic case, Glyn Mills v East and West India Dock Co (1882) 7 App Cas 591 He relies on the classic case of Glyn Mills v East and West India Dock Co (1882) 7 App Cas 591.Thiscaseestablishesthateven if the original genuine bill of lading is marked "second," there is a duty on the part of the carrier to deliver the goods to that person unless the carrier is informed that some one else is in possession of the goods. 1 (However, this is not true of a counterfeit bill of lading. (However, a forged bill of lading is void: [2000] 1 Lloyd's Rep 211 at [19]-[20]. Similarly, in the present case, he argues, there should be no difficulty in regarding the delivery of the pin code as a relevant symbolic act, and in regarding possession of the pin code as conferring on the holder the right to take delivery of the goods; the carrier's duty is to deliver the pin code to the person who first entered it into the machine.Intheearly21st century, he argues, now that ports like Antwerp are using ERS, it makes no sense to

[43] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf

distinguish between the presentation of a paper bill of lading and the use of a code that would provide at least equal, if notgreater,security.27.Delivery of the pin code is equivalent to delivery of the goods in law The argument that delivery of a pin code is equivalent to delivery of goods as a matter of law was not presented in the lower court. However, we find it unpersuasive for the following reasons:28. In this context, we do not find it at all helpful to speak of delivery by symbolic act. If the carrier delivered the cargo to the first presenter of a genuine bill of lading, the presenter did not merely receive the bill of lading or take delivery by some symbolic act. The shipper secures actual delivery of the cargo against presentation of the bill. A related question is to whom does the carrier (in fact) make delivery? The classic answer is" the first presenter of the bill of lading."29 The MSC argues that delivery need not be only a physical transfer of property. Symbolic or constructive delivery is also possible, a typical example of which is as follows Generally speaking, several subsequent cases have established that the carrier's duty is to deliver to the first presenter of the bill of lading: Sze Hai Tang Bank Ltd v Rambler Cycle Co. Ltd [1959] AC 577.586; The Somorvesky [1994] 2 Lloyd's Rep 266,274.delivery of the keys to the warehouse where the goods were stored; Benjamin's parastates.: *"Delivery may be effected by the handing to the buyer the key of a warehouse or other place where the goods are stored, provided that a licence to enter and take the goods can be implied..."* A number of authorities from 1789 to 1921 are cited. 30 One of these, Dublin City Distillery v Doherty [1914] AC 823, in which Lord Atkinson considered the authority on constructive delivery and referred to the delivery of a warehouse key as an example of delivery In the case of the case of the plaintiff, the plaintiff was a distiller's company. In that case, the plaintiff had loaned money to a distillery company as security for the storage of manufactured whisky in a warehouse, and there were two keys to the warehouse door, one kept by the company and the other by a customs officer. The whisky was subject to a valid pledge, which pledge was subject to the following conditions: (i) a document called a war rant issued by the distillery company to the plaintiff, which detailed the whisky and stated that it could be "delivered" to the plaintiff or his assignee;(ii) the company had a pledge that each time an advance was made, the(iii) that the company consisted of a combination of (i) that it entered the plaintiff's name in pencil in the stock ledger for the whisky that was to be pledged and delivered to the plaintiff. Lord Atkinson held that this evidence did not establish that there was a constructive delivery of the whisky to the plaintiffs. Lord Atkinson stated as follows: *"the giving by the owner of goods of a delivery order to the warehouseman does not, unless some positive act be done under it, operate as a constructive delivery of the goods to which it relates" and "the delivery of a warrant was, in the ordinary case, …. no more than an acknowledgment that the goods are deliverable to the person named therein or to anyone he may appoint. The warehouseman holds the goods as the agent of the owner until he has attorned in some way and agreed to hold the goods for him; then and not until then, does the warehouseman become a bailee for the latter; and then, and not until then, is there a constructive delivery of the goods. The delivery and receipt of the warrant does not per se amount to a delivery and receipt of the goods."* Lord Parker considered that " as a whole, "the war rant implied that the company had authorized the plaintiff or its assignees to hold the goods for them. In other words, at common law, this was a fine pledge. Lord Sumner took the same view as Lord Atkinson.31This case concerned a pledge achieved by the endorsement and delivery of a bill of lading. We do not believe that this precedent assists MSC in the present context, i.e. delivery under a contract of carriage. Whether the delivery of the means of access to the goods

constitutes the delivery required by such a contract must depend on the context and terms of the contract. In the present case, since the parties contemplated either actual delivery contingent up on presentation of a bill of lading or delivery pursuant to a delivery order, delivery of the code itself cannot be considered to constitute delivery. Delivery usually means actual delivery and not delivery of the means of access. Nor does the fact that MSC Belgium sent are lease note imply that MSC Home was obligated to Glencore with respect to the goods or that it had stored the goods on Glencore's be half from that point on.32 An example of a symbolic delivery that is customarily given is the provision of a key to a warehouse. This example assumes that the key opens the door and the goods are there. In this case, by entering the number, only one of the three containers was accessible; the MSC would say that the container already delivered (by providing the PIN) was stolen when it belonged to Glencore. It would depend on whether the theft was before or after the provision of the code to TEINWEG. It is unlikely that the parties intended that Glencore's rights would depend on such circumstances. 233 Theargument now presented was not presented in the lower court, but the judge addressed the issue of what constitutes extradition as follows: *“ 17 …..…[MSC] does not contend that it met its obligation under the B/L by delivering to Glencore the goods in exchange for it. Nevertheless, I shall say something about what would constitute delivery of goods in order to set the scene for the parties' submissions on what is in issue. In the context of the sale of goods, Sale of Goods Act, 1979 s.61(1) provides a general definition of "delivery" as "voluntary transfer of possession from* 2 Although the key to the warehouse is often referred to as a means of symbolic delivery, careful consideration would need to be given, in any specific case, as to what exactly the contract contemplated. It must be doubtful, for instance, whether delivery of the key is sufficient if the donor retained a spare – a question which would be relevant if the goods were stolen before the buyer had entered into actual possession. *one person to another". In Barclays v Customs & Excise, [1962] 1 Lloyd's Rep 81,89, Diplock J observed that a bill of lading contract is "not discharged by performance until the shipowner has actually surrendered possession (that is, has divested himself of all powers to control any physical dealing in the goods) to the person entitled under the terms of the contract to obtain possession of them". Thus, as it is put in Cooke on Voyage Charters (4th Ed, 2014) at para 10.4, delivery is "a bilateral act, involving the receipt of the goods by the consignee or his agent as well as the relinquishing of possession by the carrier, and so it cannot be effected merely by discharging the goods over the ship's side at the port of delivery. Equally delivery cannot, in the absence of special terms, be effected merely by putting the goods into the custody of a person who is not the agent of the consignee". 18 Mere discharge of cargo therefore does not constitute delivery as a general rule. ….. In some circumstances, delivery might be effected by putting goods into a port authority's custody, but it is accepted that this did not happen here. First, the goods were not deposited into the custody simply of the Port Authority: they were put into the MSC Terminal. The evidence does not make clear quite what role the Port Authority had in managing goods that were stored there, but the MSC Terminal was operated by MSC Home and operated for MSC. Secondly, although by emailing the pin codes MSC Belgium provided Steinweg with the means to take possession of the goods as long as they were valid, as I have explained, under the ERS in so far as its procedures reflected the model covenants, MSC Belgium had at all times the power, albeit not the contractual right as against Glencore or Steinweg, to invalidate them. To that extent, MSC did not, in Diplock J's words, divest itself of all powers to control*

any physical dealing in the goods." 34. [4445]Mr. Howard argues that this analysis was flawed. There are two model provisions approved by the Antwerp Port Authority in its September 3, 2010 resolution.[46] agent and (i) the terminal operator and (ii) the forwarder. The former entitled the shipping company or ship's agent to announce that the "*release has expired or has been withdrawn*". The latter provided for the "*release*" (i.e. the making available for delivery) being withdrawn if the container was not withdrawn within the free period specified in the release note or if during that period additional costs were incurred or in other special cases. These covenants were, as the judge found [10], never agreed by MSC with the Port Authority or with Steinweg. All that he found was that the ERS was operated by the parties "*broadly as the covenants contemplated*" [10]. In those circumstances it is unclear, Mr Howard submits, why the judge thought that the pin codes might be revocable at all. The fact that MSC Home operated the Terminal for MSC would not give MSC any control over MSC Home's activities; nor was there anything to suggest that once pin codes were generated MSC could revoke the codes or countermand the handing over of the goods by MSC Home. Even if such revocation was physically possible, of which there was no evidence, it could not legitimately have been done. If it was physically possible for the codes to be recalled by MSC, such revocation would not affect the delivery that had taken place by their provision; and the legal effect of that recall would be that, delivery having taken place, MSC would be guilty of conversion. 35. I do not find consideration of the revocability of the codes by or at the behest of MSC to be particularly fruitful because, as I have said, the most important question is as to what form of delivery the contract contemplated. Nor do I think *Barclays Bank v Customs & Excise* (see [33] above) to be of assistance to MSC. The case did not concern symbolic delivery but whether the bill of lading could effectively be pledged to a party other than the consignee after the goods had been discharged but before they had been delivered to the consignee. They had not been delivered because they were in the possession of a custodian who held the goods to the order of the shipowners and who had made no acknowledgment that he was holding them on behalf of the consignee. 36. Lastly, the judge was satisfied that MSC Belgium had the power, albeit not the contractual right, as against Glencore or Steinweg to invalidate the codes [18] and thus prevent delivery of the containers. The basis of this was his inference at [10] that MSC "*operated the ERS broadly as the covenants contemplated"*. Those covenants provided for withdrawal of "*the release*" by the shipping company or its agent: see [34] above. This power was expressed by the judge as being "*under the ERS in so far as its procedures reflected the model covenants"*. The use of the expression "*in so far as*" is, perhaps, not wholly clear but I take the judge to be saying that the ERS procedure did in fact reflect the model covenants in this respect so that the reality was that MSC Belgium would be able to prevent delivery: see what he said in [10]. Further the Release Note incorporated the terms of the Alfaport Antwerp Resolution which approved the two model covenants. So someone claiming the benefit of the Release Notes would have to recognise the power of recall by MSC of the release contemplated by those covenants, even though such recall might involve a breach of obligations as to delivery. Article 1 of the operator's covenant provided that the conditions of the covenant applied "*without prejudice to the applicable legal and contractual provisions*". 37. The judge also accepted that MSC Home would act at MSC Belgium's behest (and, thus, that of

[44] http://beta.bailii.org/ew/cases/EWCA/Civ/2017/365.rtf
[45] http://beta.bailii.org/ew/cases/EWCA/Civ/2017/365.html
[46] http://beta.bailii.org/ew/cases/EWHC/Comm/2015/1989.rtf

MSC its principal) because the Terminal was "*operated for MSC*". That seems to me an inference that he was entitled to draw, particularly having regard to the fact (i) that the goods, once discharged, were being stored for MSC, a situation which continued after the provision of the codes and (ii) the provisions of the operator's covenant which, on the judge's finding, the procedures of the ERS reflected and which entitled the shipping company to forbid release of the goods. 38. Accordingly, the judge held, MSC did not, in Diplock J's words divest itself of "*all powers to control any physical dealing with the goods*" [18]. 39. The finding set out in the previous paragraph begs the question as to what is relevant in this context. Is it whether in practice MSC had power to prevent release against the codes or whether it could, vis a vis Glencore, legitimately do so? Mr Howard submits that it must be the latter since otherwise symbolic delivery could almost never take place. The seller of goods who tendered the key to the warehouse can always change the locks. 40. It seems to me that Diplock J was concerned with practice rather than legitimacy. In determining whether delivery has actually occurred it is the position in practice that is relevant. He was concerned, as his language indicates, with whether the shipowner had "actually surrendered possession", That practical ability to prevent discharge was the criterion (as opposed to legitimate entitlement to do so) was also the approach adopted by this court in *The Jag Ravi* [2012] 1 Lloyd's Rep 637, where at [45] Tomlinson LJ referred to the possibility that the ship-owner might attempt to revoke the authority given by a delivery order, and might succeed in doing so, as a relevant consideration in determining whether delivery had taken place. I would accept that, in the ordinary case, where a shipowner discharges goods into a storage facility the goods remain undelivered so long as any order given by the shipowner to the facility remains revocable. Thus in *The Jag Ravi* the court rejected the proposition that the discharge of the cargo and the issue of a delivery order in the form of a request to the yard to deliver, constituted delivery within the meaning of the letter of indemnity. 41. Neither of those cases were cases of symbolic delivery. In the first the court was concerned to discern when (actual) delivery had been made under a bill of lading contract. In the second the question was whether delivery had taken place within the meaning of a letter of indemnity. I would accept that where the parties have agreed that symbolic delivery suffices, then such delivery takes place when the symbol is delivered, notwithstanding that the deliverer of the symbol may in practice be able to deprive the recipient of the actual goods after the symbol has been handed over, or does so, the remedy in the latter case being in conversion. 42. In the present case the B/L does not, in my judgment, provide that provision of the pin codes amounts to delivery. At best the code was some form of delivery order. *Ground 2 The Release Note and pin codes as a Delivery Order* 43. MSC submits, in the alternative, that the Release Note containing the pin codes was itself a Delivery Order for the purposes of the bill of lading. 44. The expression "Delivery Order" is not defined in the B/L; and the term is capable of different meanings. It may mean an order given by an owner of goods to someone who is in possession, or who is expected to come into possession, of the goods to deliver them to the person named in the order. That person may be a warehouseman or other bailee. (MSC contends that the Release Note was at least that. The provision of the codes to Steinweg was a means of instructing the Terminal to deliver to whoever entered the correct codes.) It may be a statement by a person in possession of goods that he will deliver them to a specified person. It may constitute an undertaking to deliver to the person specified in the order. It may be both an instruction and an undertaking. In each case the order may or may not cover assignees. 45. The expression "ship's delivery order" depends, at common law on the

context in which it occurs: see *Carver on Bills of Lading* (3rd edition) 8 -030. In essence "*the document should give the person in whose favour it is issued some rights (probably of a contractual nature) against the ship*": ibid 8-031. For the purposes of CoGSA 1992 it has the definition set out in [13] above. 46. I agree with the judge that, under an English law contract, such as the present, a delivery order should be regarded as having the same meaning as a ship's delivery order, as now defined under CoGSA *1992*, subject to the minor qualification in [61] below. The Delivery Order is to be provided by the owners of the ship as an alternative to actual delivery in exchange for the B/L and in substitution for it. It seems to me implicit in those circumstances that the parties intended that the Delivery Order should have the key attribute of a bill of lading, namely an undertaking by the carrier to deliver the goods to the person identified in it, which would, here, have to be Glencore or Steinweg, Glencore's agent. As the judge found, it is improbable that a shipper would agree to a term whereby he might surrender the bill without receipt of either the goods or the benefit of a substitute undertaking in his favour from the carrier. Further, a construction of a "Delivery Order" to be given by the carrier under an English law contract, which tallies with the definition of a ship's delivery order in UK statute law, is appropriate. 47. In *Krohn & Co v Thegra N.V.* [1975] 1 Lloyd's Rep 146, 153 Kerr J, as he then was, observed (i) that in a c.i.f. contract it was a fundamental feature that the buyer should as far as possible obtain control over the goods by means of the document against which he parts with his money; (ii) that this object was fully achieved in the classic and ordinary case in which the required documents included bills of lading by means whereof the buyer acquires ownership and contractual rights against the carrier; and (iii) that where a c.i.f contract entitled the seller to tender delivery orders instead of bills of lading, so as to enable him to split cargoes covered by a single bill of lading for the purposes of delivery, the contract should be so construed that these objects, although they could not be attained in full, were nevertheless attained so far as possible. An option to tender delivery orders instead of bills of lading in a c.i.f contract should, he held, prima facie be interpreted as intended to confer upon the buyer, inter alia, some right against the person in possession of the goods. This could be done by an instruction to deliver to the buyer given to the person in possession and the attornment of the latter to the buyer; or by a direct undertaking by the person in possession to deliver the goods to the buyer or his order. That approach was, he held, consistent with earlier authorities including *Colin & Shields v W.Weddel & Co* [1952] 2 AER 317; *Cremer v General Carriers SA* [1974] 1 WLR 341. These concerned what were described as ship's delivery orders. 48. The B/L is not, of course, a c.i.f. contract, only a document likely to be required under such a contract. But, as it seems to me, the considerations to which Kerr J referred, are equally applicable in the present case, governed, as it is, by English law, and that the contract should be construed so as to require an undertaking on the part of MSC to deliver to Glencore/Steinweg. I do not accept that MSC could provide any form of document, or number, that they liked provided it could be regarded as some form of delivery order. 49. Mr Howard submitted that the judge's interpretation of "Delivery Order" involved writing in the word "*ship's*" which was not there, and that it should be rejected on that account. I do not agree. The judge had to interpret a somewhat loose term which can have different meanings (including "ship's delivery order", which could, in some contexts, be no more than an instruction by the ship); and "*where a contract uses the term [delivery order] the question in which sense the term is used is one of construction in each case*" - *Benjamin Sale of Goods* (1974) paras 1389-1390 as applied by Kerr J, in *Krohn*. That exercise requires consideration of

what, in the context of this contract, the words are to be taken to mean. The absence of the word *"ship's*" is in no way determinative. 50. In short, I do not regard it as possible to treat the obligation to produce a Delivery Order as satisfied by a Release Note which does no more than instruct the Terminal to deliver against the entry of pin codes which it provides to Steinweg. *Ground 3 Release Note and pin codes as ship's delivery order* 51. Mr Howard submits that the Release Note with the pin codes contained in it was, on proper analysis, a ship's delivery order within section 1 (4) of *CoGSA 1992*. The Release Note, sent by MSC Belgium to Steinweg identifies the cargo and identifies to whom the cargo is to be delivered. In MSC's skeleton produced shortly before the hearing entitled "Delivery Orders" the Release Note was said to represent an undertaking by MSC (not MSC Home) to deliver to Steinweg (see paragraph 12), but MSC's case as expounded at the hearing and in its earlier skeletons is that the undertaking, if there was one, was to deliver to whoever first entered the correct code. 52. The Release Note, which notified Steinweg of the codes, has the following clauses: *"3 All terms and conditions contained in the MSC bill of lading concerned are applicable to subject release note. The addressee of the subject release note expressly confirms to have knowledge of these terms and conditions and to accept them unconditionally. … 5 Discharge of the cargo will constitute due delivery of the cargo. After discharge the cargo will remain on the quay at risk and at the expense of the cargo, without any responsibility of the shipping agent or the shipping company/carrier"* 53. MSC does not rely on clause 5 and says that the terms of the bill of lading would override it in any event. This is not surprising in the light of *Sze Hai Tong Bank,* where the Privy Council held that a similar clause did not protect the carrier who had delivered goods otherwise than to the holder of a bill of lading. MSC contends that there was an obligation to deliver under the B/L which continued under the Release Note but in such a manner that the mode of delivery was different, namely that the obligation was to deliver against the pin codes i.e. to Glencore/Steinweg if it was the first presenter of the codes or to the first presenter if it was not. Alternatively. MSC submits, the Release Note confirmed the delivery obligation under the B/L but in that modified form. 54. I have some difficulty in accepting that an obligation to deliver continued *under the B/L* after discharge. The B/L provided that it was to be exchanged for the goods or a Delivery Order. Accordingly, it is first necessary to look at what is said to be the Delivery Order to see whether it contains an undertaking to deliver, although, if it does not and by virtue of the B/L it should have done, there would be a breach of MSC's obligations under the B/L to produce a document which did contain such an undertaking. That was what the judge found to be the case. If, after discharge, there was a continuing obligation on the part of MSC to deliver to Glencore/Steinweg it may not, of course, matter whether the obligation arose under the B/L or the Release Note or both. 55. The critical question is as to the nature of the obligation (if any) which is required to be accepted in order for a document to constitute a Delivery Order. In my view, as I have said, a Delivery Order within the meaning of the B/L does require an undertaking on the part of MSC to deliver and the undertaking required is, as the judge found, one in favour of Glencore or Steinweg. As the judge pointed out – see [18] above - MSC did not suggest below that it gave an undertaking to deliver to either of those. 56. I entertain some doubt as to whether the Release Note is to be treated as providing any undertaking to deliver at all. On its face it notified Steinweg of the code which the hauliers would need to enter if delivery was to be given to them. It also contained a provision (albeit one not relied on) that discharge would constitute delivery of the cargo and a provision that all the terms of the B/L were applicable. The applicable term is that the carrier shall provide a

Delivery Order. Hence one looks at the Release Note to see what it provides which is either no undertaking at all or, on MSC's case, an undertaking to deliver to the first presenter of the correct codes. In either case it is not the Delivery Order called for by the B/L. namely to deliver to Glencore/Steinweg. A promise to deliver to whoever first enters the right code, whether or not that isGlencore/Steinweg, is not the same. 57. A possible alternative analysis is that, since the B/L requires a Delivery Order to contain an undertaking to deliver to Glencore /Steinweg, and since the terms and conditions of the B/L are, by the terms of the Release Note, applicable to it, the Release Note contains, impliedly or as a matter of construction, an undertaking to deliver to Glencore provided, at any rate, that the right pin code was entered. If so, MSC was in breach. So, either way, MSC is liable. I would prefer the judge's analysis since I find it difficult to *imply* an obligation to deliver to Glencore/Steinweg in a Release Note which has a clause that discharge will constitute due delivery (even though that clause might not prevail over an express obligation) and an obligation to provide a Delivery Order embodying an obligation to deliver to Glencore/Steinweg when the latter obligation is absent from its wording. 58. Mr Howard contended that, given that, ordinarily, the carrier was entitled and bound to deliver to the first presenter of the bill (who might turn out not to have been the person in fact entitled to the goods) it was illogical to hold that the Release Note with pin codes could not count as a Delivery Order so that the carrier was entitled and bound to deliver to the first presenter of the codes, particularly when the system had been in operation without objection since the beginning of 2011. The fact that the codes might be used by a thief was neither here nor there. Use of the correct numbers by a thief did not involve forgery and the fact that there might be more than one person who could claim delivery, provided he was first in time, was no different to the position that applied when there was more than one original bill. 59. Whilst I see the force of those submissions the position in relation to bills of ladingis well established but the position in relation to pin codes is not. No "custom of merchants" applies. Both Glencore and the range of addressees to whom the B/L could pass, might, or might not, have been prepared to accept that the goods should be deliverable to the first person to key in the pin code. They might have preferred to have the goods deliverable to the producer of the bill of lading or the beneficiary of any delivery order given in exchange, preferring to have the level of security provided by a paper document (which might be difficult to forge) rather than the risk of unauthorised electronic access to a code, e.g. by hacking. As it was Glencore was, on the judge's findings, unaware when it made the contract that any ERS was in use. I am not satisfied that what Glencore must be taken to have agreed by subscribing to the B/L was that delivery could and should be made to the first presenter of the code, whoever that was, and that, if it was, they would have no rights under the contract. 60. It may be that a system whereby delivery against a pin code is valid, even if presented by a thief, is sensible because of the benefits of using modern technology in place of paper. But, if that is to be done, it requires, in my view, either appropriate contractual provision or statutory imposition. 61. Glencore contends that the Release Note cannot be a Delivery Order because it was not a document: unlike the B/L for which it was to be a substitute. If, as I think, a Delivery Order required an undertaking by MSC to Glencore/Steinweg I doubt that it would matter that the undertaking was only given in an email which could be printed out since (a) the obligation would only be performed by actual delivery to Glencore/Steinweg; and (b) there would be no problem about proving that the undertaking was in fact given. Further Mr Passmore accepted, as I understood him, in answer to a question from Lewison LJ, that if Steinweg printed out

the Release Note sent to it, that would count as an original. If someone else made a copy delivery to them would not be good delivery anyway. Further, if "*any document*" in section 1 (4) of CoGSA 1992 does not extend to an email, which I doubt, I would still regard an email which contained the requisite obligation to deliver to Glencore/Steinweg as a Delivery Order. 62. If a Delivery Order could be an obligation to deliver to the first presenter of the code I do not think it would be necessary for the code to be set out in an original document since it would be the number which entitled the possessor to delivery. No question would arise as to whether the number was an original or a copy. A number is a number. 63. Reference was made by Glencore to the fact that the Secretary of State has not exercised his power under section 1 (5) of CoGSA 1992 which provides: *"The Secretary of State may by regulations make provision for the application of this Act to cases where a telecommunication system or any other information technology is used for effecting transactions corresponding to– (a) the issue of a document to which this Act applies; (b) the indorsement, delivery or other transfer of such a document; or (c) the doing of anything else in relation to such a document"* I do not regard the failure of the SOS to make any such order as casting any light on the true interpretation of the obligations under the B/L. *Ground 4 Estoppel* 64. MSC submits that in any event Glencore is estopped from contending that delivery of the cargo upon presentation of a pin code was a breach of contract and/or duty on the part of MSC. Glencore, it submits, gave the appearance that it was content for the ERS to be used for the 69 previous shipments and cannot now complain that it was used for the three containers under the B/L. The judge rejected that argument in the following terms [33]: *"I can see no basis on which it could be said that Glencore represented, or so conducted itself as to let it be understood, that it was or would be content for the goods to be delivered to anyone who presented the correct pin code: still less did it make a sufficiently clear representation along these lines, or sufficiently indicate that it would be so content, as to give rise to an estoppel. The estoppel arguments are also answered by my findings about the limited knowledge that Glencore had about the use of the ERS.* 65. MSC submits that what happened in relation to the previous 69 shipments (namely delivery against pin codes) established that the pin codes procedure was an acceptable substitute for the Delivery Order procedure, as that phrase was interpreted by the judge. Steinweg had authority to handle delivery procedures. The judge found [11] that its task was to arrange that goods consigned to Glencore were duly delivered at Antwerp and that it was entitled and authorised by Glencore to adopt any proper procedures to do so. It had authority to permit departures from the contract so far as delivery was concerned. The judge appeared to have accepted [34] that in view of the previous pattern of dealings the B/L allowed MSC to use the ERS and so not to deliver the goods immediately the B/L was surrendered. But he has in effect held that Glencore are estopped from complaining about the use of the Release Note procedure instead of the Delivery Order procedure but are not estopped from complaining that the procedure has been followed. 66. If, MSC submits, there had been a contractual variation to the effect that the supply of pin codes in a Release Note was a fulfilment of the obligation to give a Delivery Order in substitution for a bill of lading, or that the pin code system was to be employed by way of replacement for the Delivery Order system, it could not sensibly have been argued that MSC was in breach of contract in failing to deliver the cargo to Glencore even though it had followed the contractually agreed mechanism for delivery by delivering to the first person who entered in the code. A waiver or equitable estoppel should have the same effect. 67. I do not think that the judge was in error in concluding that there was no estoppel on

which MSC could rely. If there had been a variation of the contract to the effect that delivery to the first presenter of the code was a fulfilment of the delivery obligation under the contract, Glencore would have no claim. There was, however, no such agreement and, importantly, no question arose in the case of the first 69 shipments, where delivery was in fact made to Glencore or its agents, as to what the position would be if delivery was made to someone who had stolen the codes. The judge was right when he said that the breach relied on by Glencore was not simply that delivery was made against the codes but that delivery was not made to Glencore or its agents at all. No representation let alone a clear one was made by Glencore or on its behalf that delivery otherwise than to it would be acceptable provided that it was made to the first presenter of the codes. The fact that cargoes had been delivered to Glencore after presentation of pin codes on many occasions did not say anything about what the position would be if they were not. 68. In addition, I would not accept that Steinweg had any authority to make such a representation. It had no express authority. Nor is one to be implied. Authority to make arrangements to ensure delivery to Glencore pursuant to the B/L or Delivery Order did not impliedly extend to accepting that delivery pursuant to the B/L would validly be made by delivery to the first presenter of the codes whether that was Glencore or a thief, especially when Glencore was not even aware of the ERS system. 69. For all these reasons I do not accept that provision of the pin codes constituted the provision of a delivery order within the meaning of the contract. *Ground 5* 70. By an application notice dated 13 February 2017 MSC applied to adduce new evidence and to amend its notice of appeal so as to include a request for an order that, if the appeal was unsuccessful on grounds 1 to 4, the case should be remitted to the Court below on the issues of causation and/or contributory negligence. The issue of contributory negligence was not pursued before us. 71. The application was supported by a witness statement from Mr Jonny Duval of MSC's solicitors which set out information derived from MSC's Antwerp lawyer and its Area Manager for Europe, P & I Insurance, Legal and Claims Department. This revealed that shortly after the theft of the two containers the Antwerp police launched a criminal investigation under the supervision of an Investigating Magistrate. Access to the records of such an investigation cannot be obtained unless special authorization is granted by the Magistrate. An application to view the file was made on 27 May 2014 but was unsuccessful. A second application was made on 9 December 2016 and on 19 December 2016 the Magistrate gave permission to inspect the file between 29 and 30 December 2016. Inspection of some of the documents contained in the 30 or so boxes took place then. 72. On 5 January 2017 Mr Duval was copied in on an email message from Glencore's solicitors – Gateley Plc - referring to an article in Bloomberg which suggested computer hacking at the offices of MSC Belgium. The article reported that technicians had found a bunch of surveillance devices on an MSC network and that MSC had hired a private investigator who had called PWC's digital forensics team which learned that computer hackers were intercepting network traffic to steal pin codes. Gateley on behalf of Glencore sought disclosure from MSC of documents in their control in respect of the matters referred to in the article. Mr Duval emailed later saying that he was instructed by MSC that there was not and never had been a PWC report. 73. The material obtained from the criminal file included two statements which, Mr Duval suggested, revealed that the hacking had not been at MSC but at Steinweg. The first statement from Ms Sarah Ooms to the police dated 20 June 2012, two days before MSC Belgium sent the codes to Steinweg, stated that on 14 June 2012 her computer was hacked and that a second attempt was made on 19 June 2012 on both her computer and that of Charles Reynolds-Payne, Steinweg's commercial

manager. 74. What the hacking consisted of was that an email of 14 June 2012 appeared to come from CSAV, another shipping line which makes use of the MSC Home Terminal, and was sent to what was a general email address for Steinweg so that everyone in the office received it. Attached to the email was a PDF file to which a CSAV bill of lading was attached. In the bill, Ms Ooms was mentioned in the box specifying Steinweg as the Notify Party as the person for whose attention any notification should be given. On opening the document she received an indication that she should execute an Acrobat Reader update from a specified website. She did not do so. Nor did she believe that any of her colleagues did so either. She contacted a man at CSAV in the Netherlands who said that he had not sent the email. 75. On 19 June 2012, one day before the date of the arrival notice she and Mr Reynolds- Payne received an email from a named individual at Containerships Rotterdam NV with the same PDF and its accompanying bill of lading attached. It was signed by a named individual. When she contacted Containerships she was told that he was unknown to them. 76. On 20 June 2012 she received a phone call from the MSC terminal to the effect that they had also received the same email that she had received from Containership, who had contacted her because she was mentioned in the bill. Ms Ooms said that she did not know whether MSC installed the software update. 77. Ms Ooms also said that she had heard that EKB Container Logistic Group NV received a similar email sent in her name (which she did not in fact send). 78. The second statement was from Mr Graziano Asnot, the Steinweg systems manager, and was dated 15 July 2014. He stated that an NAS appliance was found in the office next to the office of Steinweg's financial director. This is apparently an appliance which permits unlawful remote electronic eavesdropping and snooping. A check was made of log data which revealed that an active appliance had tried to make outside contact. This had been blocked by the fire wall so that, Mr Asnot suspected, no data had got out through the company network. There was no information as to when the appliance was placed and MSC submits that there was, therefore, no reason to think that it had not been in place for a long period and indeed as far back as June 2012, the time of the theft. On that evidence there is, in fact, no way of telling. 79. At trial Ms Corin Gautschi of Glencore and Mr Reynolds-Payne of Steinweg gave evidence that there had been one previous theft of cobalt from Antwerp in November 2011 which involved the use of pin codes which had been misappropriated where Steinweg had been acting. Both she and Mr Reynolds-Payne gave evidence at the trial without mentioning the incidents of June 2012. Mr Reynolds-Payne said in his statement that "*Steinweg has only being[sic] involved in one other similar case, but I am now aware in general terms that the so-called cyber-crime had been an issue in the port of Antwerp*". He also said that he understood from the police that it was thought that in some way the thieves were able to hack one or other of the parties involved in order to gain the containers but that, so far as he was aware, the police inquiries into the incident had not yet reached a conclusion. He did not mention the incidents in June 2012 to MSC or MSC Belgium. 80. On 16 January 2017 Mr Duval for MSC sought disclosure from Glencore of all reports regarding the hacking of Steinweg's systems and all documents referred to in the documents released to MSC's Antwerp lawyer by the police, which were attached to his email. He said that he would be considering with Counsel the extent to which any further disclosure was required. In response Mr Andrew Messent of Glencore's solicitors pointed out, in an email of 17 January 2017, that the report in respect of the earlier incident involving CSAV and MSC Terminal had been disclosed and he sent a copy of the disclosed document the next day. On 7 February 2017 Gateley Plc said that they were informed by Steinweg's Belgian

lawyers that Steinweg did not prepare or commission any report in relation to the breaches of computer security in this case. 81. In a witness statement of 17 February 2017 Mr Messent reported that Glencore, in the persons of Ms Gautschi and Ms Catherine Zanetti, who was responsible for insurance matters, had confirmed that Glencore had no knowledge of any hacking of Steinweg's computer system potentially connected to the loss of the containers and in particular of any spying device found in Steinweg's office or the hacking of the computers of Ms Ooms and Mr Reynolds-Payne. There had been no correspondence between Glencore and Steinweg about any such hacking of which they were aware nor had Glencore or any agent of Glencore made a report into the hacking of Steinweg's computer system. A report in respect of the theft of the two containers had been made by Steinweg's liability insurers but this had not been disclosed by Steinweg. He exhibited to his statement a series of documents obtained from Steinweg's lawyers. These showed that in relation to the statement given by Ms Ooms on 20 June 2012 it was reported to the police 2 days later that according to "*the first findings*" nobody was infected at Steinweg. Her computer was handed over to the police who took a copy of the hard disc and did not, to the best of Steinweg's lawyers' knowledge, revert with any communication that the disc contained any indication of viruses or hacking. Further, inquiries of the police of the MSC Terminal produced confirmation from the IT department that employees were not allowed to perform updates save onto laptops. *MSC's submissions* 82. MSC contends that Glencore had failed to make disclosure on a matter that was central to the trial and that that failure was compounded by the provision of evidence which was deliberately misleading. Mr Reynolds-Payne's statement made a glancing reference to Steinweg having been involved in another similar case without making any reference to all to the contemporaneous hacking or likely hacking of its own computers. Ms Ooms did not give evidence. MSC could not be expected to have realised that this material was available; it was misled into the belief that the theft of the containers came out of the blue when it was, in truth something that Glencore should have anticipated. It is probable that with more time to carry out a proper investigation MSC would uncover more internal documentation. Steinweg, Glencore's agents, should have alerted MSC Belgium to what had occurred as a matter of urgency. Had they done so the overwhelming likelihood is that simple additional security measures would have been taken to prevent the ill effects of the hacking as was in fact done after the incident. The non-disclosure has thus deprived MSC of a potential defence that the loss was solely caused by Steinweg in failing to warn MSC of the hacking. Causation was not the subject of any express pleading because there was no material on the basis of which it could have been. But causation is always an issue. *Glencore's submissions* 83. Glencore relies on the fact that, as it contends, MSC's defence never raised any issue about how the pin codes became known by the thieves. Paragraph 11 simply said that no admissions were made as to how the pin codes became known to the people who took the goods, the precautions taken by Steinweg to keep the pin codes safe and secure, or the identity of the people who took the goods. MSC purported to reserve a right to plead further "*in this regard*" after disclosure. It was not pleaded that any loss was not caused by MSC or that any question of contributory negligence arose. Disclosure was thus limited to what was raised on the pleadings. At trial, no issue remained as to how the codes came to be known. No such issue appears in the List of Issues. In consequence there was no evidence directed towards how the codes came to be known; and the judge made no findings on that topic. 84. In MSC's further skeleton argument in relation to grounds 1 and 4 of 14 March 2016 it was said that "*Control of the relevant codes was lost by or*

within Glencore". It was that which led to Glencore's application for disclosure referred to in [72] above. After MSC lost its application to the Investigating Magistrate in May 2014 no further application was made until December 2016 although the trial took place in July 2015. Contrary to what Mr Duval suggested in his witness statement the new evidence does not show that there had been no hacking at MSC Belgium's site. In the light of Ms Ooms' complaint to the police it was not at all clear that the Steinweg system was accessed or hacked at any time, let alone prior to the pin codes being accessed in the present case. The evidence at trial was that the codes were generated only when the Release Note was sent by MSC which happened on 22 June: so they could not have been accessed on either 14 or 19 June. There was nothing misleading in the statements of Mr Reynolds-Payne or Mr Gautschi. Nor has any relevant evidence been suppressed. MSC has simply assumed from the fact that Steinweg received one rogue email on 14 June 2012 and two on 19 June 2012 and that MSC Home received a similar one on 20 June 2012 that Steinweg's computer system was hacked in a way which allowed the PIN codes to be taken, and then complains that Mr Reynolds- Payne in failing to make that assumption gave deliberately misleading evidence. *Conclusion* 85. I would refuse permission to amend the notice of appeal and to remit the case for further investigation on the question of causation for a number of reasons. 86. First, I regard it as too late to raise this issue now. It was tolerably clear from an early stage that one of the ways in which the thieves might have gained access to the codes was by hacking someone's computer. I accept that, in the absence of any evidence that there was or might be a leak known to Steinweg, MSC could not plead that that was so. But, if MSC was satisfied from their inquiries that the leak could not have come from any of MSC, MSC Belgium, or MSC Home it would have been open to it to invite the court to infer that it came from Steinweg. However, any potential issue as to whether the leak came from Steinweg, and whether Steinweg knew that there was a risk of that, faded from view. It was never pleaded in terms that control of the codes was lost by or within Glencore or Steinweg (or that Glencore was put to proof that that was not so), although MSC felt able to assert in March 2016, before the Investigating Magistrate ordered disclosure of the police file in December, that control was lost within Glencore. The agreed list of issues did not raise any issue as to how the codes came to be made known or any issue as to causation. 87. Second, whilst I recognise that disclosure does not have to await a specific request, no attempt appears to have been made, in the disclosure process before the trial, to ask whether there was any documentation which indicated that there might be a leak from either Glencore or Steinweg. Further, no renewed application was made to the Magistrate before the trial. Whilst it is impossible to know what the result of such an application would have been there is some reason to suppose it would have succeeded. Inspection was initially refused because "*in the current state of affairs all suspects could not yet be apprehended and interrogated*" such that "*the necessities of the investigation*" meant that the application could not be granted. That state of affairs cannot have applied in December 2016 and may well not have done so in the first half of 2015, by which time over 2 ½ years had elapsed since the loss. At trial Mr Reynolds-Payne was not asked any questions about whether he knew whether anything that had happened at Steinweg might have caused the leak. Nor was the issue taken up or disclosure sought after MSC in March 2016 said that the leak of the pin codes came from Glencore. 88. Third, I am not convinced that the evidence sought to be adduced would have an important influence on the result of the case. It seems to me far from clear that the thieves got access to the codes from access to a Steinweg computer (as opposed to an MSC Belgium or MSC Home computer or

some other means) or that it was apparent to Steinweg that the risk that access to the codes might be so obtained was sufficiently great that a failure to alert MSC Belgium/MSC Home could be said to break the chain of causation. As to the latter Glencore submits that, in circumstances where a Delivery Order would have obliged MSC to deliver to Glencore/Steinweg, delivery against a pin code without any further verification was at MSC's risk; and, when that very risk materialised, it cannot be heard to say that there was any such break. I am disposed to accept that the chain of causation could be regarded as broken by sufficiently egregious action or inaction on Glencore/Steinweg's part but it seems to me doubtful that what is described in Ms Ooms' evidence in relation to June 2012 falls into that category. I also note that MSC Home received on or before 20 June 2012 the same email as Steinweg received on 19 June 2012 and, since that was discussed with Ms Ooms in a telephone call between MSC Home and her, MSC Home must, I infer, have been aware that Steinweg had received the same hacking email. 89. Lastly, I am not persuaded that Mr Reynolds-Payne or Mr Gautschi have been underhand. 90. For these reasons I would not grant permission to adduce the evidence of Jonny Duval or to amend and would dismiss the appeal. Lord Justice Henderson 91. I agree. Lord Justice Lewison 92. I also agree.

Annexies of list of concise and chronological listing of cyberattack cases

Impact / Area Organisation / Location / Affected System / Method /Impact /Reference / Accused State

- 2011 / Shore / IRISL / Cargo tracking system/ - / Operational interruption / (Torbati and Saul 2012) (Cyber Keel 2014) / – /
- 2011 / Shore / Ports of Belgium and the Netherlands / Container tracking system / Spear phishing / Smuggling / (Bateman 2013) (European Cybercrime Centre 2013)/- /
- 2012 / Shore / Australian / Customs and Border Protection Service Agency / Container tracking system / - / Smuggling / (Kochetkova 2015) / – /
- 2012 / Shore / Danish / Maritime Authority Network / Spear phishing / Data theft / (Cyber Keel 2014) (The Local 2014) / China
- 2013 / Vessel / Gulf of Mexico / Network / Malware / Operational interruption / (Shauk 2013) / – /
- 2016 / Vessel / Coast off South Korea / GPS / GPS jamming / Blocking GPS signal / (Saul 2017) (Graham 2017) / North Korea
- 2016 / Shore / A Broker's e-mail account / E-mail / - / $500,000 financial loss / (Belmont 2016) / – /
- 2017 / Shore / Clarksons / Network / - / Data theft / (Leyden 2018) (Esage 2018) / – /
- 2017 / Shore / Maersk / Network / Ransomware (Petya) / $250-300 million financial loss, data contamination / (Maersk 2017) (Tung 2018) / – /
- 2017 / Vessel / En route from Cyprus to Djibouti / Navigation system / - / Full control by attackers / (Blake 2017) / – /
- 2017 / Vessel / Coast off Russia / GPS / GPS spoofing / Wrong GPS location / (Goward 2017) (Humphreys 2017) / Russia /
- 2017 / Shore / BW Group / Network / - / Operational interruption / (Mohindru 2017) (Ngai 2017) / – /
- 2018 / Shore / Svitzer Australia / E-mail / E-Mail forwarding / Data theft / (WMN 2018b) / – /
- 2018 / Shore / COSCO Shipping / E-mail, phone, website, network / Ransomware Operational interruption / (WMN 2018a) / – /
- 2018 / Shore / Austal / Network / - / Data theft / (Maritime Executive 2017) / – /
- 2018 / Shore / Port of Barcelona / - / - / - / (IMarEST 2018) / – /

- 2018 / Shore / Port of San Diego / Network / Ransomware (SamSam) / Data contamination / (Senzee 2019) / Iran
- 2018 / Vessel / Coast off Cyprus / GPS / GPS Jamming / - / (2018 cited Denizcilik Bilgileri 2018) / Turkey
- 2019 / Shore / James Fisher and Sons / Network / - / Data contamination / (Safety4Sea 2019) / – /
- 2019 / Shore / Princess & Holland America / E-mail / - / Data theft / (Coble 2020) / – /
- 2019 / Shore / Crew and Concierge / Network / - / Data theft / (Safety4Sea 2020) / – /
- 2019 / Shore / London Offshore Consultants / Network / Ransomware / Operational interruption / (Chambers 2020) / - /

Annexies of examples of recent cyber incidents in the maritime transport sector.

Year Incident Consequences

2016 GPS jamming attack in South Korea 280 vessels were affected

2017 Cyberattack against the navigation system Hijack of the vessel for 10 h

2017 Cyberattack against the navigation system U.S. Navy ship collided with a boat

2018 GPS spoofing attack against ships in the Black Sea Deviation of 20 ships to an airport

2018 Remotely compromising onboard computers Stealing sensitive data

2018 GPS spoofing attack Manipulation of the ship position

2018 NotPetya malware attack Affected shipping infrastructures

2018 ECDIS was infected by a virus Delay in the ship sailing

2019 Malware attack targeted a U.S. vessel Critical credential mining

2020 Ransomware Hermes 2.1. attack on 2 ships Infection of the whole network

2020 Ransomware attack "Mespinoza/Pysa" Maritime infrastructures infected

2021 Ransomware attack on shipping companies All their files were encrypted

2022 Installation of malicious code Gain access to the port network

Modern and autonomous ships are equipped with a variety of complex automated systems that have made the sea a much safer place than before. However, some of these systems are often insecure and vulnerable to attack because they are considered less critical to security and performance. As shown in figure below, these systems include navigation systems, radio detection and ranging (radar), Automatic Identification Systems (AISs), communications systems, and control systems for the wide range of electromechanical systems on board ships, such as the main engine, generators, converter drives, etc.. [47]

[47] https://www.mdpi.com/2673-8732/2/1/9 1 Cyber Security Research Group, University of Portsmouth, ortsmouth PO1 2UP, UK; Frank.Akpan1@myport.ac.uk 2 Department of Electronic, Faculty of Sciences of Technology, University of Freres Mentouri, Constantine 25000, Algeria; bendiab.kelthoum@umc.edu.dz 3 Faculty of Pure & Applied Sciences, Open University of Cyprus, Nicosia 2220, Cyprus 4 Department of International Shipping, Plymouth Business School, University of Plymouth, Logistics and Operations, Cookworthy Building, Drake Circus, Room 321, Plymouth PL4 8AA, UK; stavros.karamperidis@plymouth.ac.uk 5 TMS Cardiff Gas, Marousi, 151 24 Athens, Greece; mmichaloliakos@tms-management.org * Correspondence: stavros.shiaeles@port.ac.uk, "**Cybersecurity Challenges in the Maritime Sector**", Frank Akpan, Gueltoum Bendiab, Stavros Shiaeles, Stavros Karamperidis and Michalis Michaloliakos.

Annexies of Courtesy of Brett Sayles. In 2017, the most widespread and devastating cyberattack was launched against the global shipping giant Maersk. It began on a quiet afternoon in June, when staff began seeing messages informing them that the file system was being repaired, while others received messages that critical files had been encrypted. The encryption key required $300 in bit coins. The Maersk headquarters panicked. The entry system and phone network had been rendered useless by malware that was spreading rapidly within and outside the company network. By the end of the day, the network was so deeply disrupted that the company simply shut down. Maersk is a global shipping company that transports all kinds of goods in 76 ports and more than 800 vessels worldwide, and is responsible for about one-fifth of global trade. This entire enterprise was brought to its knees by mysterious malware that spread to all Maersk locations around the world: Sandworm, Not Petya, and Ukraine Since 2012, Ukraine and Russia have clashed in an undeclared war that serves as a testing ground for Russian cyberwar fare tactics. A group of Russian hackers known as the Sand worm thoroughly compromised the Ukrainian government and dozens of Ukrainian companies. The attackers were firmly entrenched in the networks and systems of Ukraine's most important and critical infrastructure. Among the atrocities committed at the behest of the Russian government, the Sandworm installed and regularly activated malware on the power grid, causing the most damage and demoralizing the population. A classic example of this was the shutdown of the power grid in the middle of winter. A series of malicious attacks on Ukrainian businesses, especially banks, resulted in the complete destruction of large amounts of data. One of the ways Russia was able to conduct such a wide spread and thorough destruction campaign was the breach of the Lynkos Group, a small software company that sells an accounting software package called M.E.Doc. This software is used by nearly every one doing business in Ukraine, giving Sandworm a vast attack surface area; Sandworm's ads hijacked the company's update server in early 2017, which all owed thousands of computers running M.E.Doc computers through a back door. In June of the same year, Sandworm released a particularly malicious cyberweapon called Not Petya, which spread rapidly and automatically. The code was indiscriminate in its attack targets and designed to inflict maximum damage as quickly and as broadly as possible. The ransomware spread so quickly and effectively that by the time the message appeared on the screen, the damage was already extensive. Not Petya was created by the National Security Agency (NSA) and leaked

in early 2017with a penetration tool called Eternal Blue, Mimi Katz, a software application with the ability to pull users' passwords out of RAM and reuse them to compromise target machines, which consisted of two main elements. Although Microsoft had issued a patch against Eternal Blue, Mimi Katz was able to obtain the password, which in turn all owed it to infect unpatched machines worldwide. The origin of the name, which Kaspersky called Not Petya to distinguish hit from the Petya strain, is also indicative of its designers' intent: Petya was a ransomware package used to extort money from infected users in exchange for decryption keys. Not Petya was a "legitimate" ransomware, and its intent was purely destructive. The ransom payment was in vain. There was no decryption key for the destroyed data. The Sandworm targeted only Ukraine with Not Petya, but its impact was felt worldwide. First Maersk, then the world. Within hours of Not Petya's release, the malware traveled around the world, infecting countless computers. Victims included FedEx's European subsidiary TNT Express, several French companies, a hospital in Pennsylvania, the pharmaceutical company Merck, and of course Maersk. The radiation monitoring system at the Chernobyl nuclear powerplant went off line. The infection spread to Russia, contaminating the state oil company Rosneft. The attack caused about $10 billion in damage. It was the equivalent of using a nuclear bomb to score a small tactical victory, "said Tom Bossert, then White House Homeland Security Advisor. It was a completely reckless act that the national community should not condone. This was cyberwar fare of the worst kind, in which nations exploited the border lessness of the Internet with callous disregard for human life. Political attack son rival states became attacks on other countries. Although this attack was aimed at Ukraine, it also hit Maersk, and in turn affected then tire world. The back door exploited by the Sand worm had been present in Lynkos' servers for several weeks before the attack was launched. Lynkos denied that they were the perpetrators of the attack and claimed that they were victims; in July 2017, Ukraine's cybercrime unit seized a server from Intellect Services, the company that produces the M.E.Doc software. Analysis of the server showed that it had not been updated for at least four years and no security patches existed. There was evidence of Russian presence on the server and several employee accounts had been compromised. Intellect Services later closed the back door to its software, and state prosecutors promised to hold the company responsible for the enormous damage caused by its lax security procedures. Maersk was left in the lurch. It turned out that only one infection was responsible

forMaersk'sinformationbreach:M.E.Doc had been installed on the company's computers in Odessa, a Ukrainian port city on the Black Sea. Not Petya was able to do just that, infecting the entire system. Port facilities were shut down around the world and tens of thousands of trucks were unable to move cargo. Maersk's entire booking system went down, as did the complex loading system used to systematically load container ships to prevent them from capsizing. Maersk was dead in the water; an incident response team was formed and an emergency recovery center was set up in the UK to mitigate and recover from the Not Petya attack. This was a global effort, requiring hundreds ofstafftowork24/7 to rebuild the network. All computer equipment was confiscated and new computers were obtained and distributed to recovery personnel. The staff began rebuilding the servers from scratch. However, this effort ran in to an impasse when it was discovered that there was no clean backup of the company's domain controller. A domain controller is a server that responds to user authentication and confirmation requests. Domain controllers check usernames and passwords or other access credentials to allow or deny user access to network resources. Without a functioning domain controller, the network becomes a collection of disparate servers and data that can only be accessed locally. Maersk has approximately 150 domain controllers throughout the global system, which can normally be synchronized with each other and thereby could serve as a backup for compromised or damaged servers. This was an effective and decentralized backup strategy that allowed for rapid recovery from localized events. However, no one imagined a scenario in which a major attack would wipe out all of the company's domain controllers. If the domain controllers could not be recovered, the chances of recovering anything were slim. Maersk's staff finally found one complete backup in their Ghanaian office. A sluck would have it, the server had been taken off line and disconnected from the network due to a power outage prior to the Not Petya attack. The server contained one clean copy of the company's domain controller data, and its discovery was a great relief to the recovery team. Getting the data to the recovery center was a daunting as kin itself. Ghana's public network infrastructure was still in its infancy and available bandwidth was very limited. Backups were hundreds of gigabytes of data, which would take days to send to the recovery center. The next option was to put the staff on a plane from Ghana to London, but none of the staff had UK visas. The next plan was to fly the staff member to Nigeria to meet the Maersk employee and give him the hard drive personally. The Maersk employee then boarded

the plane again and took the 6.5 hour flight back to Heathrow. The recovery team setup Maersk's core services and concentrate don port services. Key to this was the ability to read the ship's inventory (each ship has 18,000 containers) and determine what was there and where it was going. The booking system came back online a short time later, but it took at least two weeks before the port facilities were working properly again. The recovery team then began distributing clean laptops and computers to staff. Hard drives were erased and new, clean Windows was installed. The Future of Cyberwar When all was said and done, Maersk estimated that Not Petya had cost the company between $250and $300 million, a figure many consider low. Trucking companies lost tens of millions of dollars, TNT Express lost about $400 million, and Merck lost awhopping$870 million. The disruption to the global supply chain, of which Maersk is a major component, was widespread, with losses in the billions of dollars. The Maersk incident was a costly and serious wake-up call. Not Petya offered a glimpse of the potential for cyber warfare. Without preparedness at all levels, no one can escape the kind of damage this malware has caused.