ThessISMUN 2017

Thessaloniki International Student Model United Nations

International Maritime Organization

Topic Area B: Hacking Ships: Maritime Shipping Industry at Risk/ Combatting Cyber Attacks at Sea

University of Macedonia
Thessaloniki, Greece

www.uom.gr/mun - www.thessismun.org

Table of Contents

1. Welcoming Letter

Dear delegates,

it is our distinct pleasure to welcome each and every one of you to the 2017 Session of Thessaloniki's International Student Model United Nations and the International Maritime Organization (IMO). This year in the IMO we will be discussing the following issues:

Topic Area A: Prevention of maritime pollution: (Facilitating ships recycling via revising the Hong Kong Convention).
Topic Area B: Hacking Ships: Maritime Shipping Industry at Risk/ Combatting Cyber Attacks at Sea.

The IMO is currently facing numerous challenging issues that have not been so far successfully addressed by the international community. Although multiple problems are being acknowledged, little to almost nothing has been done to fully address them. It's therefore your chance as delegates of the IMO to recognize the predicaments caused by the issues we will be discussing and propose appropriate and innovative solutions in the short and long term.

This guide will serve as the first step to your research and it will attempt to introduce you to the key points of the topic. It should therefore not be the sole source of your preparation for the conference. As delegates you are expected to study well in advance for the topics in questions as well as becoming familiar with the Rules of Procedure of the conference in order to be confident with the diplomatic aspect of the committee. Should you have any questions regarding the topics or the rules please do not hesitate to contact any of us, we are at your disposal.

Looking forward to meeting you all in April!!!

Yours sincerely,

The Board of the International Maritime Organization

Evangelos Halatsis

President

Lambrini Pliatsika

Vice President

Ananias Kapourkatsidis

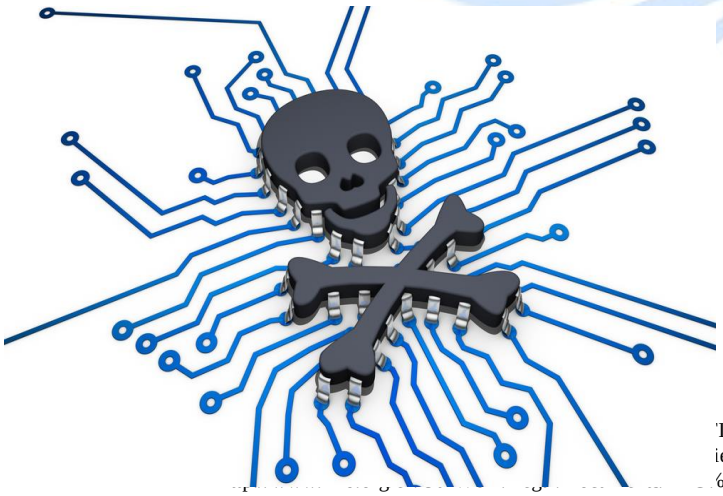
Secretary-General

2. The mandate of the IMO

The International Maritime Organization is the United Nations body responsible for "maritime safety, efficiency of navigation and the prevention and control of marine pollution from vessels and by dumping"[1] . The main goal of the IMO is to create an international regulatory framework within which the shipping industry will operate safely, effectively and in an environmentally friendly way.

The IMO is considered by the United Nations Convention on the Law of the Sea (UNCLOS) as the sole "competent international organization" with the authority to adopt international rules concerning the shipping industry. The scope of the IMO is to secure the safety of maritime activities and the protection of the marine environment. Moreover, the efficiency of navigation and the availability of shipping services to all states are considered global priorities. In the attempt to regulate the international shipping industry the IMO seeks to cooperate with other specialized agencies, governmental and non- governmental organizations.

3. General Introduction to the Topic



It is true that shipping, as with every other sector, is subject to evolving and adapting to the constantly changing demands of the international community. With the great advancement of Information Technology (IT) over the past decades, it is

'IONS CONVENTION ON THE LAW OF THE SEA FOR THE
ieved from
%20MISC%208.pdf

only natural that it would find certain applications in the shipping industry as well. Like always, new technologies are initially introduced to facilitate procedures and minimize the amount of work that needs to be done to achieve specific goals. However, their use in the shipping industry confirms the idea that they can also be a curse apart from a blessing. Although the introduction of new IT services such as GPS navigation control, faster cargo tracking and unloading, identification systems etc. are only a few of the contributions that have rendered modern age shipping the way we know it know. Nowadays, almost all modern vessels are completely computerized meaning that shore-based personnel remotely control them, perhaps from thousands of miles away from them vessel[2]. GPS systems are even used to move cranes and to ensure the quick unloading of goods. Overall it is evident that scheme is shifting towards one of smaller crews, larger ships and more reliance on automation, something that one the hand makes the whole process of shipping more efficient but leaves it vulnerable to cyber attacks[3].

Although one can argue that cyber attacks can occur in any sector, one must also not ignore the significance of the maritime sector in global trade and thus economy, as well as its role in military operations. The shipping industry covers many important aspects of modern everyday life, economy, employment and security thus its applications affect billions of people. The International Chamber of Commerce (ICC) estimates that in 2010, 52% of goods trafficking in Europe relied on maritime transport while a decade ago this was only at 45%[4]. Movement of people, transportation of natural goods (such as energy sources) and the role the sea plays in accessing lands easily for military purposes are all reasons why the maritime sector is a key player of the financial, social and military chessboard and should therefore not be underestimated when it comes to cyber security. With the figures showing that the

[2] Paganini, P. (2016). *Hacking Ships: Maritime Shipping Industry at Risk*. [online] Security Affairs. Available at: http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html [Accessed 8 Dec. 2016].

[3] Reuters. (2016). *All at sea: global shipping fleet exposed to hacking threat*. [online] Available at: http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424 [Accessed 13 Dec. 2016].

[4] TTD. (2016). *The Vital Role of Maritime Transportation In Our Economy - TTD*. [online] Available at: http://ttd.org/policy/policy-statements/the-vital-role-of-maritime-transportation-in-our-economy/ [Accessed 13 Dec. 2016].

world becomes more and more dependent on shipping, it is the duty of the IMO to ensure that such matters will not endanger the shipping industry and to establish global guidelines and recommendations for resolving the issues arising from cyber security threats.

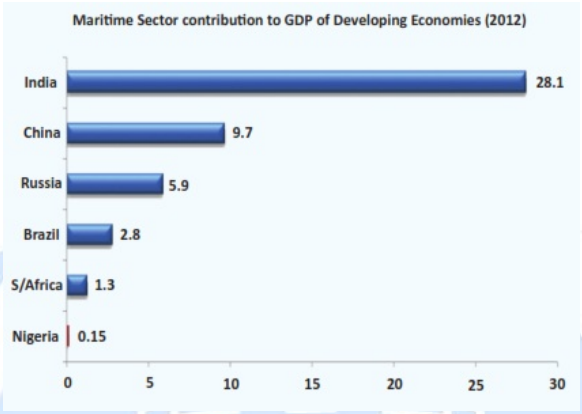


Figure 1: The role of the maritime sector in some developing economies[5]

4. Definitions of Key Terms and Concepts

Information Technologies: the technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data[6].

Cyber Attack: A deliberate exploitation of computer systems, technology-dependent enterprises and networks. Cyber attacks use malicious code to alter computer code, logic or data, resulting in disruptive consequences that can compromise data and lead to cybercrimes, such as information and identity theft[7].

[5] Oxford Economics, (2015). The economic impact of the UK Maritime Services Sector. [online] Oxford, UK: Maritime UK. Available at: https://www.maritimeuk.org/documents/1/Combined_The_economic_impact_of_the_UK_Maritime_Services_Sector_ezucVrL.pdf [Accessed 13 Dec. 2016].

[6] Merriam-webster.com. (2017). *Definition of INFORMATION TECHNOLOGY*. [online] Available at: https://www.merriam-webster.com/dictionary/information%20technology [Accessed 6 Jan. 2017].

[7] Techopedia.com. (2017). *What is a Cyberattack? - Definition from Techopedia*. [online] Available at: https://www.techopedia.com/definition/24748/cyberattack [Accessed 6 Jan. 2017].

Malware: "Malware" is short for "malicious software" - computer programs designed to infiltrate and damage computers without the users consent. "Malware" is the general term covering all the different types of threats to your computer safety[8].

Phishing: Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords. It can involve sending malicious attachments or website links in an effort to infect computers or mobile devices[9].

5. Historical and Factual Background

It is true that when it comes to shipping, looking back in time and viewing past cases where maritime cyber security was breached, can help identify key parts of the issue that need to be amended. Probably the most memorable highjack in the history of the IMO was the one the Italian cruise ship Achille Lauro on 07/10/1985 that served as an initial trigger for the organization to draft one of the very first resolutions towards preventing the incidence of such events[10]. There are countless examples of shipping hijacks ever since, and although some of them were quite devastating for the shipping and cruising industries, none of those were of a particular cyber-attack nature. For example, the attack on an oil tanker called SS Limburg, in the Gulf of Aden, off the coast of Yemen on 6 October 2002 depicts a case where almost no cyber measures were used to plan and deploy the attack[11].

[8] Bullguard.com. (2017). *A definition of malware*. [online] Available at: http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx [Accessed 6 Jan. 2017].

[9] Action Fraud. (2017). *Phishing*. [online] Available at: http://www.actionfraud.police.uk/fraud-az-phishing [Accessed 6 Jan. 2017].

[10] HISTORY.com. (2016). *Palestinian terrorists hijack an Italian cruise ship - Oct 07, 1985 - HISTORY.com*. [online] Available at: http://www.history.com/this-day-in-history/palestinian-terrorists-hijack-an-italian-cruise-ship [Accessed 13 Dec. 2016].

[11] IMO, (2012). *IMO and Maritime Security Historic background*. [online] London, UK: IMO. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/IMO%20and%20Maritime%20Security%20-%20Historic%20Background.pdf [Accessed 13 Dec. 2016].

With so many incidents of pure piracy attacks on maritime security taking part in very particular parts of the world, the IMO and related bodies inevitably had to shift all the focus of the discussions towards battling piracy itself and have not managed to fully recognise the severity of the current situation. On top of that, reports such as the one produced by Allianz, argue that ship losses have declined by 3% since 2014 with the large-scale ones reduced by an almost-utopic 45%[12]. Such results sound promising and can even be misleading when assessing the importance of the topic of maritime security. This is because, especially when it comes to cyber attacks, the relevant authorities either fail to recognise the incidence of an attack or do not disclose all the necessary information to the public. As a result, reports talking about a decrease in maritime security threats should not be viewed as reliable and not render the current measures taken as adequate[13].

Over the last few years, however, cyber attacks seem to be occurring at an increasing rate. The most shocking example of this is the **Antwerp Port** (Belgium) **case**, where a group of Belgian cyber terrorists hacked the IT security systems of the port in order to establish one the biggest drug-trafficking operations in history[14]. The Belgian authorities failed to recognise this at the time of its breakout, resulting in the hackers working freely for a two-year period, until large amounts of cargo used as disguise started disappearing unexpectedly. It all started with the terrorists passing emails to port's IT staff, that acted as malware-vectors providing access to undisclosed information and allowing the hackers to delete the records of any additional container shipped. What is even more alarming is that after the hackers were caught and the Belgian authorities investigated the case, they discovered that the

[12] Agcs.allianz.com. (2016). *Safety & Shipping Review 2016*. [online] Available at: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/safety-and-shipping-review-2016/ [Accessed 13 Dec. 2016].

[13] Bueger, C. (2015). *Learning from Piracy: Future Challenges of Maritime Security Governance*. 1st ed. [ebook] Cardiff: Cardiff University. Available at: https://www.cardiff.ac.uk/__data/assets/pdf_file/0013/42412/dr-christian-bueger.pdf [Accessed 13 Dec. 2016].

[14] TradeWinds. (2016). *How hackers attacked the Port of Antwerp*. [online] Available at: http://www.tradewindsnews.com/weekly/342065/How-hackers-attacked-the-Port-of-Antwerp [Accessed 13 Dec. 2016].

equipment used to hack not only the port's IT security systems but also the vessel's security protocols was relatively inexpensive and simple to obtain. Dr Humphreys of the University of Texas, an expert on GPS systems, argues that with as little as 3,000 USD a group of hackers can easily breach the average security system that currently exists in most parts of the world[15].

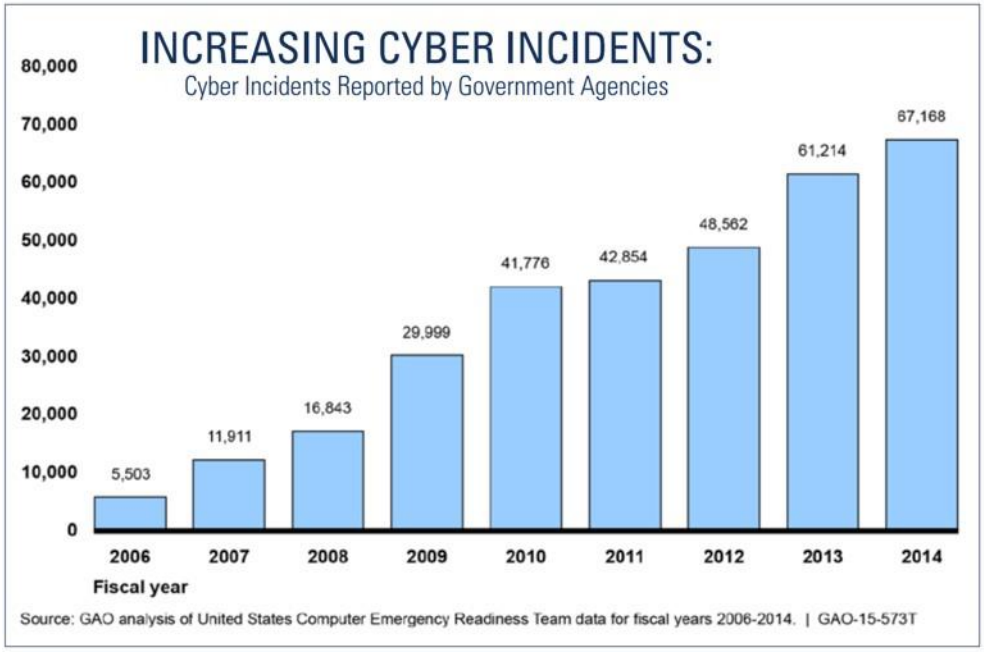


Figure 2: The trend of cyber attacks from 2006 to 2014[16]

Another example that was identified quite recently is the one that occurred near the sea territories of Somalia in June 2016, when terrorists and hackers collaborated in an unprecedented fashion. The hackers were accessing confidential information about the nature of the cargo in vessels passing through the area and

[15] Blogs.cornell.edu. (2016). *A Red Team, a Blue Team, and the White Rose*. [online] Available at: http://blogs.cornell.edu/yachtspoof/ [Accessed 13 Dec. 2016].

[16] FedScoop. (2016). *Federal cybersecurity incidents increased more than 1,000 percent since 2006*. [online] Available at: http://fedscoop.com/federal-cyber-incidents-increased-1-121-percent-since-2006 [Accessed 13 Dec. 2016].

helped terrorists identify those with valuable goods "worth" of attacking[17]. The terrorists also had access to key information with regards to the exact co-ordinates of the vessel at all times, thus being able to strategically plan their operations well in advance.

Looking back into such cases like the one in Antwerp is very helpful in not only reading into the ways in which hackers attempt to breach security facilities but to also recognise the flaws of the current measures and policies around maritime security. As hackers are notorious for their innovation in most sectors, it is probably wise to not rely solely in establishing pattern recognition of their actions but to rather prepare for the worst and create sturdy security systems, able to withstand any imminent attack.

6. Analysis of the Topic

The issue of maritime security and its being at risk from cyber attacks has multiple aspects that need to be understood and dealt with individually and thereafter collectively. Reading into the pitfalls that the extensive use of IT systems in shipping poses along with its valuable applications, is vital in ensuring that the problem can be addressed efficiently and with more success. In this guide, the major aspects are going to be discussed in detail. However, delegates are strongly recommended to view the "Further Reading Section", where additional information on more aspects can be found in detailed analyses.

5.1.The lack of information exchange

As it was mentioned earlier, one of the most alarming issues around the topic of cyber security is that governmental authorities of individual member states are

[17] Saunders, B. (2015). *Maritime Cyber Security Threats and Opportunities*. CIRM Annual Meeting. [online] Nicosia, Cyprus: NCC Group. Available at: https://www.nccgroup.trust/globalassets/resources/uk/presentations/2015/maritime-cyber-security-threats-and-opportunities.pdf [Accessed 13 Dec. 2016].

either not identifying cyber attacks on time or not revealing their incidence. For the past decade, the controversy around information exchange had some legitimate grounds, as stakeholders viewed that confidentiality and protection of national competence and interests were far more important. However, after the recent spikes in cyber security breach in the maritime sector, many bodies and organizations such as the European Network and Information Security Agency (ENISA), have warned the international community that this can no longer be the case when it comes to issues of cyber security. ENISA published a study in November 2011 whose analysis clearly showed that not only individual states, but also several of the intergovernmental organizations involved, shared little if no information at all about the nature, circumstances and reasons of cyber attacks during the period of May to September 2011[18]. According to the report by ENISA, this can be responsible for two main issues that deteriorate the impacts of cyber security attacks in the maritime sector.

First and foremost, as it was seen in the past with the issue of simple piracy, there are specific regions where the incidence of shipping attacks is significantly increased when compared to the rest of the globe. The ICC identified 10 major areas where piracy was found to be out of control over the past decade: The Malacca Straits, the South China Sea, the Gulf of Aden, the Gulf of Guinea, Benin, Nigeria, Somalia, Indonesia, the Arabian Sea and to a greater extent the Indian Ocean[19]. Such a conclusion could be drawn because proper information exchange was established between the regions involved and the inter-governmental organizations relevant to the case coordinated sufficiently with regional authorities to identify these so called "red-zones". Similar reports regarding the incidence of cyber attacks were not possible to be conducted with accuracy due to this unprecedented lack of information exchange between stakeholders. While such an attitude is in place, it is impossible for

[18] Cimpean, D. (2011). *ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR*. [online] Heraklion, Greece: ENISA. Available at: http://www.qcert.org/sites/default/files/public/documents/ENISA-CIIP-RP-Analysis%20of%20Cyber%20Security%20Aspects%20In%20The%20Maritime%20Sector-Eng-2011.pdf [Accessed 13 Dec. 2016].

[19] Marine Insight. (2016). *10 Maritime Piracy Affected Areas around the World*. [online] Available at: http://www.marineinsight.com/marine-piracy-marine/10-maritime-piracy-affected-areas-around-the-world/ [Accessed 13 Dec. 2016].

organizations such as the IMO and its member states to identify patterns of hacking that may be prevented and impose the regulations that are necessary to put the situation under control. The areas, where cases like piracy are ordinary, are already common knowledge and should not be correlated with areas where cyber attacks can take place. The Antwerp Port case is a clear example that a maritime cyber attack can occur in unexpected places and under circumstances for which states are not prepared to tackle.

The other predicament caused by the lack of information exchange lies in the fact that maritime cyber security is not currently considered a priority in terms of budgetary allocations. Investments in this sector are not shown to be promising, and ENISA blames the lack of information exchange for that, as it does not allow insurers to have a clear idea of the situation and understand its severity[13]. Insurers are currently lacking the necessary information to improve their actuarial models, reduce own risks, and therefore offer better contractual insurance conditions to the involved maritime stakeholders. On the same note, the lack of information exchange causes problems nationally as well, as parliaments find it increasingly difficult to pass the necessary legislations towards improving cyber security [13]. As long as the governments of each state are not willing to share the complete picture, they cannot justify higher budgetary allocations to cyber-security facilities and their improvement, leaving the maritime sector vulnerable for once more.

5.2. The competence and awareness of those involved

Among the various reasons for which cyber security attacks seem to be increasing during recent years, human error and lack of awareness appear to be the prime one as found in most reports published by intergovernmental organizations. Phishing attacks, social engineering and malicious downloads are only a few examples of how untrained personnel can make grave mistakes and their sadly quite common events. The “Axelos” study that was conducted in the United Kingdom in 2015 revealed that 75% of the nation’s large organisations and one third of the small

ones faced staff-related security breaches, while data obtained from the UK Government's 2015 Information Security Breaches survey reveals that 33% of the nation's shipping companies experienced human-error-related cyber attacks in their IT systems[20]. Such results prove how underestimated cyber security is particularly in the maritime sector. This can also be viewed as a vicious circle in which employee awareness leads to more and more attacks that are not spoken of (as mentioned earlier) leading to even worse awareness and to a perpetuation of the problem.

As staff and their actions are usually the primary vectors for facilitating a cyber attack, one can understand that even the most serious cases of security breaches begin in a very simple way. Malware systems sent via email still remains one of the most common ways of infiltrating IT systems by hackers.[21] Although we are in the 21st century and basic IT skills are considered common knowledge even for the average person, it is striking to see reports like the one by "Axelos" claiming that over 50% of employees are unaware of the simplest dangers that can lead to a security breach. Nick Wilding, the head of the "Axelos" study argues that one of the primary reasons for which employees find themselves "outsmarted" by hackers so easily is that they are not aware of the significance of their role when it comes to maritime cyber security[22]. For many years now cyber security has been viewed as a quite complex concept that only IT experts and high-ranking staff need to be aware of and worry about and that is probably why hackers are targeting the bottom of the hierarchy ladder to initiate an attack.

The truth is that the low levels of employee cyber-security awareness are not a recent realization in the maritime sector. The IMO had identified the problem in the past as well and the importance of training and hiring employees with certified security awareness is part of The International Ship and Port Facility Security Code (ISPS Code) the code by which all member states are to comply. Although the ISPS

[20] HM Government, (2015). *2015 INFORMATION SECURITY BREACHES SURVEY*. London, UK: Ministry of Culture and the Digital Economy.

[21] Rider, D. (2016). *The maritime security cyber threat | Maritime Security Review*. [online] Marsecreview.com. Available at: http://www.marsecreview.com/2015/11/the-maritime-security-cyber-threat/ [Accessed 13 Dec. 2016].

[22] AXELOS. (2016). *Cyber Resilience: Bridging the Business and Technology Divide*. [online] Available at: https://www.axelos.com/case-studies-and-white-papers/cyber-resilience-bridging-the-business [Accessed 13 Dec. 2016].

code may explicitly ask for the training of employees in the maritime sector it is clear that imposing training and maintaining its effectiveness are two completely different concepts. The World Economic Forum issued a report in 2011 that stated that only 33% of businesses were confident about the quality of training the employees are receiving[23]. Cyber attacks are unique in that their facilitators are more flexible than piracy ones for instance as they can find new, innovative ways of performing their plan, overcoming strategies that were used in the past. Alarmingly, security training of employees in the maritime sector does not follow a similar trend, as training schemes are not re-evaluated and remain stagnant, unable to address the continuously changing picture of cyber threats.

5.3. The issue of underdeveloped facilities

Having addressed the importance of human factor in maritime cyber security, it is imperative not to forget that IT facilities and their competence also place a crucial role in the maintenance of safe shipping. When it comes to IT services both hardware and software systems need to be considered, as both require constant updating and careful handling to ensure maximal results[1].

To begin with, portable devices such as computers, laptops and USB sticks, their use in shipping and its correlation with increasing cyber attacks has raised many concerns. It has been argued by many maritime organizations such as ENISA and the NCC group that one key measure towards increasing maritime cyber security is to minimize the use of portable electronic devices to the maximum level possible, in order to eradicate the threat of malware systems being introduced in IT systems of vessels, ports etc[12-13] .It is true that some of the major events of cyber security breaches worldwide started with the use of something as simple as a memory stick used by either infiltrators or employees themselves without their own knowledge. For instance, the DPRK used lorry-mounted portable devices to block GPS signals in

[23] ComputerWeekly. (2016). *Lack of cyber security awareness putting UK organisations at risk*. [online] Available at: http://www.computerweekly.com/news/4500278074/Lack-of-cyber-security-awareness-putting-UK-organisations-at-risk [Accessed 13 Dec. 2016].

South Korea for 16 days, causing 1,016 aircraft and 254 ships to report disruption[24]. Hardware may be more expensive to create but it is significantly faster than having to produce a new code to remotely breach security of a port or especially a vessel that could thousands of miles away from an accurate signal source. As such, it is the primary vector that hackers prefer using to initiate a cyber attack. Although most security regulations are trending towards almost completely banning the use of portable electronic devices in shipping facilities, IT companies like IBM and Cisco are calling for the reconsideration of such measures as they argue that the use of hardware is a double-edged sword when it comes to security. Steve Morgan, founder and CEO of "Cybersecurity Ventures" explained that sophisticated hardware use can be exploited by shipping companies themselves as new, promising hardware systems are designed specifically for maritime security purposes[25].

The software facilities of ports and vessels also find themselves significantly outdated when compared to the ones used by hackers targeting the shipping industry. Again this can be viewed as a consequence of the low position cyber security has in governmental priorities. As it was mentioned, developing and deciphering IT codes can be a very prolonged process and several IT experts on maritime security such as Pierluigi Paganini of "Security Affairs" argue that shipping companies should focus on establishing and frequently renewing their antivirus systems and security protocols rather than spending wasted time trying to determine what code was used by the hackers and implementing that into their IT systems to prevent future attacks of similar nature[1].

The above make the debate of hardware vs. software prioritizing an on-going one, as governments and intergovernmental organisation need to consider whether to invest in innovative hardware facilities that will be present in the short term but will cost vast amounts of funds or to take the risk and stick to the usual strategy of keeping

[24] The Economist. (2016). *Out of sight*. [online] Available at: http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out [Accessed 13 Dec. 2016].

[25] Cybersecurity Ventures. (2016). *The Cybersecurity Market Report*. [online] Available at: http://cybersecurityventures.com/cybersecurity-market-report/ [Accessed 13 Dec. 2016].

software facilities updated, saving on costs but potentially leaving the shipping industry vulnerable to unpredictable attacks.

7. Legal Background

When it comes to Maritime Security the IMO provides support, assistance and guidance to Member Governments on matters relating to the implementation of the following instruments:

6.1. The International Convention for the Safety of Life at Sea (SOLAS)[26]

The SOLAS is probably the most important treaty signed by the member governments of the IMO. It was signed in 1974 and amended several times ever since in order to address newly emerging predicaments. The SOLAS was the first major international treaty to impose global regulations on merchant ships and serves as the primary tool to refer to when needing to deal with issues of maritime security.

6.2. The International Ship and Port Facility Security Code (ISPS Code)[27]

One of the amendments of SOLAS occurred in July 2004 in response to the events of 9/11/2001 in the United States after the terrorist attack at the World Trade Centre. The new chapter added to the Convention included the ISPS Code, the first code created by which all contracting Governments, Government agencies, local administrations and the shipping and port industries have to abide. The ISPS Code requires all contracting parties to determine and allocating roles to the parties involved with security procedures, provides the algorithms for security assessments at port facilities and vessels and ensures that there appropriate exchange of maritime security-related information, at national, regional and international levels.

[26] Imo.org. (n.d.). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. [online] Available at: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx [Accessed 13 Dec. 2016].
[27] Imo.org. (n.d.). *SOLAS XI-2 ISPS Code*. [online] Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx [Accessed 13 Dec. 2016].

6.3. The Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention)[28]

The Achille Lauro incident in November 1985 triggered the meeting of the IMO Assembly and the creation of resolution A.584(14) on "*Measures to prevent unlawful acts against passengers and crews on board ships"*. 3 years later the SUA convention was signed in Rome that among its many articles, most significantly established a legal framework for defining and dealing with unlawful acts against vessels. The SUA convention also explicitly requires all contracting governments to extradite or prosecute the offenders of such actions. The IMO has also introduced several "Code of Conduct" documentation such as the Djibouti and Gulf of Guinea Codes of conduct that aim at addressing specialized cases of regional piracy and identifying idealized solutions and regulations.

Although the above conventions and codes play a crucial role in establishing the very first global scheme for coordination of shipping industries when it comes to maritime security, the all have a very serious limitation: the all focus greatly on aspects of safety and physical security and they do not seem to be addressing the one of cyber security adequately. Apart from the areas discussed above, this limitation can also be attributed to the fragmentation of maritime governance context. With many stakeholders now involved in shipping matters and in a framework that includes intergovernmental organizations, national and global guidelines the coordination between all of those becomes more and more challenging and make the establishment of new regulations quite difficult. Another problem is that apart from the IMO, many regional maritime organizations such as ENISA tend to release their own reports where regional interest may be prioritised over global ones and with cyber security needing a rather international approach to be ensured sufficiently, the IMO has to

[28] Imo.org. (n.d.). *SUA Treaties*. [online] Available at: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx [Accessed 13 Dec. 2016].

make an effort to appear resilient and reliable in being the sole facilitator of such recommendations.

8. Recent developments and on-going action

Despite the many promising steps the IMO has taken towards establishing a global framework for organisations, governments and industries to work within, it has not adequately addressed the issue of cyber security through the majority of its passed resolutions and proposed recommendations. However, the latest Interim Guidelines on Cyber Security Risk Management, introduced in June 2016 show that the IMO is starting to react to the new emerging threat of cyber terrorism[29]. The document was introduced under the work of the MSC (MSC.1/Circ.1526) and offers a detailed approach towards dealing with cyber attacks. The guidelines not only provides adequate information in educating member states on how cyber attacks can emerge, but it also offers a clear algorithm on how to deal with a cyber attack. Namely the guidelines call member states to act in a manner of five steps: 1) **Identifying** the roles and responsibilities of personnel, 2) **Protecting** the continuity of shipping operation during a cyber-event, 3) **Detecting** a cyber-event in a timely manner, 4) **Responding** by restoring shipping operations impaired by the event and 5) **Recovering** sufficiently from the event. These guidelines also endorsed the proposals and recommendations by other maritime organizations such as BIMCO, CLIA, ICS, INTERCARGO and INTERTANKO making the first step towards a sufficient coordination between stakeholders.

[29] IMO, (2016). *Interim Guidelines on Cyber Security Risk Management*. [online] London, UK: IMO. Available at: http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/MSC1Circ1526%20%20Interim%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management.pdf [Accessed 13 Dec. 2016].

9. Possible solutions

The solutions to be obtained can be viewed in three-categories according to how recent their implementation can be, thus adopted according to the severity of situations. They can be seen as short-term, mid-term and long-term ones.

8.1. Possible short-term proposals

The most simple action can be taken right away is to ensure adequate awareness is raised primarily to the public in terms of cyber security in the maritime sector. As it was discussed the importance of the maritime sector in global economy, employment and social stability is of immeasurable value and appealing to that can sensitize the public about the importance of maintaining cyber security. Raising awareness through campaigns for example, will also eventually reach relevant employees indirectly aiming at making more resilient and ready to identify potential threats[13].

Information exchange can also begin to improve in the short-term in order to primarily convince insurance brokers to invest in maritime security management measures. Once this is achieved, stakeholders should start focusing in improving ties between themselves and making sure that important information such as but not limited to the nature of previous attacks, repetitive areas being attacked and patterns used by hackers is shared adequately.

8.2. Possible mid-term proposals

On the basis of employee competence and awareness, stakeholders need to start evaluating the already established training schemes in the public and private sector and amend them accordingly. Governments will need to begin by focusing on facilities such as ports as most cyber attacks focus on such places rather than vessels and then they will need to start imposing assessment checks in shipping companies, requiring them to hire employees that are competent according to the most recent IMO regulations[13].

The IMO also needs to start pushing contracted parties to take appropriate measures in order to add considerations towards cyber security in the regulatory frameworks governing the maritime sector.

The aspect of revolutionizing hardware facilities can also be done in the mid-term. However such a measure needs careful consideration and is dependent on the motives of insurance brokers to invest in cyber security risk management.

8.3. Possible long-term proposals

Evolving software facilities is definitely a long-term measure due to its nature. Stakeholders can start putting this measure into effect even at an earlier time and gradually implement it into the rest of their policies. As it is a relatively cost-effective measure it should be easily integrated by all contracted parties and through time it will have the chance to excel and ensure cyber security management is as efficient as possible.

Other long-term proposals can look into conducting continuous studies and assessments to make sure that other proposed short- and mid-term solutions are in line with concurrent developments and that aspects such as facilities and training schemes remain up-to-date and defendable should hackers find ways to overcome the already established strategies.

9. Conclusion

All in all, it is obvious that the issue of maritime cyber security is one that the international community has not addressed adequately over the last decades. The low awareness on the issue along with the awkwardness that governmental authorities show towards it both hinder real progress and solution establishment. There are a lot of steps that have to be taken in order for the appropriate environment a background to be constructed so that the solutions proposed actually provide the necessary results. With the maritime sector playing such a crucial role in today's economy and social

stability, it is vital that the issue is no longer neglected and that the IMO first takes immediate actions to alert the rest of the world on this huge matter.

10. Structure of the debate during sessions

This section is to help you understand the key questions that need to be answered during debate and to provide you with a template order in which this can be done. However, discussion within the committee may change the order of precedence for the information below, so always keep in mind how the debate proceeds during sessions.

All member states should first attempt to voice their opinion on what they expect from the IMO in terms of improvements when it comes to cyber security. However, member states are advised to not trap themselves in generalizations and to quickly proceed to discussing each aspect of the problem individually and proposing solutions. A template overview of such questions that need to be answered can be:

- Why are member states not disclosing information about cyber attacks and why are they not recognising the threat of hackers in shipping industries? Countries such as China, Somalia, Guinea, Benin, Nigeria and Japan that are known to face such threats need to explain this:
- How can information exchange be encouraged and improved by member states?
- What can the IMO do to ensure the fragmentation of regulation between global, national and intergovernmental stakeholders is minimized?
- What can be done about the very low level of awareness of the public and shipping employees with regards to cyber security?
- Should priority be given towards investing in hardware or software facilities to tackle cyber threats? Why?

11. Further reading

- IMO Member States and Structure: http://www.imo.org/en/About/Pages/Default.aspx

- Interim Guidelines on Maritime Cyber Risk Management: http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/MSC1Circ1526%20%20Interim%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management.pdf
- ENISA Analysis on Maritime Security: http://www.qcert.org/sites/default/files/public/documents/ENISA-CIIP-RP-Analysis%20of%20Cyber%20Security%20Aspects%20In%20The%20Maritime%20Sector-Eng-2011.pdf
- The ISPS Code: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

12. REFERENCES

1. Paganini, P. (2016). *Hacking Ships: Maritime Shipping Industry at Risk*. [online] Security Affairs. Available at: http://securityaffairs.co/wordpress/35504/hacking/hacking-maritime-shipping-industry.html [Accessed 8 Dec. 2016].

2. Reuters. (2016). *All at sea: global shipping fleet exposed to hacking threat*. [online] Available at: http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424 [Accessed 13 Dec. 2016].

3. TTD. (2016). *The Vital Role of Maritime Transportation In Our Economy - TTD*. [online] Available at: http://ttd.org/policy/policy-statements/the-vital-role-of-maritime-transportation-in-our-economy/ [Accessed 13 Dec. 2016].

4. Oxford Economics, (2015). *The economic impact of the UK Maritime Services Sector*. [online] Oxford, UK: Maritime UK. Available at: https://www.maritimeuk.org/documents/1/Combined_The_economic_impact_of_the_UK_Maritime_Services_Sector_ezucVrL.pdf [Accessed 13 Dec. 2016].

5. HISTORY.com. (2016). *Palestinian terrorists hijack an Italian cruise ship - Oct 07, 1985 - HISTORY.com*. [online] Available at: http://www.history.com/this-day-in-history/palestinian-terrorists-hijack-an-italian-cruise-ship [Accessed 13 Dec. 2016].

6. IMO, (2012). *IMO and Maritime Security Historic background*. [online] London, UK: IMO. Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/IMO%20and%20Maritime%20Security%20-%20Historic%20Background.pdf [Accessed 13 Dec. 2016].

7. Agcs.allianz.com. (2016). *Safety & Shipping Review 2016*. [online] Available at: http://www.agcs.allianz.com/insights/white-papers-and-case-studies/safety-and-shipping-review-2016/ [Accessed 13 Dec. 2016].

8. Bueger, C. (2015). *Learning from Piracy: Future Challenges of Maritime Security Governance*. 1st ed. [ebook] Cardiff: Cardiff University. Available at: https://www.cardiff.ac.uk/__data/assets/pdf_file/0013/42412/dr-christian-bueger.pdf [Accessed 13 Dec. 2016].

9. TradeWinds. (2016). *How hackers attacked the Port of Antwerp*. [online] Available at: http://www.tradewindsnews.com/weekly/342065/How-hackers-attacked-the-Port-of-Antwerp [Accessed 13 Dec. 2016].

10. Blogs.cornell.edu. (2016). *A Red Team, a Blue Team, and the White Rose*. [online] Available at: http://blogs.cornell.edu/yachtspoof/ [Accessed 13 Dec. 2016].

11. FedScoop. (2016). *Federal cybersecurity incidents increased more than 1,000 percent since 2006*. [online] Available at: http://fedscoop.com/federal-cyber-incidents-increased-1-121-percent-since-2006 [Accessed 13 Dec. 2016].

12. Saunders, B. (2015). *Maritime Cyber Security Threats and Opportunities*. CIRM Annual Meeting. [online] Nicosia, Cyprus: NCC Group. Available at: https://www.nccgroup.trust/globalassets/resources/uk/presentations/2015/maritime-cyber-security-threats-and-opportunities.pdf [Accessed 13 Dec. 2016].

13. Cimpean, D. (2011). *ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR*. [online] Heraklion, Greece: ENISA. Available at: http://www.qcert.org/sites/default/files/public/documents/ENISA-CIIP-RP-Analysis%20of%20Cyber%20Security%20Aspects%20In%20The%20Maritime%20Sector-Eng-2011.pdf [Accessed 13 Dec. 2016].

14. Marine Insight. (2016). *10 Maritime Piracy Affected Areas around the World*. [online] Available at: http://www.marineinsight.com/marine-piracy-marine/10-maritime-piracy-affected-areas-around-the-world/ [Accessed 13 Dec. 2016].

15. HM Government, (2015). *2015 INFORMATION SECURITY BREACHES SURVEY*. London, UK: Ministry of Culture and the Digital Economy.

16. Rider, D. (2016). *The maritime security cyber threat | Maritime Security Review*. [online] Marsecreview.com. Available at: http://www.marsecreview.com/2015/11/the-maritime-security-cyber-threat/ [Accessed 13 Dec. 2016].

17. AXELOS. (2016). *Cyber Resilience: Bridging the Business and Technology Divide*. [online] Available at: https://www.axelos.com/case-studies-and-white-papers/cyber-resilience-bridging-the-business [Accessed 13 Dec. 2016].

18. ComputerWeekly. (2016). *Lack of cyber security awareness putting UK organisations at risk*. [online] Available at: http://www.computerweekly.com/news/4500278074/Lack-of-cyber-security-awareness-putting-UK-organisations-at-risk [Accessed 13 Dec. 2016].

19. The Economist. (2016). *Out of sight*. [online] Available at: http://www.economist.com/news/international/21582288-satellite-positioning-data-are-vitalbut-signal-surprisingly-easy-disrupt-out [Accessed 13 Dec. 2016].

20. Cybersecurity Ventures. (2016). *The Cybersecurity Market Report*. [online] Available at: http://cybersecurityventures.com/cybersecurity-market-report/ [Accessed 13 Dec. 2016].

21. Imo.org. (n.d.). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. [online] Available at: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx [Accessed 13 Dec. 2016].

22. Imo.org. (n.d.). *SOLAS XI-2 ISPS Code*. [online] Available at: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx [Accessed 13 Dec. 2016].

23. Imo.org. (n.d.). *SUA Treaties*. [online] Available at: http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/SUA-Treaties.aspx [Accessed 13 Dec. 2016].

24. IMO, (2016). *Interim Guidelines on Cyber Security Risk Management*. [online] London, UK: IMO. Available at: http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/MSC1Circ1526%20%20Interim%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management.pdf [Accessed 13 Dec. 2016].