National Maritime Foundation

www.maritimeindia.org

Industry 4.0 in the Shipping Industry: Challenges and Preparedness – The Prevailing Scenario

Namita Barthwal[1] and Cdr (Dr) Nitin Agarwala[2]

Introduction

The rapid and inexorable rise in the 1990s of the internet, networking, and digital communication, which, in aggregate, represents 'cyberspace', has produced startling and indelible changes in almost all aspects of modern life. The accelerated growth of cyberspace has given birth to a new industrial revolution, often called the 'Fourth Industrial Revolution'. In this revolution, which is an ongoing one, industry is experiencing a distinct movement towards digitalisation,[3] automation and data-exchange, in both, the secondary[4] and the tertiary sectors.[5] In the continuing effort to create a holistic and better-connected ecosystem, this phase in the industrial landscape, which focuses intensely on interconnectivity, machine learning, and real-time data, has resulted in a sharp enhancement in productivity and has been branded '**Industry 4.0**'. In recent times, the concept of Industry 4.0 has been deployed in the global shipping industry, too, and has led to the development of an ecosystem that is increasingly being defined by the Internet of Things (IoT), for the shipping industry to manage navigation and operations, through computers.

Industry 4.0, is, of course, not without significant challenges of its own. Today, cybercriminals are embezzling users of virtual space (cyberspace). Their targets range from individuals to companies. In this scenario, the shipping industry has become an especially attractive target for cybercriminals, largely because it moves goods of large monetary value from and to ports, through shipping. Unfortunately, this industry is also amongst the least prepared to guard itself against cyber transgressions. In 2017, a major cyber-attack on AP Møller-Maersk, the world's largest container shipping company, using the *NotPetya* virus, served to dramatically (and quite catastrophically) highlight the severe vulnerabilities of the shipping industry in this digital world. These vulnerabilities are now a major area of concern, thereby necessitating the need-for and the consequent growth-of the 'maritime cybersecurity' market.

According to predictions by *Cybersecurity Ventures*, a leading source of cybersecurity facts, figures and statistics, global spending on cybersecurity products and services is likely to exceed US$ 1 trillion, cumulatively, during the period from 2017 to 2021.[6] This growth is a direct outcome of rising cyber-crimes and the increases in frequency and level of sophistication of cyber-attacks on the shipping industry. This has made the shipping industry a very significant consumer of cybersecurity products so as to be able to safeguard its IoT-dominated ecosystem. These products include guidance, sensors, controls, command and communication systems, and, their hydra-headed linkages to coastal infrastructure.

This article offers an empirical overview of**:** **(a)** the digital revolution in the shipping industry; **(b)** the cyberspace challenges in the shipping industry; **(c)** the level of preparedness of the shipping industry to handle prevailing and future cyber-threats, and **(d)** the role of the cybersecurity market in providing solutions to these cyber-threats.

The Digital Revolution in the Shipping Industry

As industries revolutionise themselves through Industry 4.0 by using technologies such as machine-to-machine communication, cognitive computing, Radio Frequency Identification (RFID), IoT, robotics, cloud computing, mobile technologies, etc., computing, data-storage, connectivity and production-efficiency improved by leaps and bounds, resulting in a spurt in the growth of the world economy. Taking careful note of the fact that this growth was being achieved through the increasingly ubiquitous use of technology, the global shipping industry — which is the lifeblood of the global economy and is manifested in the 50,000 ships that are at sea or in ports at any given moment of time (see Figure 1), moving about 90 per cent of world-trade by volume, and, in the process, generating an estimated annual income of over half trillion USD in freight rates[7] — felt the need to replicate this technology-driven growth. Hence, Industry 4.0 was embraced by the shipping industry to improve its value-chain and its management, in an effort to enhance profits and reduce overheads by improving efficiency.

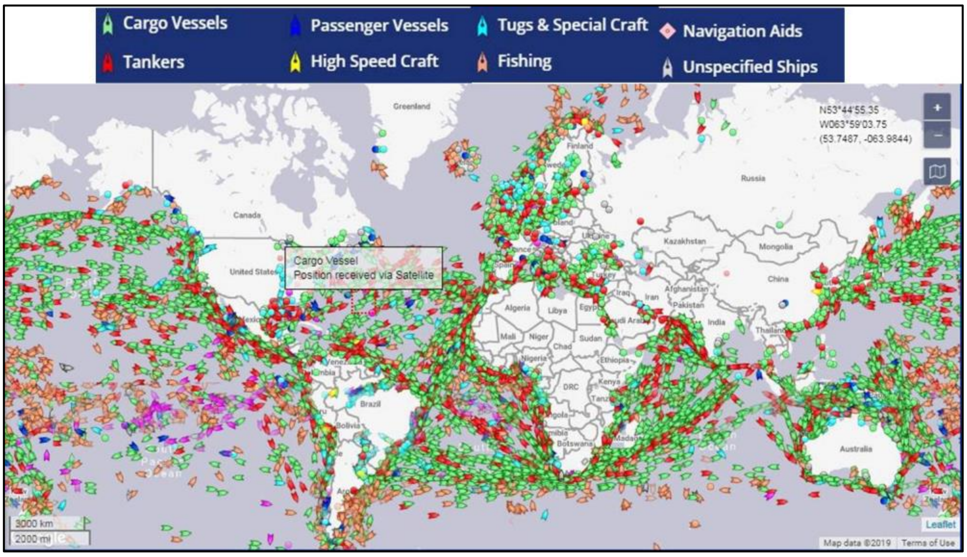

Figure 1: Vessels at sea and in port
Source: www.marinetraffic.com

This effort drove the shipping industry to promote sophisticated developments in areas such as connectivity, maintenance and safety, etc., through digitalisation. Today, the shipping industry uses digitalisation for connectivity — to get real-time information about a ship's performance at sea; for maintenance — to enable remote diagnostics of machinery of ships at sea; and, for safety — to ensure the shore-based monitoring of gas-emissions and cargo temperatures of its seagoing assets, so as to decrease the operational cost and risk of failure due to negligence.

Although digitalisation in the shipping industry is still in an embryonic phase, it has already become hugely popular. This popularity has led to an exponential creation of data that is supported efficiently by hardware (computing power) and 'Cloud'-based data-storage solutions (on-site storage). Another area where digitalisation is being implemented in the shipping industry (even though it is still in a nascent stage) is in cargo shipment using **blockchain technology**. A 'blockchain' is basically a way to store, share, and verify information, using a 'ledger'. The stored information in the blockchain exists as a shared, secured, decentralised, and encrypted 'public ledger', which inherently resists any modification and is easily verifiable. This therefore enhances cybersecurity, resulting in the blockchain process becoming a platform of trust and value in industries that have adopted this technology. The introduction of blockchain technology in the shipping industry has the potential to cut administrative and operational risks for shipowners, charters and brokers,[8] as it ensures greater transparency, enhances security, improves traceability, increased efficiency and speed of transactions, and reduces costs. In January of 2018, AP Moller-Maersk (Maersk) and IBM jointly announced the launch of 'TradeLens'[9] — an internet-based platform intended to apply blockchain technology to the global supply chain. In August of that same year, in a follow-up of their January announcement, the two partner companies also announced that 94 organisations were actively involved or had agreed to participate on the TradeLens platform, built on open standards.[10] In the first year of its use alone, the time of shipments in the United States has been reduced by 60 per cent.

As it stands, overall digital transformations, as part of Industry 4.0, are in progress for the betterment of the shipping industry. However, at the same time, it is essential to acknowledge the challenges associated with this technological development. To understand challenges faced by the shipping industry due to the growth of cyberspace, it is instructive to look at prevailing cyber-threats.

Cyberspace Challenges in the Shipping Industry

In the shipping industry, cyber-dependence has spawned unprecedented threats from unknown sources that are difficult, if not impossible, to identify. Cyber-threats in the shipping domain may be divided into two categories – targeted and untargeted.[11] *Targeted* attacks are where a company or a ship's systems and data are, indeed, the intended targets. Targeted attacks include the use of brute force, denial-of-services, spear-phishing, subverting the supply chain, port-scanning, etc.[12] On the other hand, *Untargeted* attacks are those where a company or a ship's systems and data are merely one of many potential targets. These untargeted threats include, *inter alia*, malware attacks, phishing, water-holing, and, scanning. In addition, cyber-threats in the shipping industry may be 'intentional' or 'unintentional'. *Intentional* cyber-threats are those where the cyber breach comes from intentional malicious actions, while *unintentional* cyber-threats are those where the breach is a result of negligence or ignorance. It is essential that the shipping industry identifies the predominant cyber threats before looking at means to address them.

With digitalisation, even piracy has gone high-tech. Today, cargo ships, oil tankers, and super yachts are facing an increasing threat from cyber-attackers[13] who can cause service-disruption, system-downtime, financial loss, cargo-theft, loss of contracts, and, reputational-damage. These cyber-attackers are able to attack critical systems of a target-ship, such as the propulsion, machinery, and navigation systems. They can threaten or actually cause ecological disasters such as oil spills by actions such as the opening of remotely-controlled or automated discharge valves,[14] or, causing groundings or collisions through the malicious manipulation of GPS signals and receivers. Malicious manipulation of positional, heading and speed data can cause a ship to change direction, making it susceptible to piratical attacks. Likewise, shipborne radars can be jammed, making the ship blind to its surroundings. Any attack of this nature can lead to disruption and collision of ships in busy shipping lanes[15] and can severely harm the shipping industry, the energy industry, and also the marine environment.

A maritime cybersecurity survey, conducted in 2018 by the 'The Baltic and International Maritime Council' (BIMCO), Fairplay, and ABS Advanced Solutions,[16] provides some idea of the nature of cyberthreats experienced by the maritime industry. These threats include phishing, malware, spear phishing, threat of credentials, ransomware, theft of data, man-in-middle application-level attacks, breach of procedure, known vulnerability-exploitation, brute force, network-protocol attack, manipulation of data, loss of operational control, and, honeytraps. The study revealed that: **(a)** of these threats, phishing and malware are the *major cyber challenge*, **(b)** the shipping sector is the *major target*, **(c)** 'theft of credentials' was the *major reason* of cyberattacks, which increased significantly from 2 per cent in 2017 to 28 per cent in 2018, and, **(d)** the *major result* of these attacks was loss of corporate data, lowering of performance of IT system and financial loss.

In recent years, the shipping industry has faced many cyber-attacks. The most significant and an extremely high-profile incident was that the attack on AP Møller-Maersk,[17] on 27 June 2017, when a malware called 'NotPetya'[18] destroyed almost the entire AP Møller-Maersk computer network. 'NotPetya' was a 'ransomware' that came through software used by companies to file their tax returns. After hijacking the network of the company, the attackers, based in Ukraine,[19] demanded a payment of US$ 300 worth of bitcoins (~ US$ 16,88,926/-) to decrypt the important files from the Maersk database. The company refused to pay the ransom and tried to resolve the problem on its own. Since the ransomware attack was a severe one, it corrupted the Maersk's network extensively, preventing the company's IT experts from recovering the data. In the end, instead of recovering the data, the company chose to reinstall over 4,000 servers, 45,000 computers, and 2,500 applications. The resulting loss to Maersk is estimated to have been between 250 million and 300 million US Dollars.

In January of 2018, after the cyber-attack, AP Møller-Maersk's Chairman, Jim Hagemann Snabe, accepted that *"we were basically average when it comes to cybersecurity, like many companies, and this was a wake-up call."*[20] At nearly the same time, on 24 July 2018, the Chinese shipping and logistics company, the China Ocean Shipping (Group) Company (COSCO), too, became a victim of a ransomware attack. The attack was not severe, but it alarmed the shipping sector.[21] Other large shipping companies that have faced cyber-attacks include the BW Group[22] and the Clarksons.[23] These cyber-attacks on big and powerful shipping houses brings into question the level of preparedness of the shipping industry to cyber-attacks.

Level of preparedness to tackle cyber-threats

Several reports and surveys indicate that the *maritime industry* is ill-equipped to deal with cyber threats. The Global Maritime Issues Monitor,[24] in its report of 2018, brings out that cyber-attacks and data-theft are among the top issues impacting the maritime industry, while the preparedness to tackle these specific cyber-threats is the poorest. Similarly, in 2017, in order to diagnose the lack of preparedness of the *shipping industry* in tackling prevailing cyber threats, the Jones Walker LLP[25] conducted a maritime cybersecurity survey of the US maritime industry. The report revealed that the US maritime industry had a false sense of preparedness. While 69 per cent of the respondents believed that the industry was ready to handle devastating cyber-attacks, only 36 per cent believed that their own company was prepared. Highlighting the insignificant level of preparedness to deal with cyber-threats in the maritime sector the survey brought out that, *"Hackers are modern day pirates who have the ability to sink maritime industry sectors that are unprepared for what's coming at them."*[26]

When talking of preparedness of the *crew* to protect a ship from cyber-attacks, the lack of preparedness is starkly visible. In the Crew Connectivity Survey 2015[27] (conducted by Futurenautics) it was found that only 12 per cent of crew members had received any form of cyber training. In addition, only 43 per cent of crew members had any knowledge of cyber hygiene provided by their company for personal web-browsing. Unsurprisingly, 43 per cent of the survey participants revealed that they had sailed on vessels that had become infected with a virus or malware. Even now, these figures have not changed by much.

While there certainly is a distinct lack of preparedness of the shipping industry and the crew to tackle cyber-attacks, much of the blame must be attributed to the lack of a regulatory framework for cyber security in the shipping industry. Although the International Maritime Organisation (IMO), in 2017, amended its two general security-management codes — the International Ship and Port Facility Security (ISPS) Code and the International Safety Management (ISM) Code to explicitly include cybersecurity and how the maritime industry should undertake cyber risks management processes, these amendments will come into force only by 01 January 2021. These slow developments in maritime cybersecurity regulation have left the shipping industry to face the brunt of repeated cyber-attacks.[28]

The slow development notwithstanding, in 2018, a group of the world's largest shipping associations, which included BIMCO, the International Union of Marine Insurance (IUMI), the International Association of Independent Tanker Owners (INTERTANKO), the International Association of Dry Cargo Shipowners (INTERCARGO), the Oil Companies International Marine Forum (OCIMF), the World Shipping Council, and, the International Chamber of Shipping, collaborated to jointly prepare and release a manual titled, *"Guidelines on Cyber Security Onboard Ships"*. This manual is aimed at improving a ship's safety management system, risk assessments for operational technology, and, in addition, offers guidance for identifying and tackling on-board cyber security threats arising from the external supply chain. The guidelines also set-out the cyber risk-management approach and exhorts the IMO to stay engaged throughout the process so as to ensure that the protection, and contingency- and response-planning, are balanced in relation to the threats, vulnerabilities, risk-exposure and consequences of a potential cyber accident.[29]

Despite realising the accelerated dangers of the cyberspace, cyber risk-management in the maritime industry is moving at a painfully slow pace. This has forced the owners of the shipping companies to engage with cyber-security providers to minimise the losses arising from cyber incidents. This has, in turn, led to the emergence of the maritime cybersecurity market.

The Cybersecurity Market

In order to achieve requisite cyber protection, the shipping industry relies heavily on external parties such as technology consultancies, security experts, and software suppliers. These external parties sell cybersecurity products to shipping companies and enhance the security of their Information technology (IT), Operational technology (OT) and navigation systems. It is essential to mention that the cyber-industry is not currently investing in the shipping industry directly, due to the lack of consciousness about cyber threats in the industry. Further, the industry and its IT infrastructure is obsolete and does not adhere to the latest IT standards.

Over the years, several cybersecurity companies and consultants have emerged, specifically to address the cyber challenges of the shipping industry and to provide solutions to develop a secure digital environment. Some of these key firms are:

(a) The ‘MTI Network’, which trains shipping industry employees to recognise cyber-attacks and implement policies on computer hardware usage, particularly the use of USB memory sticks.[30]

(b) Marlink, which has provided a facility called Cyber Guard that enables Marlink customers to protect, detect and resolve any cyber-threat through a holistic combination of network resilience and redundancy, dedicated maritime cyber-security technology and maritime security experts.[31]

(c) The Seawall Scan, an open source firewall, helps the industry to test ship systems to detect security weaknesses.[32]

(d) Other cybersecurity firms such as the Cydome, the CyberSail, the Hudson’s Cyber Risk Management, the Solace Global, and the Gard, are dedicated to provide cybersecurity services to the shipping industry.

Recommendations to Improve Cybersecurity in the Shipping Industry

Although it is believed that in the shipping industry cyber security has to be expensive and supported by external parties, this is not true. Simple measures that are inexpensive and safe can be put in place to provide a secure cyber-environment. These measures include actions such as regularly and frequently updating systems, configuring networks features, testing security features, and, training users to operate the systems optimally.

Further, it is an accepted fact most shipowners do not have a comprehensive knowledge of the cyber risks. There is, therefore, a clear need to improve this situation. Towards this end, four key steps have been recommended by Max J. Bobys, Vice President of the Hudson’s Cyber Risk Management. These are:

(a) To develop cyber-loss scenarios that could impact the business and determine their exposure values. Since smaller scale scenarios cover site-specific instances, such as how a vessel or an office might be impacted, the need is to have a broader thinking to characterise how a multi-vessel/site attack might impact the overall business.

(b) To review and test existing insurance policies against the loss scenarios.

(c) To perform a top-down, cybersecurity capability maturity-model based evaluation. This is considered essential since cyber risk needs to continuously and proactively managed as an organisational risk.

(d) To sustain cyber risk management resources. This can be achieved by ensuring that personnel are trained; insurance policies are updated to support incident reporting and recovery; and, to maintain budgets to support a range of technical and non-technical cybersecurity investments.

Conclusion

A majority of the world's trade is moving by sea, along International Shipping Lanes (ISL). Statistics by the United Nation Conference on Trade and Development (UNCTAD) shows that international seaborne trade gathered considerable momentum in 2017, with volumes expanding by 4.0 per cent. It is expected that this trend will continue over the coming years. Simultaneously, ships, ports, and mobile offshore units, are becoming increasingly connected and reliant on software-dependent systems. In this scheme of things, the shipping industry is clearly a vulnerable target for cyber-attackers. Hence, it is essential for the shipping industry to develop a protected IoT ecosystem and the ability to recognise the risks associated with the cyber domain, including technologies such as radars, sensors, and drones. It is essential to understand that if digitalisation were to continue without proper security measures, it could have serious repercussions on both, the shipping industry and the world economy. It is hence vital to maintain the integrity and resilience of cyber-physical system through a holistic approach.

This article has sought to provide an overview of the lack of consciousness, awareness and protection mechanisms against cyber-attacks within the shipping industry. At the moment, the preparedness of the shipping industry to deal with cyber threats is unacceptably low. Currently, the internal mechanisms of the industry are slow in framing cyber risk management policies, while those policies that have been adopted by the IMO are still to come in force. Consequently, there is no available and usable framework to deal with the vulnerabilities associated with Industry 4.0.

As digitalisation facilitates an efficient business environment, a gain in the value chain, and serious damage to the business if adequate precautions are not taken, it is necessary that adequate steps are taken by the shipping industry to increase opportunities and decrease risks associated with Industry 4.0, through qualitative management.

Although technology-consultants are supporting the shipping industry in tackling this demand of cyber-security, the need of the hour is to train personnel and ensure upgradation of the IT infrastructure aboard ships, so as to have better involvement of the cyber industry in developing and ensuring a robust cyber-system for the shipping industry. However, until that is done the shipping industry must persist with inhouse measures that would provide for the requisite degree of cyber-security.

****

The views expressed by the authors are their own and do not reflect the official policy or position of the Government of India, the Indian Navy, or, the National Maritime Foundation.

Notes and References

[1] Research Intern at the National Maritime Foundation. Can be contacted at namita.barthwal@gmail.com

[2] Research Fellow at the National Maritime Foundation. Can be contacted at nitindu@yahoo.com

[3] The *digitisation* and *digitalisation* are different terms that are mistakenly used as synonyms. *Digitisation* means taking analogue information and encoding it into binary format (using *zeroes* and *ones*), so that computer could store, process and transmit such information, whereas *digitalisation* is an ambiguous term, which means a way in which many social domains are structured or restructured around digital communication and media infrastructure.

[4] The secondary sector encompasses manufacturing — the making, building, and assembling of finished products.

[5] The tertiary sector provides services to consumers and businesses and includes retailers, transportation and entertainment companies, banks, and healthcare providers.

[6] Steve Morgan, Cybersecurity Market Report, 2018; retrieved on 18 April 2019 from https://cybersecurityventures.com/cybersecurity-market-report/

[7] Shipping and World Trade, data by International Chamber of Shipping (ICS); retrieved on 18 April 2019 from http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade

[8] Alexander Farnsworth, "BlockChain- The case for digitalising shipping", Wartsila, 2 January, 2019; retrieved on 18 April 2019 from https://www.wartsila.com/twentyfour7/innovation/blockchain-the-case-for-digitalising-shipping

[9] Is an open and neutral industry platform underpinned by Blockchain technology, supported by major industry players? See, *for example*, https://www.tradelens.com/

[10] IBM Newsroom: "Maersk and IBM Introduce TradeLens Blockchain Shipping Solution", Copenhagen, Denmark, and ARMONK, NY, 09 Aug 2018, from https://newsroom.ibm.com/2018-08-09-Maersk-and-IBM-Introduce-TradeLens-Blockchain-Shipping-Solution

[11] Sotiria Lagouvardou, *Maritime Cyber Security: concepts, problems and models,* Thesis, DTU Management Engineering: 2018, pp. 44-48; retrieved on 18 April 2019 from http://orbit.dtu.dk/files/156025857/Lagouvardou_MScThesis_FINAL.pdf

[12] ibid, p. 44

[13] Luke Graham, "The new face of piracy: cybercrime is threatening the shipping industry", City A.M, 26 November, 2018; retrieved on 18 April 2019 from http://www.cityam.com/269633/new-face-piracy-cyber-crime-threatening-shipping-industry

[14] Luke Graham, "The new face of piracy: cybercrime is threatening the shipping industry", City A.M, 26 November, 2018; retrieved on 18 April 2019 from http://www.cityam.com/269633/new-face-piracy-cyber-crime-threatening-shipping-industry

[15] In 2016, 280 South Korean vessels returned to the port after experiencing problems with their navigation systems. The South Korean government blamed North Korea behind the disruption, but was unable to obtain evidence for the accusation. See, *for example*, Jonathan Saul, "Cyber threats prompt return of radio for ship navigation", Reuters, 7 August, 2017; retrieved on 18 April 2019 from https://www.reuters.com/article/us-shipping-gps-cyber/cyber-threats-prompt-return-of-radio-for-ship-navigation-idUSKBN1AN0HT

[16] IHS Markit, *2018 Maritime Cyber Security Results*, Results Overview; retrieved on 18 April 2019 from http://www.nepia.com/media/977540/Fairplay-and-BIMCO-Maritime-Cyber-Security-survey-2018.pdf

[17] A Danish maritime business conglomerate, operating in more than 120 countries; provide services in 300 ports around the world and nearly 800 vessels. The company represents one-fifth of the entire world's shipping capacity.

[18] A malware that aims to encrypt the hard drive of infected computers and does not require human intervention to spread itself

[19] Andy Greenberg, "The untold story of NotPetya, the most devastating cyberattack in the history", Wired, 22 August, 2018; retrieved on 18 April 2019 from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

[20] Catalin Cimpanu, "Maersk Reinstalled 45,000 PCs and 4,000 Servers to Recover From NotPetya Attack", Bleepingcomputer, 25 January, 2018; retrieved on 18 April 2019 from https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/

[21] "COSCO Shipping Lines Falls Victim to Cyber Attack", World Maritime News, 25 July, 2018; retrieved on 18 April 2019 from https://worldmaritimenews.com/archives/257665/cosco-shipping-lines-falls-victim-to-cyber-attack/

[22] Jamey Bergman, "Tanker group says it faced cyber-attack in July", Maritime Digitalisation and Communications, 17 October, 2017; retrieved on 18 April 2019 from https://www.marinemec.com/news/view,tanker-group-says-it-faced-cyber-attack-in-july_49564.htm

[23] Notice of cybersecurity incident, CLARKSON PLC, 29 November 2017; retrieved on 18 April 2019 from https://www.clarksons.com/media/1129201/notice_of_cyber_security_incident.pdf

[24] Global Maritime Issues Monitor, 2018, MARSH and IUMI; retrieved on 18 April 2019 from https://www.globalmaritimeforum.org/content/2018/10/Global-Maritime-Issues-Monitor-2018.pdf

[25] Jones Walker LLP 2018 Maritime Cybersecurity Survey; retrieved on 18 April 2019 from https://sites-communications.joneswalker.com/38/1033/uploads/2018-jones-walker-llp-maritime-cybersecurity-white-paper.pdf?intIaContactId=8590524490&intExternalSystemId=1&strExternalSystemType=Interaction%205.6

[26] Hellenic Shipping News Worldwide article "Maritime Cybersecurity Survey Indicates Industry is Unprepared for Risks"; retrieved on 18 April 2019 from https://www.hellenicshippingnews.com/maritime-cybersecurity-survey-indicates-industry-is-unprepared-for-risks/

[27] Lean Kinthaert, "8 Experts Weigh In on Cybersecurity in Shipping & Maritime", KNet365, 9 April 2017; retrieved on 24 April 2019, https://knect365.com/shipping/article/56554e0a-1356-42ac-88cd-564a389bcd1e/cybersecurity-shipping-maritime

[28] Forbes Vivian Louis, 2018, "The Global Maritime Industry Remains Unprepared for Future Cybersecurity Challenges", Future Direction International, 21 August 2018; retrieved on 18 April 2019, http://www.futuredirections.org.au/wp-content/uploads/2018/08/Global-Maritime-Industry-Remains-Unprepared-for-Future-Cybersecurity-Challenges.pdf

[29] The Guidelines on Cyber Security Onboard Ships, Version 3; retrieved on 18 April 2019 https://iumi.com/uploads/2018-Cyber_Security_Guidelines.pdf

[30] MTI Network article "Taking Cyber Security seriously" Retrieved on 18 April 2019 https://www.mtinetwork.com/taking-maritime-cyber-security-seriously/

[31] "Cyber Security in the Maritime Industry", 20 November 2018, Maritime Digitalisation & Communication; retrieved on 18 April 2019 https://www.marinemec.com/news/view,cyber-security-in-the-maritime-industry_55948.htm

[32] Seawall cybersecurity protection package presentation; retrieved on 18 April 2019 https://docs.wixstatic.com/ugd/90f4b3_ef08ea2b9f7f4d288eca48289f70c744.pdf