MARITIME CYBERSECURITY: VULNERABILITIES AND COUNTER MEASURES

Zaheema Iqbal[*] & Muhammad Khurram Khan[**]

Abstract

In the era of technological advancements and digitization, the security phenomenon encompasses both physical and digital paradigms. The recent developments in cyber security domain reveal an increased number of cyberattacks on critical infrastructures, organizations, and industries. The maritime industry, being the critical infrastructure of any nation, is no exception to it, which is also vulnerable to cyberattacks. With terminals, vessels, ships, transport operators, ports and any other interconnected and integrated critical infrastructure are prone to cyberattacks. This paper discusses the important concepts such as 'maritime' and 'cyber security in maritime industry' and explains the utmost significance of cyber security at sea both on land and on board. It further discusses the major global cyber security incidents to determine vulnerabilities in maritime industry and also highlights challenges faced by maritime stakeholders amidst the COVID-19. Finally, this paper looks into existing cyber security measures and guidelines in the maritime industry.

Keywords: *Maritime, Cybersecurity, Cyberthreats, Maritime Cyber Security, Covid-19*

Introduction

The maritime sector is known as 'reactive' in terms of setting regulations and standards based on catastrophic incidents. Citing an example in this context would be the sinking of 'RMS Titanic' which clashed with an iceberg during her first journey to New York City from Southampton, United Kingdom on April 15, 1912.[1] The Titanic was

[*] Senior Research Associate at National Institute of Maritime Affairs, Bahria University Islamabad. Email*:* zaheemaeckbaull@gmail.com

[**] The founder and CEO of the Global Foundation for Cyber Studies and Research. Email*:* mkhurram@ksu.edu.sa

[1] Charles D. Michel, Paul F. Thomas, and Andrew E.Tucci, "Cyber Risks in the Marine Transportation System, The US Coast Guard Approach," 2009,

believed by the world to be indestructible, and it departed on her first trip having minimum lifejackets and lifeboats for the crew. It is noteworthy to mention that the shortage of safety and security equipment wasted more than 1500 lives.[2] As a result, the global maritime community stepped forward and initiated the Safety of Life at Sea (SOLAS) Convention in 1913 to lay down shipping practices and regulations for international seafaring vessels.[3] The next year brought together world maritime leaders in 1914, who mandated maritime safety requirements including capacity, loading, durability, lifeboat building requirements, and availability of lifejackets to every person onboard.[4]

In the context of cyber threats, global maritime community usually acts in reaction to the unprecedented event, which happens in cyber domain. There is no doubt that maritime cyberattacks are increasing than the maritime community believed due to unregulated attacks.[5] It is largely due to the fact that ships of any country are foreign vessels and crewed by foreigners.[6] For instance, the US Department of Transportation's Maritime Administration Office of Financial and Rate Approvals released a report, which analyzed the leading five port concentration areas in the US: Los Angeles, Houston, Miami, Newark/New York, and New Orleans.[7] They actually drew special attention to the size of crew and nationalities of foreign-flag cargo vessels calling at US ports. The notable five flags for ships, which visit these ports include: Panama, Liberia, Cyprus, Bahamas, and Malta. The report stated that crewmembers belonging to 123 different

https://www.dco.uscg.mil/Portals/9/CGFAC/Documents/USCG_Paper_MTS_CyberRisks.pdf

2 Mandy Savage, "Five Safety Lessons Learned from the Sinking of the Titanic," *EHS Today*, April 14, 2015, https://www.ehstoday.com/safety/article/21916859/five-safety-lessons-learned-from-the-sinking-of-the-titanic

3 Michael Clancy et al., *Cruise Ship Tourism* (Oxford: CABI, 2017).

4 Jolanta Joszczuk Januszewska, *Importance of Cloud-Based Maritime Fleet Management Software* (Springer, 2013), https://link.springer.com/book/10.1007/978-3-642-41647-7.

5 Don Walsh, "Oceans - Maritime Cyber Security: Shoal Water Ahead?" *U.S. Naval Institute*, February 21, 2019, https://www.usni.org/magazines/proceedings/2015/july/oceans-maritime-cyber-security-shoal-water-ahead.

6 Steven L Caponi, and Kate B Belmont, "Maritime Cyber Security: A Growing Threat Goes Unanswered," *Intellectual Property & Technology Law Journal Vol 27, Issue 1, (2015)*, 16-18.

7 Alexeis Garcia Perez, Mick Thurlbeck, and Eddie How, "Towards Cyber Security Readiness in the Maritime Industry: A Knowledge-Based Approach," Coventry University, 2017. https://pure.coventry.ac.uk/ws/portalfiles/portal/12219284/Towards_Cyber_Security_Readiness_In_The_Maritime_Industry.pdf.

countries were found on foreign-flagged vessels.[8] It shows that with so many distinct nationalities and stakeholders involved, regulating the vessels entering a port under cybersecurity standard is arduous to implement.

Since the developments of information technology, computer networking, and software systems in maritime industry, various cybersecurity challenges have emerged with the passage of time. The information and data, driving the maritime operations and infrastructure are exposed to cyber criminals and groups who may pose a grave threat for the security of maritime industry. Within the context of maritime industry and maritime infrastructure, cybersecurity may be taken as the safeguarding of electronic networks, communication systems, software, control algorithms, users, unauthorized access, damage, manipulation and underlying data within the maritime infrastructure from various cyberattacks.

In past, traditional threats like piracy were a common risk. In this regard, physical defense was all understood. On the contrary, cyber-attack at ships is not well understood thus, less countermeasures were taken. The latest technology in cyber-attacks and long durations increase cyber threats on maritime installations. Such maritime cyberattacks result in theft of information, business disruption, and damage to the reputation, environment, and goods etc. For instance, Automatic Identification System (AIS), which is used for vessel tracking and positioning, is not protected through encryption. Through spoofing, AIS signal can easily be used to disguise its position and make false navigation. Weak, unencrypted and authenticated signals are widespread for the determination of location. University of Texas has undertaken a test in 2013 in which, authentication was exploited and overpowered by a GPS spoofing device with the use of inbound signals.[9] This test resulted into taking over the $80 Million vessels' navigation system effectively.

There are majority of companies worldwide, which are in process of commercializing blockchain technology in order to enhance virtual global trade platform.[10] There are organizations, which are fostering the

---

8 Carmen Casado, "Vessels on The High Seas: Using A Model Flag State Compliance Agreement To Control Marine Pollution," *Scholarly Commons*, March 2, 2005, https://scholarlycommons.law.cwsl.edu/cwilj/vol35/iss2/3/

9 UT News, "UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea," *The University of Texas at Austin News*, August 7, 2018, https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/

10 "Annual Report 2018," *MAERSK*, 2018, https://investor.maersk.com/news-release/news-release-details/annual-report-2018,accessed 29 March 2020.

digital platforms for cyber security programs.[11] Rolls Royce and Google are working on autonomous shipping and intelligent systems.[12]

Nevertheless, interconnected shipping industry calls for effective operational time and effectiveness of various processes for the transaction of every business. It is important to remember that development and progress of cybersecurity goes in parallel with the latest technological advancements. Nevertheless, insufficient knowledge with regards to cybersecurity issues and prospective challenges, which maritime companies face these days. This paper explores the significance of cyber security in the maritime industry and the major incidents occurred in near past. It also discusses how important it is to secure maritime infrastructure from cyber threats in this age of technological advancements. The first section of paper delineates the definitions of cyber security, maritime sector, and volume of cyber security in the maritime industry. The second section looks into incidents of cyberattacks on maritime infrastructure at global level and explains the cyber threats to maritime infrastructure during the COVID-19 times. The last section deals with the cyber security measures in the maritime industry.

Cyber Security Maritime Definitions

Cyber security is a vast and broad term having context-bound, high variables, often subjective and uninformative definitions. There is literature available, which states the term cyber security, what does it mean and how it is placed within different contexts. However, the concise and broadly accepted definition of cyber security is still absent, which may capture the multidisciplinary approach.[13] The maritime experts are yet to establish the universal definition of "maritime cyber security." The Merriam-Webster defines cyber security as "measures taken to protect a computer or computer system against unauthorized access or attack."[14] From this definition, maritime cyber security could be defined as "cyber security measures adopted to protect or safeguard computer assets, networks on ports, terminals, ships, and computerized equipment which support maritime regular and classified operations." Since the

---

11 Kongsberg Group, "KONGSBERG Launches Kognifai," *Kongsberg Digital*, March 12, 2019, https://www.kongsberg.com/digital/resources/news-archive/2017/kongsberg-launches-kognifai/.

12 Sauli Eloranta, "Automated Maritime Transport: Why, How and When," accessed September 24, 2020, https://vayla.fi/documents/20485/421305/Sauli_Eloranta_180117+Rolls+Royce+v1.pdf/7fe4fb37-f501-4e78-a1fd-7513b02dcc02.

13 James M. Kaplan, Beyond Cybersecurity: Protecting Your Digital Business (Hoboken, NJ: Wiley, 2015).

14 "Cybersecurity," *Merriam-Webster*, accessed June 24, 2020, https://www.merriam-webster.com/dictionary/cybersecurity.

developments of IT infrastructure, computer networking and software systems in maritime industry, there are various cyber security challenges, which emerged in due course of time. Within the context of maritime industry and maritime infrastructure, cyber security may be taken as the safeguarding of electronic networks, communication systems, softwares control algorithms, users, unauthorized access, damage, manipulation, and underlying data within the maritime infrastructure from various cyberattacks.[15]

The cyber threats to the maritime industry are complex and researchers have identified various vulnerabilities with respect to the industry. The criminals are not only realizing the potential of the value of cargo, but they have already started trying 'blended attacks'; which can be launched on various occasions and from different locations in which cargo can be held as ransom. The known cyber vulnerabilities are likely to be targeted in near future attacks.[16] In past, non-traditional security threats like smuggling, piracy, and human trafficking were common risks and physical defense was all understood. On the contrary, cyber attack at ships is not well understood thus, less countermeasures were taken. Such maritime cyberattacks result in theft of information, business disruption and damage to the reputation, environment and goods etc.[17] The maritime industry is vulnerable to cyberattacks due to lack of encryption, standardized training, sheer cost of defending IT infrastructure, awareness of cyber security, and industry-wide smugness about cybersecurity. Most of the navigation systems, such as Automatic Identification System (AIS) and Global Positioning System (GPS) are neither authenticated nor encrypted, making it a soft target for malicious actors in cyber space. Merely spoofing or jamming of these two systems may cause collision of two ships leading to the closing down shipping channel for days or even weeks.

The Volume of Maritime Cybersecurity Industry

Maritime operations are increasingly relying on information and Communication Technology (ICT) to optimize its services due to its cost effectiveness. As there are various components used by different actors involved the supply chain process of maritime activities, these systems become vulnerable to cyberattacks. Some of the systems are used by general public, for instance the port community system to track and book

---

15 Alexis Garcia-Perez and et al., "Towards Cyber Security Readiness in the Maritime Industry."

16 Ibid.

17 Kimberly Tam and Jones D Kevin, "Maritime Cybersecurity Policy: The Scope and Impact of Evolving Technology on International Shipping," *Journal of Cyber Policy 3, no. 2* (2018): 147-164.

shipments.[18] On the other hand, a few components are used by port operators, such as Terminal Operating System (TOS) for controlling containers movement and storage on ports. Similarly, companies manage, link, and share internal processes with customers and suppliers through back-office management and integration system.[19] Cyber attackers take advantage of the complexity of this wide range of softwares. In the world of cyber space, remote access provides new opportunities to be used and misused by cyber attackers. The lack of reliable and non-standardized protocols of data sharing makes it possible for cyber criminals to intervene and manipulate the cyber space. Moreover, the absence of any cybersecurity strategy for maritime industry needs to be made as a matter of priority and urgency. Maritime industry is one of the most vulnerable critical infrastructures to malicious cyberattacks and other forms of cybercrimes. Maritime shipping accounts for 90-94 percent of global trade and any disruption to the sea lanes of communication, maritime chokepoints, and shipping companies would have cascading implications to the supply chain of global economy.[20] The economic impacts of cyberattacks on maritime industry including ports, ships, refineries, vessels, terminals, and support systems at harbor are estimated to be in hundred billion dollars.[21] Juniper recently issued a report that cybercrime will become the biggest challenge by the start of 2020 costing the maritime industry USD 2.1 trillion.[22] All sectors of maritime trade will be affected including ports, logistics, shipping, containers, in such an environment which will require a global action.

Cybersecurity Threat Environment

Cybersecurity threat environment is always evolving having various actors becoming smarter, developing their strategies to focus and target exploits in a systematic spearheaded fashion. With the passage of time, adversaries are becoming powerful enough to threaten the integrity, interest, lifestyle, and enhance their own agendas. Cyber threats are already challenging confidence in global organizations, public trust, governance, and norms imposing costs on the global economies.[23]

---

18 E. Heymann, B.P Miller, M. J. Alghazzawi, and D. Incertis, "Addressing the Cyber-Security Of Maritime Shipping,"*European Transport Conference*, https://aetransport.org/past-etc-papers/conference-papers-2016.

19 Ibid.

20 "International Maritime Organization," *United Nations Business*, accessed June 24, 2020, https://business.un.org/en/entities/13.

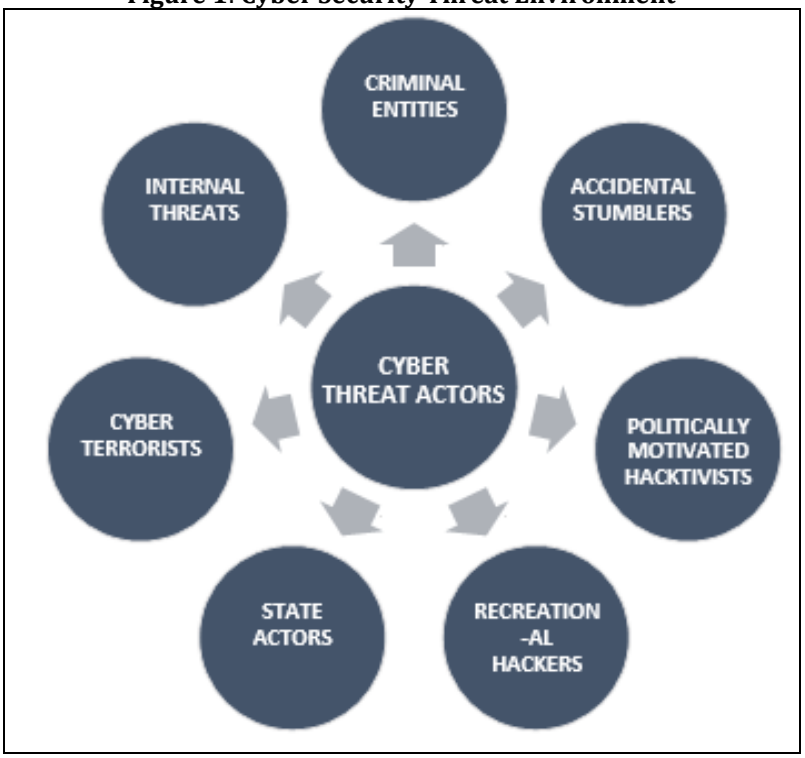
21 Chronis Kapalidis, "Cyber Security Challenges for the Maritime Industry," *Safety4sea*, September 12, 2019, https://safety4sea.com/cm-cyber-security-challenges-for-the-maritime-industry/.

22 Ibid.

23 Daniel R Coats. "Statement for the Record, Worldwide Threat Assessment of the US Intelligence Community, Senate Select Committee on Intelligence,

A malicious actor also called a threat actor, is an entity, which is wholly or partially responsible for the incident that has the potential to impact an organization's security.[24] These actors can damage critical systems by exploiting vulnerabilities in cyber system, compromise personal information, steal valuable intellectual property, conceal physical crimes or even collect business intelligence etc.

Figure 1: **Cyber Security Threat Environment**



Major categories of malicious cyber actors as shown in Figure 1 include:

Recreational hackers

These are the hackers who try to hack cyber systems just to impress their counterparts with a skilful exploit rather than making money.

Cyber Terrorists

Cyber terrorism is the combination of cyberspace and terrorism, which is generally understood as unlawful attacks or threats of attacks

Daniel R. Coats, Director of National Intelligence, May 11, 2017," In *United States. Office of the Director of National Intelligence*. United States. Office of the Director of National Intelligence, 2017.

[24] "Threat Actor," *TechTarget*. accessed August 26, 2020, https://whatis.techtarget.com/ definition/threat-actor.

through networks, computers, and the data stored therein. These attacks can be launched to coerce or intimidate the government or people in connection to social or political objectives. Cyber terrorists are the actors who use internet to achieve their goals, which results in threatening a life or damage an infrastructure through intimidation.[25]

Criminal Entities

There are individuals who perform malicious activities on networks or digital systems by the use of technology in maritime domain. These activities include importing drugs, counterfeit goods, and illegal chemical to get profits in the black market and stealing cargo.

State-Actors

State-Actors are tasked by the governments to steal sensitive information or disrupt other governments critical infrastructure by cyber means.

Accidental Stumblers

They are also known as 'Script Kiddies' who actually learn hacking from the online resources and end up penetrating into systems and disrupting sensitive operations unintentionally.

Politically Motivated "Hacktivists"

They are tech savvy organized groups who actually undertake cyberattacks against organizations and nations in order to achieve political and social causes.

The cyber threat environment is frequently shifting and complex, the fact is that there are various actors always keep on gaining access to or disrupting cyber systems for malicious purposes.

Internal Threats

There are cyber threats from service provider or an employee as well. Internal people can compromise the maritime system by the carelessness, negligence, human error or by ignorance. They may open up a malicious email, access malicious website, or use infected removable media. This unintentional act may expose classified or sensitive data to cyber threats thus putting the security of an organization at risk.[26]

---

[25] Jones, Deri, and N. T. A. Monitor. "Semantic attacks-a new wave of cyber-terrorism." *Network Security* 3 (2002): 13-5.

[26] "The Guidelines of Cyber Security Onboard Ships Version 3," Bimco, Clia, Ics, Intercargo, Intermanager, Intertanko, Iumi, Ocimf and World Shipping Council, https://www.ics-shipping.org/wp-content/uploads/2020/08/guidelines-on-cyber-security-onboard-ships-min.pdf.

Recent Cyberattacks and Incidents on Maritime Infrastructure

There are cyberattacks taking place in maritime industry which target bank records, access logistical software, penetrate into control systems and engines and hack navigation system of a ship. In the year 2017, a survey has shown the volume of cyberattacks on shipping companies to 69 percent.[27] The networks and systems used by shipping companies, vessels, flag states, and ports handle classified information, which catches the interest of criminals and can have an attractive target. Table 1 shows some recent cyber incidents and the nature of attacks on the maritime infrastructure.

Table 1: Cyber Attacks on Maritime Infrastructure (2011-2020)

a.	Cyber Attacks/ Incidents on Maritime Infrastructure	Nature of Attack	Country	Year
b.	The Islamic Republic of Iran Shipping Lines (IRISL) became the victim of cyber-attack	Iranian stevedores could not count containers, stored pier-side or placed on ships without manually verifying all twenty-foot equivalent units (TEUs).	Iran	2011
c.	Saudi Aramco Oil and Gas Operator	An employee mistakenly opened a phishing email which had an infected link.	Saudi Arabia	2012
d.	Ghost Shipping	Cyber experts to infiltrate computer networks which were responsible to manage what's inside each container at the port of Antwerp.	Belgium	2013
e.	Ice Fog	Advanced Persistent Threats (APTs) were launched on South Korean and Japanese assets.	South Korean and Japan	2013
f.	Vessel GPS	GPS was hacked of South Korean vessel, resultantly provided false information.	Korea	2016
g.	Cyber Attack on Maersk	Ransomware attacks were reported on Dutch	Maersk worldwide	2017

[27] David Silgado Miranda, "Cyberattacks: A Digital Threat Reality Affecting the Maritime Industry," *World Maritime University Dissertations,* April 4, 2018, https://commons.wmu.se/cgi/viewcontent.cgi?article=1662&context=all_dissertations.

		maritime shipping company.		
h.	Long Beach Terminal of Cosco	A ransomware attack was launched against Cosco Shipping at the port of Long Beach Terminal	USA	2018
i.	US Coast Guard Rescues a Shipping Vessel from Cyber Attack	A cyber attack was launched against a vessel bound to New York and Coast Guard rescued that.	USA	2019
j.	Global Logistics Operator Toll Group has been Subject to Cyber Attack	A ransomware attack was launched against global logistics operator Toll Group	Australia	2020

Source: Compiled by the author.

Cyberattacks on the Maritime Assets of the Islamic Republic of Iran – 2011

Shipping has been the major pillar of Iranian's economy to make it alive during the times of multilateral sanctions by the International community. In August 2011, an Iranian state-owned shipping organization named the Islamic Republic of Iran Shipping Lines (IRISL) became the victim of cyber-attack.[28] The founder of Cyber Keel, Lars Jenson stated, "the cyber attack almost damaged data related to cargo number, loading, date and place, and rates, which resulted in huge financial loss."[29] According to the IRISL, the general shipping information and cargo information was taken by the hackers. Resultantly, it became nearly impossible for Iranian stevedores to count those containers, which were stored pier-side or placed on ships without manually verifying all twenty-foot equivalent units (TEUs). Though there is no information on how long time it took to restore, but the loss to IRISL was considerable.

Cyberattack on Saudi Oil and Gas Company Aramco - 2012

The Saudi's largest oil and gas operator named ARAMCO was hit by a cyberattack. The company's employee mistakenly opened a phishing email which contained an infected link. This resulted in corruption of files, and disconnection of phone calls. Almost 35,000 computers were infected and 3 quarters of data was removed. On top of that, the oil company could

---

28 "Iran's Offshore Platforms Become Target of Recent Cyber Attacks," *The Maritime Executive*, October, 2012, https://www.maritime-executive.com/article/iran-s-offshore-platforms-become-target-of-recent-cyber-attacks

29 "Maritime Cyber-Risks Virtual Pirates at Large on the Cyber Seas," *CyberKeel*, October 15, 2014, Cophenhagen, Denmark, 6, https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf

not perform its regular functions for 17 days.[30] It took ARAMCO 5 months to recover from the loss and resume its day-to-day operations.

Ghost Shipping / Port of Antwerp – 2013

During the year 2011 and 2013, Drug traffickers in Dutch hired cyber experts to infiltrate computer networks, which were responsible to manage what's inside each container at the port of Antwerp. This way, they managed to hide cocaine in the containers and got them release to the destination without the knowledge of port authorities.[31]

Ice Fog – South Korean and Japanese Assets Incident – 2013

Kaspersky Labs, an Internet security company, released proofs of consistent cyberattacks of phishing on South Korean and Japanese assets in 2013.[32] The targeted institutions included military, telecom, media houses, government, and shipbuilding groups. The most lethal cyberattack is known as advanced persistent threats (APTs).

Vessels GPS in Korea – 2016

South Korean vessel suffered a cyberattack in April 2016 in which navigational system was jammed. The GPS was hacked by hackers; some signals were dead, and some others were providing false information. The GPS had not exhibited correct information, and eventually the ship was returned to the port. This can become a serious navigational fault, if it happens in poor weather condition, vessel traffic area or having inadequate visibility.[33]

Port Operations of A.P. Moller-Maersk - 2017

The Dutch maritime shipping company 'Maersk' was hit by cyberattack in 2017. This cyberattack was the one which raised serious cyber vulnerabilities of maritime industry. The company's loss was estimated to be around $300 million and they continued their operations

---

30 Jose Pagliery, "*The Inside Story of the Biggest Hack in History*," *CNN Money*, August 5, 2015, https://money.cnn.com/2015/08/05/technology/aramco-hack/

31 Joseph Direnzo, Dana A. Goward, and Fred S. Roberts, "*The Little-Known Challenge of Maritime Cyber Security*," *6th International Conference on Information, Intelligence, Systems and Applications (IISA*), 2015, https://doi.org/10.1109/iisa.2015.7388071.

32 "The 'Icefog' Apt: A Tale Of Cloak And Three Daggers," *Kaspersky Media,* https://media.kaspersky.com/en/icefog-apt-threat.pdf, last accessed June 25, 2020.

33 "Cyber Security Fleet Protection Digital Ship Singapore March 2018," *OSM Maritime Group,* 2018, https://static1.squarespace.com/static/57a8878837c58153c1897c2c/t/5ab3b85f88251b5549a07357/1521727638547/8PeterSchellenberger_OSM_APM18.pdf

without IT for many days till the resume of operational activities.[34] Maersk had to close down its activities from several ports across the globe reducing the volume by 25 percent. In order to resume its services, the organization had replaced its 45000 computers, 4,000 servers and installed 2500 new applications.

Long Beach Terminal of Cosco - 2018

In July 2018, Cosco Long Beach Terminal, which was associated with Cosco Shipping was affected by a ransomware cyberattack. Though, the cyberattack could not harm the company's daily operations, but the company decided to close down its connections with external regions. Later, the company sent letter to every client in order to clarify the incident.[35]

US Coast Guard Rescues a Shipping Vessel from Cyber Attack - 2019

In February 2019, the US Coast Guard received a message from a large ship bound for New York that the vessel was facing an alarming cyberattack impacting their shipboard network." An incident response team led by the Coast Guard investigated the matter and found that ship system was affected by the malware and it has significantly degraded the functionality of the vessel. Fortunately, the imperative systems for the control of vessel remained unimpeded.[36]

Global Logistics Operator Toll Group had been Subject to a Cyber Attack - 2020

Global logistics operator Toll Group has reported to be under cyberattack across its sea and land operations on 03 February 2020. The company had closed down its number of systems at various sites in order to respond the attack. As a consequence, majority of the customers were experiencing disruption or delays while the company was trying to resume its operations. The attack later on was identified as Mailto ransomware or

---

34 Jonathan Saul, "Global Shipping Feels Fallout from Maersk Cyber Attack," *Reuters*, June 29, 2017, https://www.reuters.com/article/us-cyber-attack-maersk-idUSKBN19K2LE

35 Michael Juliano, "Cosco's Long Beach Terminal Hit by Cyber-attack," *Tradewinds - Global Shipping News*, July 25, 2018. https://www.tradewindsnews.com/casualties/1541843/coscos-long-beach-terminal-hit-by-cyber-attack

36 James Rundle, "U.S. Coast Guard Warns Shipping Industry on Cybersecurity," *The Wall Street Journal*, July 11, 2019, https://www.wsj.com/articles/u-s-coast-guard-warns-shipping-industry-on-cybersecurity-11562837402.

Netwalker, which is a new malware first time reported in October 2019.[37]

The above-mentioned incidents were just few examples of cyberattacks occurred in the maritime industry. However, there are many more cyber incidents, which don't get reported due to the fear of loss of reputation. Interestingly, maritime industry was shaken by the cyberattack on Maersk shipping lines in 2017 and indeed it was the time when maritime sector has started realization that cyber threats are real and they can create serious damages to the industry.

Cyber Threats to Maritime Industry during COVID-19

Since the outbreak of the covid-19, the global maritime transport industry is performing a significant role in the smooth dissemination and relay of goods across the globe. According to United Nations Conference on Trade and Development (UNCTAD) statistics, around 80 percent of the global trade is sent by commercial ships that moves the world's energy, food, and raw materials along with all manufactured components and goods.[38] It also includes medical supplies, which are in demand worldwide and without which the prevailing situation cannot be controlled. In this context, the maritime industry, call to the government for keeping maritime trade moving by allowing commercial ships to ports globally and changing crew of ships worldwide is a significant aspect, which cannot be ruled out. In the global crisis, it is imperative to keep supply chain consistent and to allow maritime trade and trans-border transport to continue.[39] Another important aspect is the provision of food to landlocked countries, which need unhindered access to food and medical supplies through neighbouring state's seaports. Restrictions on trade may interrupt and disrupt businesses and can have negative ramifications on global economy. The recent virtual G20 Leaders Summit on the COVID-19, the state leaders should give heed to the maritime industry call to keep maritime trade moving. The backlash to global economy is yet to be ascertained, as the pandemic is called 'black swan' due to the magnified impact it brings to the businesses worldwide and halting the supply chain industry.[40]

---

37 Zoe Reynolds, "Toll Group Shuts Down IT Systems after Cyber Attack," *SafetyatSea*, February 6, 2020, https://safetyatsea.net/news/2020/toll-group-shuts-down-it-systems-after-cyber-attack/

38 Mukhisa Kituyi, "Coronavirus: Let's Keep Ships Moving, Ports Open and Cross-Border Trade Flowing," *United Nations Conference on Trade and Development* (*UNCTAD)*, March 25, 2020, https://unctad.org/news/coronavirus-lets-keep-ships-moving-ports-open-and-cross-border-trade-flowing

39 Ibid.

40 Benjamin Hilliburton, "COVID-19 is a Black Swan," *Forbes*, March 19, 2020,https://www.forbes.com/sites/forbesbooksauthors/2020/03/19/covid-19-is-a-black-swan/#211c1ea67b4b.

In this scenario, any cyberattack leading to the short term suspension or long term disruption to any operational technological activity will have a devastating impact on the maritime industry. According to a survey conducted by the Business Performance Innovation (BPI Network) in partnership with Navis stated that global maritime industry is seriously concerned about the cyber security.[41] Same concern is being observed during the pandemic, as cyber hackers have started targeting maritime industry, as reported by the cyber consultants worldwide. There are ships, which are receiving malicious emails targeting maritime sector with phishing links or malwares in order to compromise the vessel or parent organization. The maritime organizations have come under sophisticated cyberattacks where charity and International Seafarers' welfare networks are becoming the targets by cyber hackers. An email with the title 'Corona virus / Affected Vessel to Avoid' and contains list of vessels with infected crew was circulated amongst maritime industry amidst the Corona-virus.[42] There is another email promising to reveal names of infected crew members onboard specific vessels lured its readers to fill the form attached and send them back. Another incident reported about a malicious email impersonating World Health Organisation (WHO) Project Manager which was found suspicious as the language was full of grammatical errors, phrasing issues, and capitalization errors throughout.[43] The Corona virus being the only topic today evoke emotional response causing the recipient to open the spoofed message without getting cautious. Taking the lead from this, building a scenario with sophisticated and well-planned cyberattacks on maritime industry, cyber criminals can leverage the global crisis and demand million dollars as a ransom.

Cyber Security Counter Measures in Maritime Industry

In last few years, the maritime industry has taken important steps regarding devising recommendations and guidelines to address the cybersecurity threats. However, with continued call for advanced technological equipment and systems used in day-to-day shipping

---

41 "Shipping Industry Optimistic But Concerned About Trade, Cyber Threats," *Material Handling & Logistics,* November 19, 2018, https://www.mhlnews.com/transportation-distribution/article/22055334/shipping-industry-optimistic-but-concerned-about-trade-cyber-threats.

42 Sam Chambers, "Weekly Report Details Growing Number of Shipping Companies Targeted by Malware Attacks," *Splash Tech*, March 25, 2020, https://splash247.com/weekly-report-details-growing-number-of-shipping-companies-targeted-by-malware-attacks/

43 Ibid.

activities, a dire need is required for government and industry to develop and implement strong and robust security measures, which can provide risk-based prevention, mitigation and recovery stages in cybersecurity field. In this regard, a multifaced approach would consist of cybersecurity assessment, cybersecurity enhancement, penetration testing, verification of any new builds (software or hardware), assessment of onboard vessel's cybersecurity, ISO/IEC 27001 Maritime training and compliance along with profiled training of all personnel. By the time, operational technology (OT) and information technology (IT) have been coupled together, the frequency to internet has been increased as well. It further brings greater cyber risks to ships not only from unauthorized access or malicious attacks but also from personnel accessing systems onboard ships. In 2017, the International Maritime Organization (IMO) initiated and adopted resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management System (SMS). According to the resolution, cyber risk management should be taken into consideration an approved SMS with the functional requirements and objectives of the ISM code. The administrators are also encouraged to address cyber risks in SMS not later than the first annual verification of the company's Document of Compliance after January 1, 2021.[44] The resolution discusses various company-ship specific approaches of cyber risk management but it is regulated under relevant national, international and flag state regulations.

The same year, IMO also came up with guidelines providing recommendations on cyber risks management to ensure ships are safe from emerging cyber risks and vulnerabilities. As per guidelines, senior management is responsible for the implementation of cyber risk management, as they should harbor the cyber culture into all levels and departments of any organization.

Like the IMO guidelines, the US National Institute of Standards & Technology (NIST) made a Cybersecurity Framework (CSF), which provides instruction to find out and sort out cyber related threats for the systems and applications.[45] The prioritized, flexible, and cost-effective framework approach serves as the solid guidelines for organizations to handle cyber issues while safeguarding civil liberties, business and individual practices confidentially.

In 2019, on the basis of senior management commitment to ensure cyber risk management, the Guidelines on Cyber Security Onboard Ships

---

44 "The Guidelines of Cyber Security Onboard Ship," *BIMCO Bulletin*, December 2020, https://www.bimco.org/about-us-and-our-members/publications/bimco-bulletin.

45 "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," *National Institute of Standards and Technology*, February 12, 2014, http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

have been formulated by the BIMCO in consultation with CLIA, ICS, INTERCARGO, Inter Manager, INTERTANKO, IUMI, OCIMF and WSC. These guidelines are aligned with IMO resolution and guidelines and offer various new recommendations on maritime cyber safety and cyber security.[46] This document aimed at providing guidance to ship owners and operators on actions and procedures to maintain the cyber security of cyber systems in the organization and onboard ships.

These guidelines are third edition in the last many years thus reflecting the dynamic nature of cyber risks and challenging to the maritime sector. The difference between previous guidelines and new one lies in multiple domains, such as operational technology and supply chain risks. The cyber risk associated with ships are directly linked with information technology and operational technology. For instance, malfunctioning IT system may cause a delay in clearance or ships' loading but inoperative OT can cause real risk to the ship, people or the marine environment. Most often, the jobs at ship may be focused on protecting operational systems as compared to protecting data. If a software controlling engine is hit by a cyberattack with malware, it can lead to disastrous situations.[47]

Another aspect has been covered in the guidelines was the number of cyber incidents to demonstrate the real-world situations, faced by operators and ship owners, though the examples have been anonymized.

The supply chain risks were also highlighted in the guidelines highlighting the risks associated with malware infecting the systems of ship through external parties linked with ships and their systems. For example, ships are not just standing in the middle of ocean, it has to have close connections to security systems in the shippers', companies' and agents' offices, which make it more vulnerable in the cyber domain.

The maritime industry is to join hands with governments across the globe and take serious and specified measures to mitigate cyber threats especially in the midst of any natural disaster or pandemic. There is a dire need to train crew members of all levels to understand and realize the existence of cyber-attacks. They should be given adequate practical guidance on how to look for potential malware or phishing attempt. The maritime industry should also use direct communication in order to verify emails from the original originator.

---

46 Aron Soerensen, "Safety at Sea and BIMCO publish Cyber Security," *BIMCO Bulletin*, September 19, 2019, https://www.bimco.org/news/priority-news/20190916-safety-at-sea-and-bimco-publish-cyber-security-white-paper

47 Rasmus N Jorgensen, "Industry Publishes Improved Cyber Guidelines," *BIMCO Bulletin*, December 7, 2018, https://www.bimco.org/news/priority-news/20181207-industry-publishes-improved-cyber-guidelines.

Conclusion

In this digital age of maritime industry, information, and communication technologies play an important role through increased connectivity of networks and systems. The industry has been transformed from traditional concepts into new technologies having advanced and sophisticated systems. The modern shipping industry now facilitates routine operations, but it also becomes vulnerable to different type of cyberattacks. Organizations actually invest in cyber technology and systems but not on the training of staff. Given this, most cyber-attack incidents are associated with the human factor making the state of affairs completely paradoxical. Either we take the example of 2011 Stuxnet in Iran or Saudi Aramco cyberattack in 2012, human error and incompetency prevail in these major cyber security attacks. This scenario is mostly prevalent in developing countries or LDCs where highest cyber commitment is still lacking behind; resultantly they fall to various malicious viruses leading to cyberattacks.

Since, the maritime sector is evolving; the demonstration of new technologies makes it significant to work for a longer-term cybersecurity framework and plans. This requirement is also reflected in the IMO and United Nations' agenda in order to achieve the sustainable development goals. Since cybersecurity has emerged as a strong threat to the maritime industry, it has become mandatory for all stakeholders to collaborate and participate to address this global threat. The participation of all maritime sectors is also important to contribute in creating optimal operational conditions, implementing national regulations, enforcing and contributing to the prosperity and stability of maritime industry. This will not only help in ensuring the maritime sector plays its role, but also better develop future working conditions for new generations. For the same reason, it becomes inevitable that vessels, shipping companies, ports and harbor facilities and regulatory organizations keep working on the enhancement of cybersecurity measures in order to protect critical infrastructure and key resources from cyber threats. Though the maritime industry is becoming aware of cyber incidents and adapting cyber risks mitigation trainings, however, there is strong need not to let go of multiple unnoticed and unregulated cyber incidents.