International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0029

e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 167-172

Maritime Cybersecurity

Dr. S. Gopinath[1], Mr. M. Hemanand[2], Mr. P. Arunprasath[3], Mr. M. Vivek[4], Mr. P. Balaji[5], S.S. Leena Charan[6]

[1] Professor, Department of Marine Engineering, Coimbatore Marine College, Coimbatore, Tamil Nadu, India.

[2,3,4,5]Assistant Professor, Department of Marine Engineering, Coimbatore Marine College, Coimbatore, Tamil Nadu, India.

[6]UG Scholar, Department of Marine Engineering, Coimbatore Marine College, Coimbatore, Tamil Nadu, India.

Emails: *sgopy.suresh@gmail.com[1], hem_mariner@yahoo.in[2], me.arunprasath@gmail.com[3], viveksss2020@gmail.com[4], balaji.pacet@gmail.com[5], leenacharan2004@gmail.com[6]*

Abstract

As the maritime industry continues to digitalize in pursuit of efficiency and connectivity, it increasingly opens itself up to growing cyber threats, which may very seriously hamper operations, cause huge financial losses, or even result in environmental disasters. Specifically, this paper investigates the important aspects of maritime cybersecurity about protecting infrastructure from cyber threats. The paper points to the weaknesses brought about by the integration of IT and OT systems in the maritime sector, illustrated with high-profile incidents like the NotPetya attack on Maersk and the cyber breach at the Port of Antwerp, and calls for the establishment of sound cybersecurity frameworks in maritime operations. Advanced threat detection systems, network segmentation, data encryption, and human factors all play key roles in mitigating such risks. The paper concludes by calling for industry-wide collaboration in implementing good practices to ensure that global supply chains and the wider economy are safe and secure from the threat of cyber-attacks.

Keywords: *Maritime cybersecurity; NotPetya attack; Threat detection systems; Cyber-attacks.*

1. Introduction

On efficiency and connectivity, the industry has really moved toward digitalization; it has placed itself firmly at the very core of worldwide trade. This shift toward the digital future, however, has dramatically increased the cyber threat against maritime operations. The interlinking of IT and OT systems exposed vulnerabilities within these synergies that cybercriminals could identify very fast. Such breaches can have devastating consequences in terms of operational disruption, financial losses, and environmental disasters. [2] This paper presents the critical dimensions of maritime cybersecurity related to protecting the infrastructure from cyber threats. It reviews some key case studies on cyber-attacks, assesses vulnerabilities in maritime systems, and discusses the development of robust cybersecurity frameworks for securing operations.

2. Case Studies of Cyber-Attacks Within the Maritime Industry

In view of the high publicity accrued to some of the cyber-attacks that have targeted the maritime industry, associated case studies underline potential impact and reiterate the need for robust measures against cyber threats.

2.1 Maersk and the Not-Petya Attack

In 2017, Maersk, a giant in the global shipping industry, was hit by one of the most devastating cyber-attacks in maritime history when NotPetya ransomware struck. Believed to be state sponsored, the chain of attacks had a very devastating impact on

Maersk. The firm underwent a colossal IT recovery effort and reinstalled 4,000 servers, 45,000 computers, and 2,500 applications as a means of recovery to take control of their systems. During that time, Maersk could not process any order which led to enormous delays with estimated financial losses to the tune of about 300 million dollars as shown in the figure 1. This incident was a wake-up call; it showed that maritime companies were exposed to global cyber threats, and inadequate cybersecurity could lead to disastrous consequences. [3, 4]

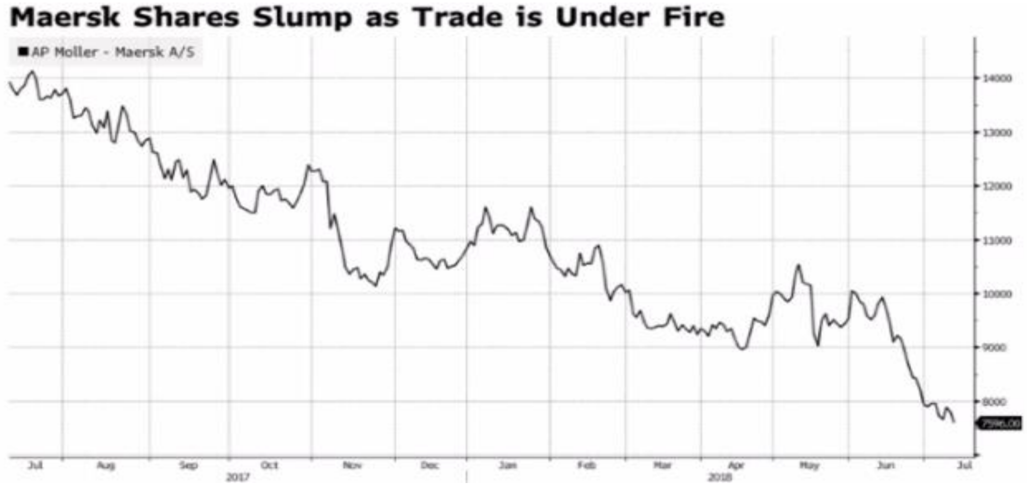


Figure 1 **Effect of Cyber-Attacks on Maersk Shares**

Source: https://www.slideshare.net/slideshow/maersk-notpetya-crisis-response-case-study/155864831#18

That is an interesting fact: Maersk was not the intended victim. The malware NotPetya was just one part of a larger cyber campaign orchestrated by a Russian hacker group called Sandworm that had broken into the Ukrainian government and many businesses. The point of entry was this small, local software company, Linkos Group, which developed software, including M.E. Doc, for use in accounting, but it became ubiquitous across Ukraine. In the beginning of the year 2017, Sandworm leveraged M.E. Doc's updating servers, thereby handing direct access towards thousands of computers using the software over to themselves. The breach that felled Maersk began in Ukraine in the port city of Odessa with just one infected computer. That singular infection was enough to spread the ransomware through Maersk's entire worldwide network, resulting in port operations being locked down entirely, with tens of thousands of truckloads refused as the company, in essence, ground to a halt.

2.2 Port of San Diego, 2018

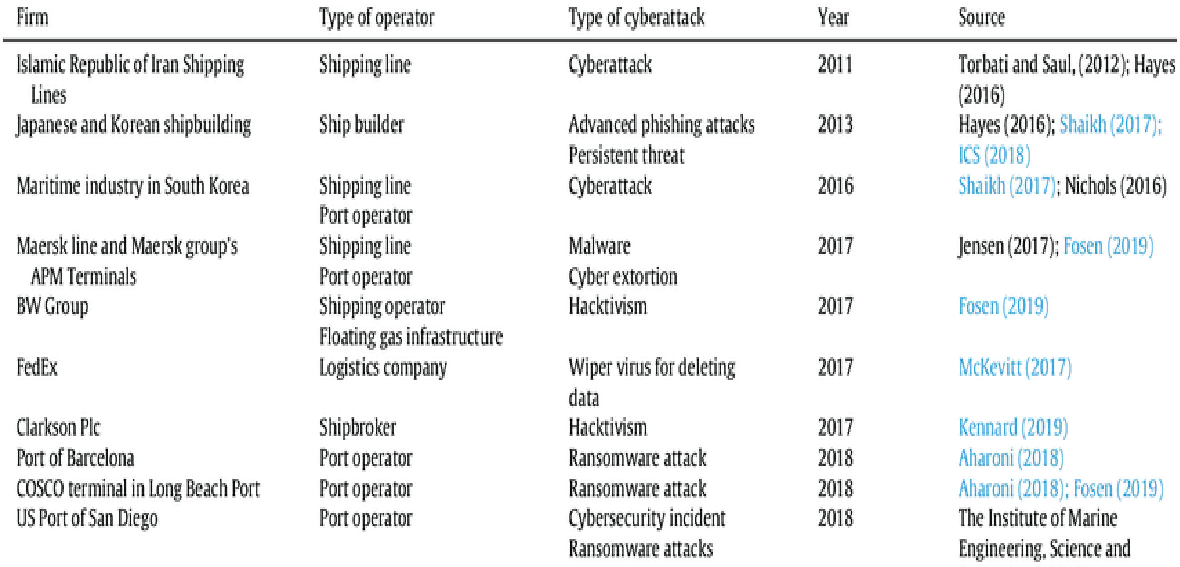
In September 2018, the Port of San Diego was hit by a ransomware attack that put its IT systems in very bad shape. Although this attack did not shut down the complete functioning of the port, it brought highly impactful delays to key administrative functions, including public safety systems so vital to the running of the port. It had to fall back on manual procedures for some days, which, of course, led to inefficiencies and slowdowns of operations. The incident proved how vulnerable port infrastructure can be to cyber-attacks and how easily such disruptions bring the activities of the port to a grinding halt. [5]

2.3 COSCO Shipping Lines, 2018

In July 2018, one of the largest logistics companies in the world, COSCO Shipping Lines, was hit by a cyber-attack that hit at the very core of its operating systems across the Americas. It shut down parts of its email and IT services to contain the malware that had led to communication breakdowns and delays in cargo handling as shown in the figure 2. Despite the mayhem, COSCO managed to keep itself going by falling back on manual processes. The incident itself drove home the lesson of putting in place strong business continuity plans in case of a cyberattack. [6]

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0029

e ISSN: 2584-2854
Volume: 03
Issue:02 February 2025
Page No: 167-172



Firm	Type of operator	Type of cyberattack	Year	Source
Islamic Republic of Iran Shipping Lines	Shipping line	Cyberattack	2011	Torbati and Saul, (2012); Hayes (2016)
Japanese and Korean shipbuilding	Ship builder	Advanced phishing attacks Persistent threat	2013	Hayes (2016); Shaikh (2017); ICS (2018)
Maritime industry in South Korea	Shipping line Port operator	Cyberattack	2016	Shaikh (2017); Nichols (2016)
Maersk line and Maersk group's APM Terminals	Shipping line Port operator	Malware Cyber extortion	2017	Jensen (2017); Fosen (2019)
BW Group	Shipping operator Floating gas infrastructure	Hacktivism	2017	Fosen (2019)
FedEx	Logistics company	Wiper virus for deleting data	2017	McKevitt (2017)
Clarkson Plc	Shipbroker	Hacktivism	2017	Kennard (2019)
Port of Barcelona	Port operator	Ransomware attack	2018	Aharoni (2018)
COSCO terminal in Long Beach Port	Port operator	Ransomware attack	2018	Aharoni (2018); Fosen (2019)
US Port of San Diego	Port operator	Cybersecurity incident Ransomware attacks	2018	The Institute of Marine Engineering, Science and

Figure 2. Effect of Cyber-Attacks on Cosmo Shipping Line
Source: https://www.researchgate.net/figure/Cyberattacks-in-maritime-transportindustry_tbl1_342167733

2.4 Port of Antwerp Drug Smuggling, 2013

In 2013, the Port of Antwerp was the scene of a cyber-attack that revealed how some hackers are still fueled by criminal motives beyond demands for ransom. Hackers attacked the port's systems using spear-phishing and malware attacks against port authority staff and shipping companies. They infiltrated the systems to preprogram the movement of containers to conceal drug shipments, after which smugglers would collect the respective containers before the arrival of legitimate haulers. [1]

3. A Critical Vulnerability: Dynamic Positioning Vessels

Dynamic Positioning Systems are state-of-the-art computerized systems that keep a vessel on its position and heading automatically using propellers and thrusters as shown in the figure 3. Such systems bring great benefits during operations, but they also pose a cyber security threat due to the requirements for interconnected digital networks and complex computerized components. Such interconnectivity creates numerous potential entry points for hackers.

Figure 3 Dynamic Positioning Systems
Source: https://www.abs-group.com/Knowledge-Center/Insights/Hacking-the-Ship-Scenario-An-Offshore-Supply-Vessels-Dynamic-Positioning-System/

A cyber incident on a DP system could be due to the loss of communication between the operator control stations and the sensors and actuators that control vessel movement. For instance, this could be initiated by a disgruntled administrator who plugs an unscanned USB device with a virus, such as a botnet, into the DP system to do an update using specialized software. Once the botnet is inside, it can infect all the systems connected to the network within a very short time, and each of the infected workstations becomes a "zombie workstation." Once the botnet activates and there are DP operations currently underway on board the vessel, it can unexpectedly engage the thrusters through the control unit, manipulate rudders, or surge the engines in such a way that the vessel moves suddenly without control. This results in the loss of equipment, lives in danger, and is bound to spark off environmental disasters. [11]

4. Protecting Maritime Infra Structure from Cyber Threats: Building Resilient Cyber Security Frame Works

The study above clearly indicates that cybersecurity is highly relevant to maritime infrastructure, especially with the growing reliance by the industry on sophisticated technologies. Digital systems being at the core of everything from navigation to cargo handling these days, new vulnerabilities have emerged that set the scene for the protection of maritime infrastructure. The growing cyber threats to the maritime sector put a demand for urgent development and effective implementation of appropriate cybersecurity frameworks exclusively in the maritime domain, able to provide broad coverage of both information technology and operational technology systems for a full security environment of all aspects related to maritime activities.

5. Threat Detection and Response Systems

In contemporary maritime operations, threat detection and response systems are the mainstream of effective cyber threat identification and neutralization in real time. In this view, technologies like Intrusion Detection Systems, Intrusion Prevention Systems, and Security Information and Event Management tools are very vital. These are tools that 'watch over' the network traffic and security events, filtering out suspicious activities for response before major damages are caused. This means segregating and isolating critical systems from less secure networks to minimize the effect of potential cyber-attacks. For instance, OT networks responsible for controlling vessels and physical processes in the ports need to be separated from IT networks used in administrative functions. This would thereby complicate the possibilities for lateral movement within a network to gain access to important systems by attackers. Enhancing and improving data encryption is quite necessary to protect sensitive information that may be transmitted through these networks. Even if cybercriminals intercept the data and it is encrypted, they will not be able to easily decrypt it or make any other use of that information. To this end, implement secure protocols for communication, such as SSL/TLS, in every case of remote access or data transfer. [7, 8, 9]

6. Human Factor and Manual Control

As said by Pen Test Partners “A Ponemon data breach report in 2017 showed that it took US organization’s an average of 206 days to detect a data breach. That’s a statistic from shore-based organizations, where IT and IT security personnel and expertise are usually available. So how does a ship’s crew, where perhaps one person on the crew has a small amount of basic IT skill, detect a breach of a vessel? If you don’t know, you can’t act. At what point do you decide that the navigation systems are no longer trustworthy? Who makes that decision? The inexperienced third officer? Do they wake the captain? Who decides to take the vessel out of track control mode? Remember, security isn’t binary – something is a bit odd, but all the digital systems seem to agree with each other.”, it is evident that the human factor in responding to a cyberattack is by far the greatest vulnerability that hackers can exploit. “Imagine a junior officer having to cope with failing navigation systems, all bridge sensors offline, steering gear not responding, and engine levers inoperative. Manual control is an option, but I know only too well, as a pilot, how quickly one can be overloaded by information and become incapable of dealing with a situation. Fixation on a single error rapidly brings loss of the wider picture.” [10] “An offset being injected into an ECDIS by Pen Test Partners as shown in the figure 4. Note the vessel has moved from one side of a breakwater to the other.” In the end, the training of crew members and building a system to detect these cyberattacks is the most important step in protecting cyberthreats in the maritime industry. [Pen Test Partners: “Ships can’t be hacked. Wrong”].

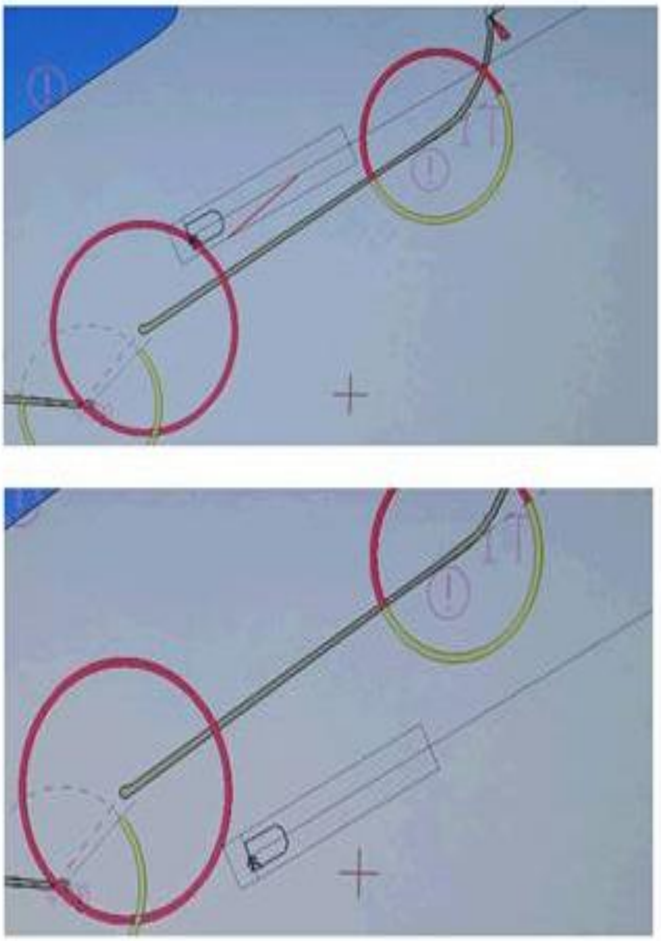


Figure 4 Human Factor and Manual Control
Source: https://www.pentestpartners.com/security-blog/ships-cant-be-hacked-wrong/

Conclusion

Cybersecurity is a growing concern with the increase in the use of digital technology in the maritime industry. Cyber-attacks are disruptive and can facilitate crime. Such vulnerabilities in the system of shipping, for example, in Dynamic Positioning and satellite communication terminals, raise an urgent need for custom-tailored cybersecurity frameworks. A fully feasible way to tackle this fast-growing cyber threat is through adoption of best practices, frequent risk assessments, and cross-industry stakeholder engagement. It is not just about the secure operation of ships and ports; when it comes to maritime infrastructure, it provides security for supply chains globally and the world's economy at large.

References

[1]. CNBC Hackers can bring ships and planes to a grinding halt. And it could become much more common. (https:// www. cnbc. Com/ 2022/06/27/ hackers-can-now-bring-cargo-ships-and-planes-to-a-grinding-halt.html)
[2]. International Maritime Organization (IMO): Guidelines on Maritime Cyber Risk Management.(https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx)
[3]. The New York Times, "The Untold Story of NotPetya, the Most Devastating Cyberattack in-History” (https: // www. nytimes. com/ 2018/08/22/magazine/ notpetya cyberattack ukraine russia-code.html)
[4]. Wired, "Inside the Cyberattack That Shocked the US, " (https:/ /www. wired.com /story/ notpetya cyber-attack-ukraine-russia-code-crashed-the-world/)
[5]. Port of San Diego Press Release, "Port of San Diego Responding to Cybersecurity Incident,". (https: //www. portofsandiego. org/press releases/general-press-releases/port-san-diego responding cybersecurity-incident)
[6]. Maritime Executive, "COSCO Shipping Hit by Cyber Attack, "(https://www.maritimeexecutive.com/article/cosco-shipping-hit-by-cyber-attack)
[7]. National Institute of Standards and Technology (NIST): Cyber security Framework.(https://www.nist.gov/cyberframework)
[8]. European Union Agency for Cybersecurity (ENISA): Port Cybersecurity - Good practices for cybersecurity in the maritime sector. (https:// www. enisa.europa.eu/ publications/ port-cybersecurity-good-

practices-for-cybersecurity-in-the-maritime-sector)

[9]. Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC). (https://www.mtsisac.org/)

[10]. Pen Test Partners: “Ships can’t be hacked. Wrong”. (https://www.pentestpartners.com/ security-blog/ ships-can’t-be-hacked-wrong/)

[11]. ABS Group: Hacking the Ship Scenario: An Offshore Supply Vessel's Dynamic Positioning System. (https:// www.abs-group.com/ Knowledge-Centre/ Insights/ Hacking- the- Ship- Scenario -An-Offshore Supply- Vessels- Dynamic- Positioning-System/)