Global Journal of Science Frontier Research: E
Marine Science
Volume 23 Issue 1 Version 1.0 Year 2023
Type: Double Blind Peer Reviewed Interenational Research Journal
Publisher: Global Journals
Online ISSN: 2249-4626 & Print ISSN: 0975-5896

Cyber Security of the Maritime ICTs, Threat Vectors and Implications on Global Sea Lanes of Commerce (SLOC)

By Md Ziaul Haque

Synopsis- This paper examines the cyber security aspect of the Maritime Transportation System (MTS) to understand the scope of the MTS, the different ways in which a hacker can infiltrate the computer systems of maritime, logistics, and port infrastructures, and the potential consequences and financial impact of a marine cyber disaster on businesses, states, and individuals.

Glossaries: *CISA (cybersecurity and infrastructure security agency), AI (artificial intelligence).*

GJSFR-E Classification: *DDC Code: 823.912 LCC Code: PR5774*

Strictly as per the compliance and regulations of:

Cyber Security of the Maritime ICTs, Threat Vectors and Implications on Global Sea Lanes of Commerce (SLOC)

Md Ziaul Haque

Synopsis- **This paper examines the cyber security aspect of the Maritime Transportation System (MTS) to understand the scope of the MTS, the different ways in which a hacker can infiltrate the computer systems of maritime, logistics, and port infrastructures, and the potential consequences and financial impact of a marine cyber disaster on businesses, states, and individuals.**

Glossaries: CISA (cybersecurity and infrastructure security agency), AI (artificial intelligence).

I. Introduction

Cybersecurity refers to the protection of information, computer systems, and networks from unauthorized access or attacks. The threat level of cyber-attacks on the Maritime Transportation System (MTS) has increased by 400% in recent months. The CISA identifies 16 essential infrastructures critical to national economic security which can be physical or virtual assets, systems, networks, or assets. Maintaining cyber security in the MTS is crucial for the functioning of the Sea Lanes of Commerce (SLOC) and supply chain resilience. Cybersecurity is the responsibility of regulatory authorities and all other stakeholders, as the MTS is dependent on every supply chain. This study aims to inform the maritime audience about the threat vectors in the upcoming Artificial Intelligence (AI) era, highlighting the various components of cyber security. This article uses experimental methodology on how data/instruction is passed from LBCC LAN to SBCC LAN to conceptualize the cyber essentials using conventional equipment, protocols, and configurations. The ship's LAN is created.

II. Maritime Transportation System (MTS) Model

The US maritime transportation system (MTS) encompasses approximately 95,000 miles of coastline, 25,000 kilometres of waterways and 361 ports. It is a complex system of interconnected physical and modern ICT networks that must be considered to address cyber security challenges. Governments, regulators, maritime stakeholders, and commercial organizations must work together to understand and address the underlying networks within the MTS. (CISA, 2020).

The maritime transportation system (MTS) consists of six interconnected subsystems that are connected by Information Communication Systems (ICTs) and physical connections. It is essential to understand and conceptualize these networks to effectively address cyber security challenges within the MTS.

(CISA, 2020), (Atlantic Council,2023)

Figure 1: Maritime Transportation System (MTS)

Author: MICS I M.SC. I B.SC. I COC (MCA) I AQP(CITB) I PQES (ICS). Director, AACL. e-mail: ziaul.haque@hotmail.co.uk

III. Comparative Contemplation of Bridge Models

Ancient Model of a Bridge of a ship	Latest Model of a Bridge of a ship
	

Figure 2: Ancient Vs Latest Bridge Model (Loomis et al., 2021, pp.1–50)

The key difference between ancient and the latest models is the presence of ICTs. The latter consists of networks of satellites, computers, routers, and servers in the latter. The figure illustrates the underlying network, with LBCC connected to SBCC in the latest Model.

IV. Ship's Information & Communication Technology (ICT)

a) Systems

These systems are central in the Worldwide Area Network (WWAN) and play a significant role in cyber security literature. If supply chain disruptions were to occur, the monetary value could reach trillions of dollars within a matter of hours.

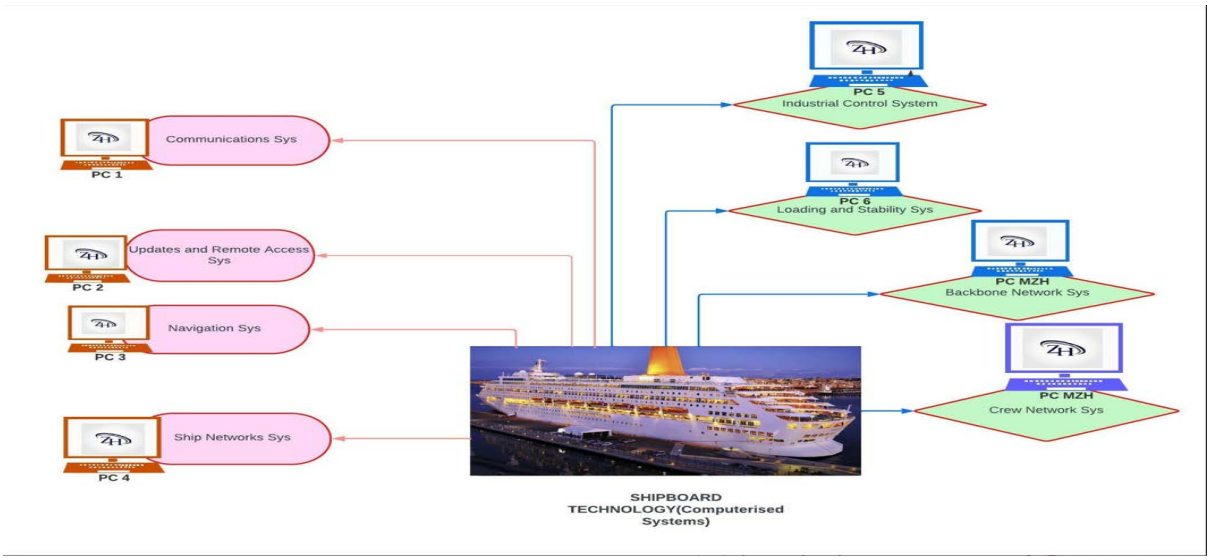
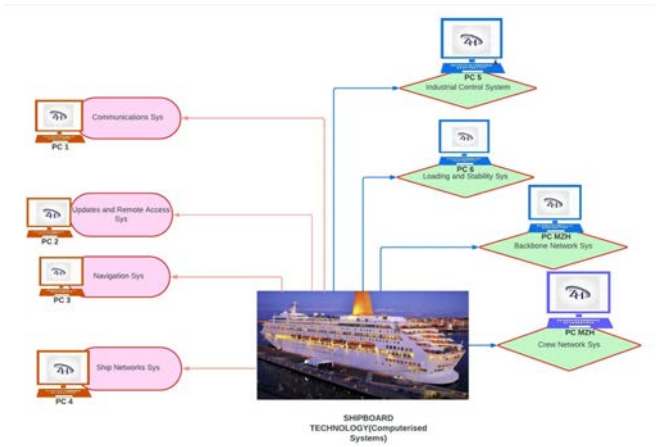


Figure 3: Ships' Core ICT Systems (Loomis et al., 2021, pp.1–50)

Therefore, ensuring the security and reliability of these ICT systems in the maritime transportation system is essential.



(Loomis et al., 2021, pp.1–50)

For example:
Navigation uses charts, ECDIS, GNSS Radar, and Weather.

Communications:
AIS, GSM, Satellite Link, ship-to-shore, VoIP and so on.
All these devices are programmed and connected to the satellite and the computer networks with a worldwide range by the internet.

Figure 4: ICT Equipment

V. Ship's Network LAN (Local Area Network)

The diagram illustrates a typical ship network connected to a shore satellite that is invisible to human eyesight. The network has some components connected in series and others in parallel and is interdependent and interconnected. The network topology is a star topology, which is scalable and can easily be extended, or new ICT systems can be included.

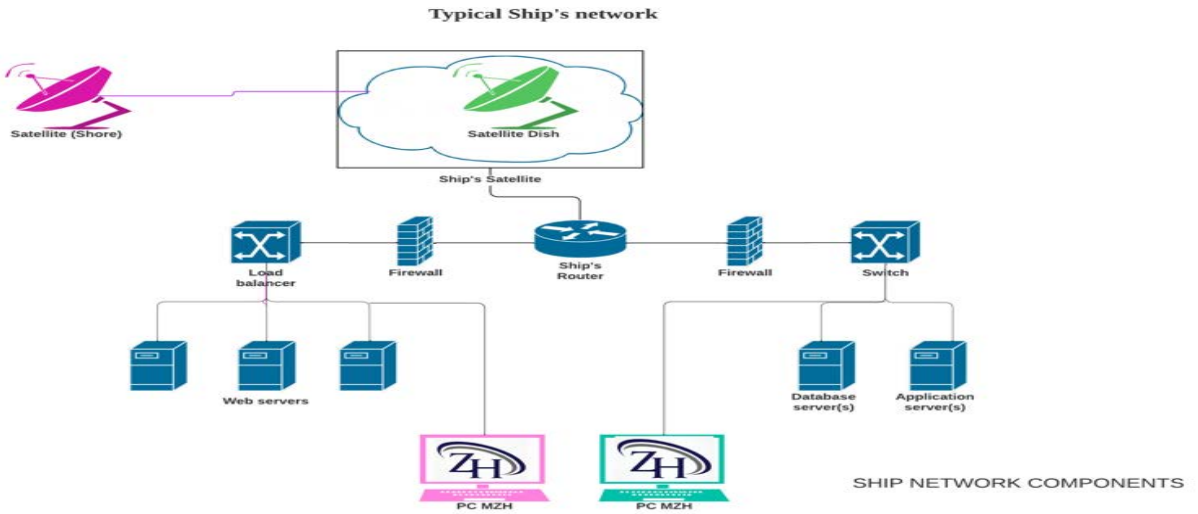


Figure 5: Ship Network Topology

However, this topology also has a drawback, where if a computer clicks a malicious link, it can install malware despite firewall security arrangements, which can have cascading impacts on servers' computers and IoT devices, leading to data being stolen, malware replication, and connecting to botnets with malicious intentions. All devices in this network require regular updates and security patches to keep the Local Area Network (LAN) safe and secure.

VI. Ship Network Topology (LBCC LAN to SBCC LAN)

The simulation illustrates an autonomous model where a central PC sends instructions to the SBCC's central PC and the LBCC, using IPSec VPN tunnelling to secure data from malicious actors. However, there is a risk that some data may not be able to be encrypted due to commercial pressures, increasing the risk of data breaches. Connecting ship systems to port and logistics systems increases the risk vectors and matrix as cross-industrial network volume increases.

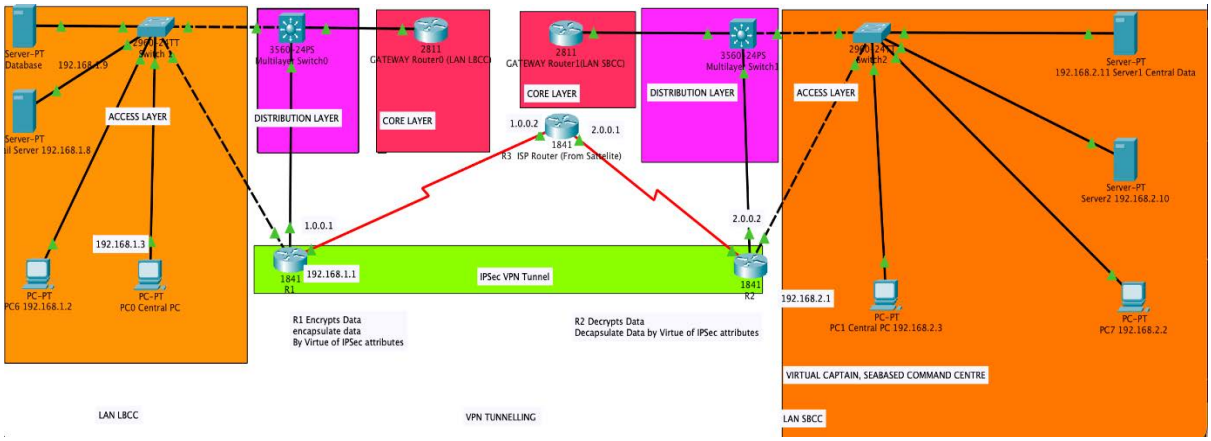


Figure 6: LAN to LAN Network Simulation

In the cyber world, all parties compete to control assets, infrastructures, and services in the supply chain (ship, port, and logistics), leading to a tug of cyber war.

VII. Computer Risk Management: (UoB, 2021)

The subsequent paragraphs focus on every network administrator's critical cyber security challenges. These challenges include threat vectors such as hacking, malware, and phishing, among others. Suppose shipboard management can effectively deal with these challenges. In that case, they will successfully handle maritime cyber challenges, avoiding supply chain disruptions and thwarting terrorist attacks or criminal and malicious intent on critical sea lanes of commerce (SLOC).

VIII. Key Maritime Cyber Challenges

The MTS computer network is a combination of LAN, WAN, and WWAN. Its main cyber security challenges include ensuring the security of networks and hardware, implementing threat monitoring, developing alternative networks, raising user awareness, and managing and configuring interfaces between networks to secure the whole network.

IX. What Does it Mean Cyber Security

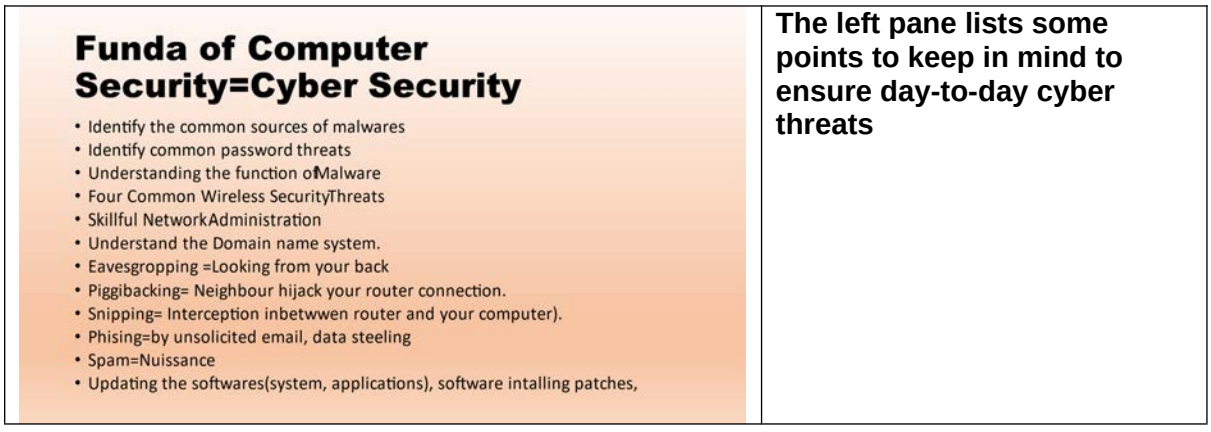


Figure 7: Fundamentals of Computer Security

a) *Overlapping*

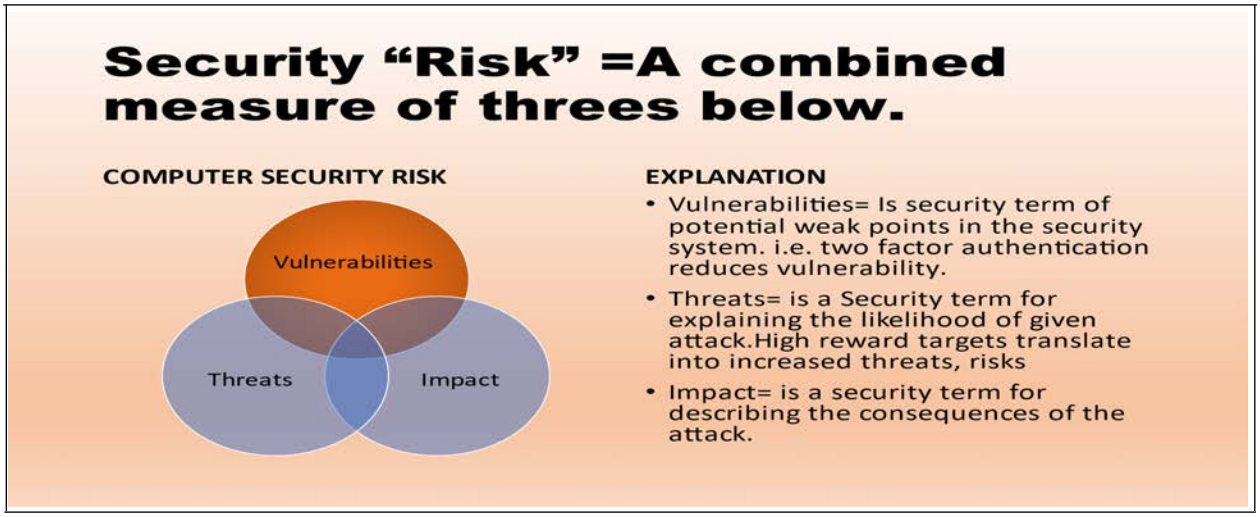


Figure 8: PC RISK MODEL IN Venn Diagram (UoB,2021)

b) *Viruses*

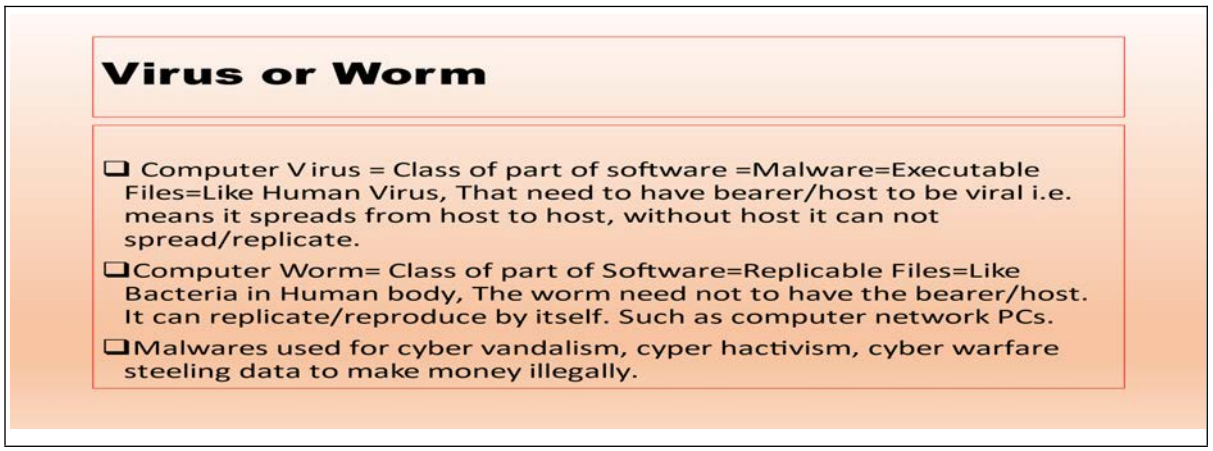


Figure 9: Virus or Worm Explanation

c) *Attack Definition*

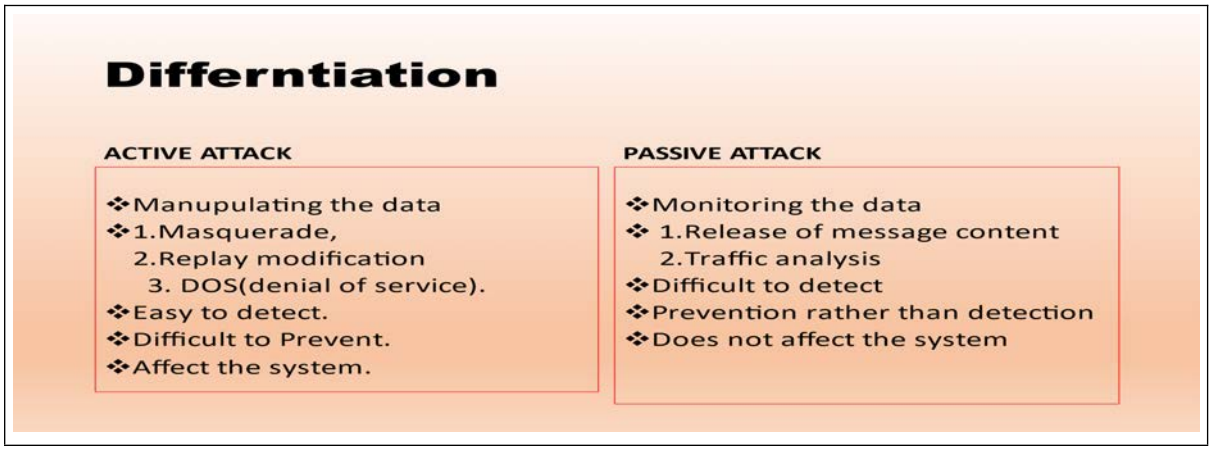


Figure 10: Attack Definition

d) Intrusion

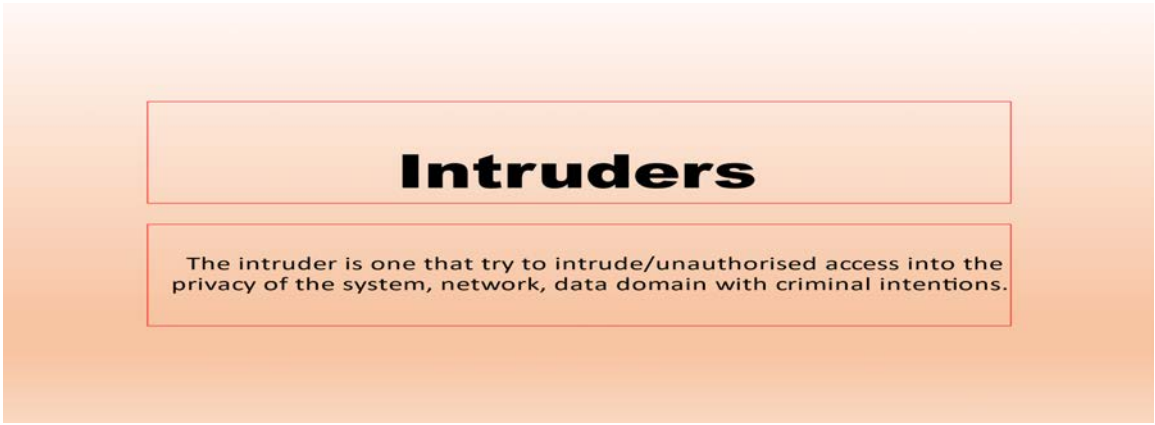


Figure 11: Intruder Definition

i. *Types of Intruders*

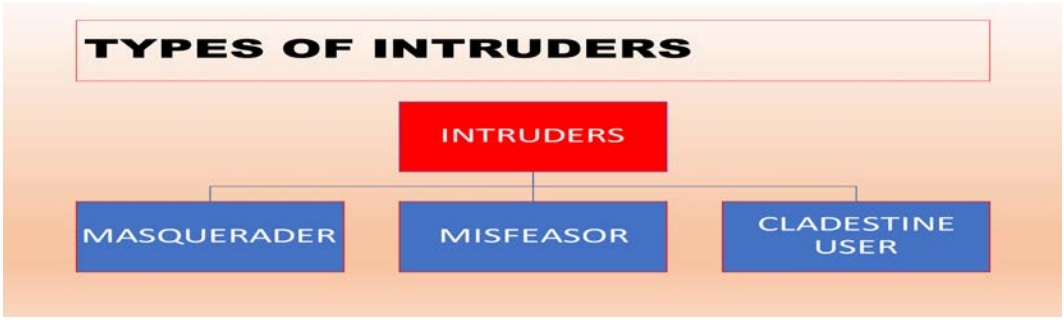


Figure 12: Types of Intruders

X. Attack Model: (IAPH, 2020)

Types of Techniques	How Delivered and Deployed
Social Engineering	Phycological Manipulation to click, tempting to click on the social media posts.
Ransomware	Email phishing, Remote Desktop Protocol (RDP), Downloads, Pirated Software, Removable Media. (Cawthra et al., 2020)
Spoofing	Domain Spoofing, Email Spoofing, geolocation GPS spoofing, TCP/IP Spoofing
Unauthorized Access	Gaining access to a company's network, endpoint, application, or device without permission is often due to flawed or misconfigured authentication measures.

XI. Attack on Model

Attack on IT System	Information Technology (IT) is used to create, process, store, securely transmit, and electronically exchange data, computers, networking, storage, and other devices.
Attack on OT System	Operational technology primarily engages with the physical world by controlling industrial equipment via hardware and software.
Attack on PNT Systems	Positioning, Navigation and Timing (PNT) is a system that includes three core capabilities: positioning, which is the ability to determine the ship's location precisely and reliably, and orientation in two dimensions (or three-dimensionally when necessary).

(Loomis et al., 2021, pp.1–50)

a) Navigation System

Modern ships use three types of navigation systems and 30 different navigational tools and resources, and communication and vessel status equipment. The ship has evolved into a floating computer network, but advanced IT interactions also increase vulnerability to specific threats as no computer equipment is 100% safe by default.

b) ICT (Information Communication Technologies)

The Internet is a complex network made up of millions of other networks. The Maritime Transportation System (MTS) is similar in that it is a system of systems. Information and Communication Technologies (ICT) play a vital role in these systems as they allow for data storage and communication between different parts of the system. However, vulnerabilities may surface when various components interact, such as from a ship to a satellite to a base station to a command and control and tracking center. The figure illustrates real-time global ship traffic, which is too vast to account for without using ICT and its applications, with red representing cargo ships.

Figure 16: Satellite Overview of Global Fleets (Marine Traffic, 2023)

Clicking on a vessel allows easy access to shipping details via satellite. Still, malign actors/hackers can alter the data and send false information to the satellite, base station, and vessel tracking centre, leading to inaccurate vessel location data.

c) Spoofing Attack

The spoofing attack on the global navigation satellite system (GNSS) aims to trick a GNSS receiver by transmitting fake signals that mimic real GNSS signals or by rebroadcasting real signals at a different location or time. The spoofing can cause the receiver to estimate its position incorrectly or at a different time, as decided by the attacker. One common type of GNSS spoofing is a carry-off attack, which starts by broadcasting signals in sync with the real signals that the receiver sees and then gradually increasing the strength of the fake signals. (Ball, 2020)

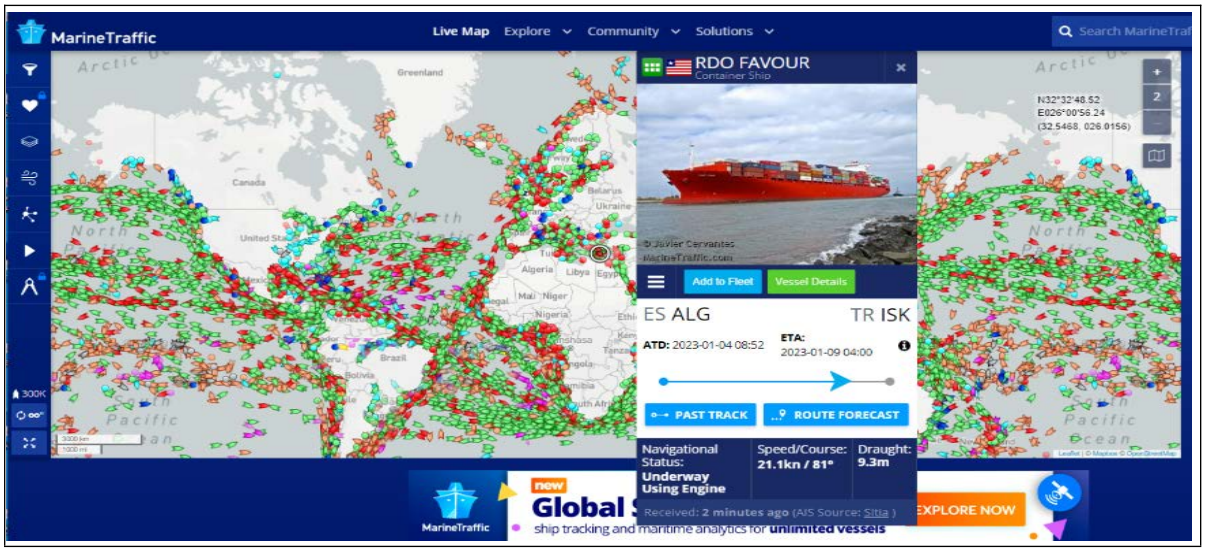


Figure 17: Ships' Data from Satellite Captures (Marine Traffic, 2023)

Ships have computerized devices connected to satellites and networks that allow for the exchange of information. However, the interconnected nature of the maritime transportation system means that when one component breaks down, it can significantly impact the entire system. (Brewin, 2013)

XII. Implications of the Cyber Disaster

The implication model illustrates the relationship between computer systems and the supply chain and how breakdowns can affect the entire system. The Defra Impact Calculator and methodology can be used to predict and calculate the monetary costs and impact of such breakdowns and help identify critical areas and interdependencies to mitigate risks.

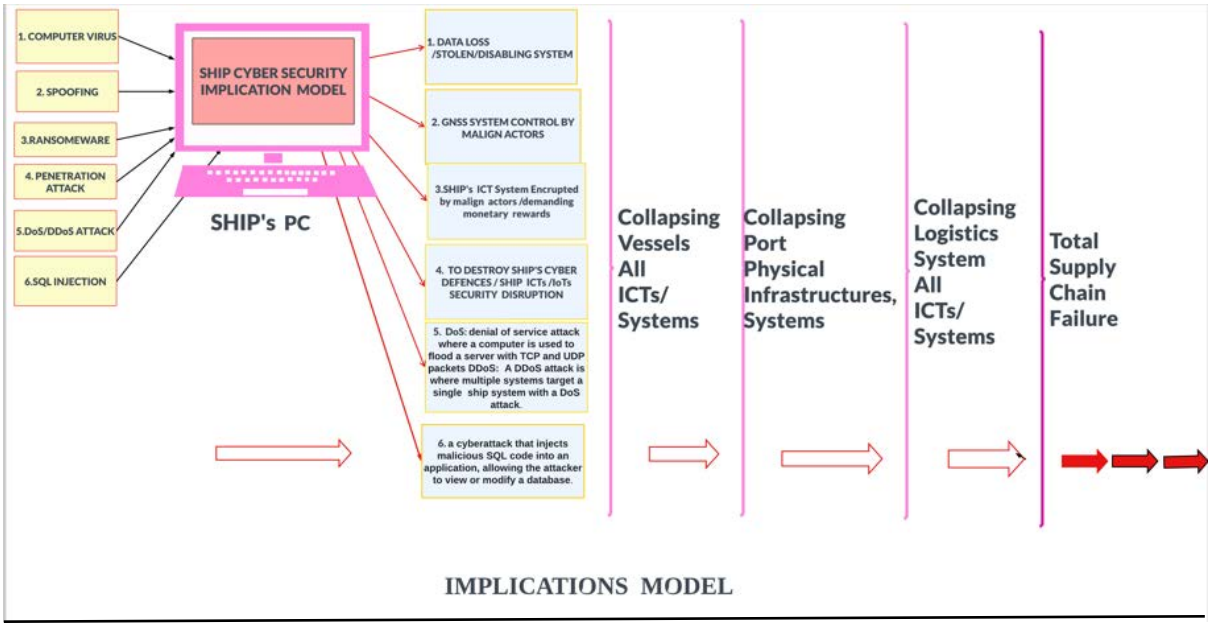


Figure 18: Cyber Disaster Implication Model

Shortages of essential items, price increases, industrial closures, unloaded shipping containers, and other factors can negatively impact a country's economic health.

XIII. Conclusions

It is important to remember that computer viruses need hosts to harm a system, service, or infrastructure. Cyber security can be effectively managed by understanding how malicious actors can take control of an organization's assets and services. The objectives of this article are looked at /conceptualized from various angles. They will help maritime professionals promote their awareness of cyber responsibilities in their workplace to uphold supply chain resilience and the resilience of its stakeholders.

References Références Referencias

1. Ball, B. (2020). Why GPS spoofing is a problem (and what to do about it). [online] NextNav. Available at: https://nextnav.com/gps-spoofing/ [Accessed 18 Jan. 2023].
2. Brewin, B. (2013). University of Texas Team Hijacks $80 Million Yacht with Cheap GPS Spoofing Gear. [online] Nextgov.com. Available at: https://www.nextgov.com/cxobriefing/2013/07/university-texas-team-hijacks-80-million-yacht-cheap-gpsspoofing-gear/67625/ [Accessed 18 Jan. 2023].
3. Cawthra, J., Ekstrom, M., Lusty, L., Sexton, J. and Sweetnam, J. (2020). Data Integrity: Detecting and Responding to Ransomware and Other Destructive Events. NIST SPECIAL PUBLICATION 1800-26. [online] doi:10.6028/nist.sp.1800-26.
4. CISA (2020). Critical Infrastructure Sectors | CISA. [online] Cisa.gov. Available at: https://www.cisa.gov/critical-infrastructure-sectors [Accessed 18 Jan. 2023].
5. Editorial Team (2020). Cyber-attacks on maritime OT systems increased by 900% in the last three years. [online] SAFETY4SEA. Available at: https://safety4sea.com/cyberattacks-on-maritime-ot-systems-increased-900-in-last-three-years/ [Accessed 18 Jan.2023].
6. Edwards, J. (2019). The Russians are screwing with the GPS system to send bogus navigation data to thousands of ships. [online] Business Insider Nederland. Available at: https://www.business-insider.nl/gnss-hacking-spoofing-jamming-russians-screwing-with-gps-2019-4?international=true&r=US [Accessed 18 Jan. 2023].
7. Government Law Enforcement (2023). The FBI's Advice on Ransomware. [online] www.cybersecurity intelligence.com. Available at: https://www.cyber-securityintelligence.com/blog/the-fbis-advice-on-ransomware-6723.html [Accessed 18 Jan. 2023].
8. IAPH (2020). PORT COMMUNITY CYBER SECURITY Courtesy Port of Los Angeles. [online] IAPH, pp.1–15. Available at: https://sustainable worldports.org/wpcontent/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf [Accessed 18 Jan. 2023]
9. Kessler, D.Z., Gary C. (2021). Cyber Threats and Choke Points: How Adversaries are Leveraging Maritime Cyber Vulnerabilities for Advantage in Irregular Warfare. [online] Modern War Institute. Available at: https://mwi.usma.edu/cyber-threats-and-chokepoints-how-adversaries-are-leveraging-maritime-cyber-vulnerabilities-foradvantage-in-irregular-warfare/ [Accessed 18 Jan. 2023].
10. Leahy, C. (2013). UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea. [online] UT News. Available at: https://news.utexas.edu/2013/07/29/ut-austinresearchers-successfully-spoof-an-80-million-yacht-at-sea/ [Accessed 18 Jan. 2023].
11. Loomis, W., Singh, V.V., Kessler, G.C. and Bellekens, X. (2021). RAISING THE COLORS: CYBER STATECRAFT Signaling for Cooperation on Maritime Cybersecurity. Atlantic Council, pp.1–50.
12. Reid, A. and Lorenz, J. (2008). Working at a Small-to-Medium Business or ISP: CCNA Discovery Learning Guide. 1st ed. Indianapolis, Indiana, USA: Cisco Press, pp.1–747.
13. Walton, H. (2022). The Maersk cyber-attack - How malware can hit companies of all sizes. [online] www.kordia.co.nz. Available at: https://www.kordia.co.nz/news-andviews/the-maersk-cyber-attack