International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 9 Issue 4, Jul-Aug 2025 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Maritime Cybersecurity

Matthew N. O. Sadiku[1], Paul A. Adekunte[2], Janet O. Sadiku[3]

[1]Roy G. Perry College of Engineering, Prairie View A&M University, Prairie View, TX, USA
[2]International Institute of Professional Security, Lagos, Nigeria
[3]Juliana King University, Houston, TX, USA

ABSTRACT

The growing reliance on digital solutions and interconnected systems on ships and in ports has expanded the attack surface for cybercriminals, making cybersecurity a top priority. Cyber threats to maritime are increasing rapidly. Cybersecurity is an increasingly important topic for the maritime and offshore industries due to rapid digital transformation. Maritime cybersecurity refers to the measures taken to protect ships, shipping infrastructure, and associated industries from cyber threats. It involves protecting vessels and port infrastructure from cyberattacks, ensuring safe and efficient operations, and safeguarding sensitive data. Maritime cybersecurity is of paramount importance for the movement of persons and goods that underpin the global economy, including food, medicine, and energy. It holds paramount significance both within the maritime industry and in the global economy at large. In this paper, we review the issues related to cybersecurity in the maritime environment.

KEYWORDS: *security, cybersecurity, maritime cybersecurity, maritime industry.*

How to cite this paper: Matthew N. O. Sadiku | Paul A. Adekunte | Janet O. Sadiku "Maritime Cybersecurity" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-9 | Issue-4, August 2025, pp.620-629, URL: www.ijtsrd.com/papers/ijtsrd97308.pdf

IJTSRD97308

INTRODUCTION

The maritime sector plays a key role in the global economy and society. Maritime organizations create, access, process, store, and transmit data. They are involved in significant financial transactions. They manage control systems moving cargo, and security systems that protect persons and the international maritime commerce. The increasing digitalization and automation of maritime industry, and the efforts to find the right trade-off between security and usability, introduce new vulnerabilities that increase cybersecurity risks [1]. The importance of maritime cybersecurity stems from the critical role that the maritime industry plays in global trade and logistics.

Disruptions to maritime operations can have significant economic consequences, impacting global trade, supply chains, and the movement of goods. Cyberattacks could compromise navigational systems, potentially leading to accidents, collisions, or other safety hazards. Cybersecurity is a critical risk area, as ship operation is largely dependent on the effectiveness of software-based systems for operations. Cybersecurity in maritime focuses on unique challenges including the protection of onboard navigation systems, communication networks, and operational technologies that are essential for the safety and efficiency of operations.

OVERVIEW ON CYBERSECURITY

Cybersecurity refers to a set of technologies and practices designed to protect networks and information from damage or unauthorized access. It is vital because governments, companies, and military organizations collect, process, and store a lot of data. As shown in Figure 1, cybersecurity involves multiple issues related to people, process, and technology [2]. Figure 2 shows different components of cybersecurity [3].

A typical cyber attack is an attempt by adversaries or cybercriminals to gain access to and modify their target's computer system or network. Cybercriminals or ethical hackers are modern-day digital warriors, possessing extraordinary skills and knowledge to breach even the most impregnable systems. A typical cybercriminal is shown on Figure 3 [4]. Cyber attacks are becoming more frequent, sophisticated, dangerous, and destructive. They are threatening the operation of businesses, banks, companies, and

government networks. They vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists) [5].

The cybersecurity is a dynamic, interdisciplinary field involving information systems, computer science, and criminology. The security objectives have been availability, authentication, confidentiality, nonrepudiation, and integrity. A security incident is an act that threatens the confidentiality, integrity, or availability of information assets and systems [6]. These are known as the pillars of information assurance.

- *Availability*: This refers to availability of information and ensuring that authorized parties can access the information when needed. Attacks targeting availability of service generally leads to denial of service.
- *Authenticity*: This ensures that the identity of an individual user or system is the identity claimed. This usually involves using username and password to validate the identity of the user. It may also take the form of what you have such as a driver's license, an RSA token, or a smart card.
- *Integrity*: Data integrity means information is authentic and complete. This assures that data, devices, and processes are free from tampering. Data should be free from injection, deletion, or corruption. When integrity is targeted, nonrepudiation is also affected.
- *Confidentiality*: Confidentiality ensures that measures are taken to prevent sensitive information from reaching the wrong persons. Data secrecy is important especially for privacy-sensitive data such as user personal information and meter readings.
- *Nonrepudiation*: This is an assurance of the responsibility to an action. The source should not be able to deny having sent a message, while the destination should not deny having received it. This security objective is essential for accountability and liability.

Good practices for cybersecurity in construction companies should include all of these elements.

Everybody is at risk for a cyber attack. Cyber attacks vary from illegal crime of individual citizen (hacking) to actions of groups (terrorists). The following are typical examples of cyber attacks or threats [7]:

- *Malware*: This is a malicious software or code that includes traditional computer viruses, computer worms, and Trojan horse programs. Malware can infiltrate your network through the Internet, downloads, attachments, email, social media, and other platforms. Spyware is a type of malware that collects information without the victim's knowledge.
- *Phishing*: Criminals trick victims into handing over their personal information such as online passwords, social security number, and credit card numbers.
- *Denial-of-Service Attacks*: These are designed to make a network resource unavailable to its intended users. These can prevent the user from accessing email, websites, online accounts or other services.
- *Social Engineering Attacks*: A cyber criminal attempts to trick users to disclose sensitive information. A social engineer aims to convince a user through impersonation to disclose secrets such as passwords, card numbers, or social security number.
- *Man-In-the-Middle Attack*: This is a cyber attack where a malicious attacker secretly inserts him/herself into a conversation between two parties who believe they are directly communicating with each other. A common example of man-in-the-middle attacks is eavesdropping. The goal of such an attack is to steal personal information.

These and other cyber attacks or threats are shown in Figure 4 [8]. Sources of cyber threats are displayed in Figure 5 [9].

The social and financial importance of cybersecurity is increasingly being recognized by businesses, organizations, and governments. Cybersecurity involves reducing the risk of cyber attacks. Cyber risks should be managed proactively by the management. Cybersecurity technologies such as firewalls are widely available [10]. Cybersecurity is the joint responsibility of all relevant stakeholders including government, business, infrastructure owners, and users. Cybersecurity experts have shown that passwords are highly vulnerable to cyber threats, compromising personal data, credit card records, and even social security numbers. Governments and international organizations play a key role in cybersecurity issues. Securing the cyberspace is of high priority to the US Department of Homeland Security (DHS). Vendors that offer mobile security solutions include Zimperium, MobileIron Skycure, Lookout, and Wandera.

MARITIME CYBERSECURITY

Digital systems are radically enhancing the operational efficiency of ships and significantly

enhancing their environmental performance. Digital technologies are increasingly applied to areas like navigation, logistics, and communication, contributing to greater energy efficiencies and reduced emissions. However, as digital technologies make rapid advances, so do the systems that can cause them harm. The maritime industry, at the heart of global supply chains, is a prime target for cyber-attacks and cyber criminals. Adversaries may target various aspects of the maritime industry, including navigation systems, communication networks, cargo management systems, and port infrastructure. They may also target port infrastructure that can lead to disruptions in cargo handling, customs clearance, and logistical operations, impacting the flow of goods and potentially causing significant economic losses. Cybersecurity breaches that target critical systems on a vessel can have severe consequences on the vessel's stability, safety, and overall operations [11]. Figure 6 shows a representation of maritime cybersecurity [12].

Maritime cyber risk refers to a measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost, or compromised. Maritime cybersecurity refers to the practices, technologies, and policies used to protect ships, shipping infrastructure, and associated industries from cyber threats and attacks. It encompasses the strategies, technologies, and policies used to safeguard against cyberattacks that could compromise operations, safety, and sensitive information.

Key aspects of maritime cybersecurity include:

- *Protecting Vessels and Systems*: This includes securing navigation systems, engine controls, and other critical onboard systems that rely on software and digital technology.
- *Securing Shipping Infrastructure*: Protecting ports, communication networks, and other shore-based systems that support maritime operations from cyber threats.
- *Risk Management:* Identifying, assessing, and mitigating potential cyber risks to ensure safe and secure shipping operations.
- *Incident Response:* Developing and implementing plans to detect, contain, and recover from cyber incidents, minimizing their impact.
- *Training and Awareness:* Educating maritime personnel about cyber threats and best practices can prevent attacks. Educating personnel on cybersecurity best practices, including recognizing phishing attempts and handling sensitive information, is critical. It is vital to regularly train all employees on cybersecurity best practices and the latest phishing tactics.

COMBATING CYBERSECURITY IN MARITIME INDUSTRY

Cybercriminals are leveraging advanced technologies, such as artificial intelligence (AI) and large language models, to conduct more adaptive and precise attacks. The maritime industry, including shipping, ports, and offshore activities, is highly vulnerable to cyber-attacks with implications including impact to global trade, significant financial losses, environmental damage, and even loss of life. Off-the-shelf large language models have become a critical tool for hackers, allowing them to accelerate malware development, automate phishing campaigns, and refine social engineering tactics. Safeguarding the maritime sector against cyber threats is crucial to ensuring the safety, integrity, and efficiency of maritime operations as well as for protecting sensitive information and global trade. The following measures are important for combating cybersecurity in the maritime industry [13-16]

- *Risk Management*: The notion of risk may differ among various industries but typically involves evaluating the probability and consequences of potential incidents that could impact assets. A risk management strategy involves setting an organization's priorities, defining its limitations, establishing its level of tolerance towards risk, and making certain assumptions. Together, these elements impact the decisions related to operational risk. In today's evolving business environment, the significance of proficient and strategic risk management is extremely crucial. Maritime companies must implement robust cybersecurity risk management systems, addressing protection, detection, response, and recovery for both IT and OT systems.
- *Risk Assessment:* Risk assessment refers to the organization's understanding of the cybersecurity risk to its resources, employees, mission, functions, image, or reputation. Assessing cyber risks entails comprehending the likelihood of incidents and their outcomes, including collisions, operational disruptions, and economic losses. Risk assessment is an essential first step in protecting personal information and lowering the likelihood of harm to individuals, property, other organizations, and nations. It is evident that effective risk assessment is a critical component of modern ship operations, requiring constant vigilance and adaptability to protect against ever-

evolving cyber threats. Risk assessment methodologies and frameworks are paramount in managing and mitigating the growing cyber threats in the maritime industry.

- *Security Regulations:* Several research efforts have proposed autonomous systems and cybersecurity regulations focused on the development and verification of autonomous systems. Identifying and addressing the multifaceted aspects of autonomous systems and cybersecurity regulations is imperative in order to create advanced security requirements, swift cybersecurity regulations, and proactive protection models.
- *Awareness and Training*: There is a consensus on the role of education and training in enhancing maritime cybersecurity. Organization's personnel and partners should be provided with cybersecurity education to enhance awareness of their cybersecurity-related duties and responsibilities. Maritime cyber security training for personnel helps to improve the overall cyber security posture of the maritime industry. The training raises awareness of the varying cyber threats. Employees can learn about different types of cyber attacks and the impact they can have on the maritime industry. They can also learn how to identify cyber threats and how to respond to them. By raising awareness, employees can become more vigilant and take appropriate measures to prevent cyber attacks.
- *Incident Analysis:* Cybersecurity incidents that significantly disrupt operations must be reported to relevant national authorities within 24 hours of detection. Incident analysis is the crucial process of examining cybersecurity incidents to inform response activities and support recovery operations. Through systematic analysis, organizations can extract valuable lessons to enhance their overall cybersecurity posture and responsiveness to future incidents. This process is instrumental in minimizing adverse effects, ensuring rapid system recovery, preserving data integrity, and maintaining organizational resilience in the face of escalating and evolving cyber threats.
- *Ship Cybersecurity:* There are two general types of cyber attacks that can affect a marine company or a ship — untargeted attacks and targeted attacks. Untargeted attacks look for potential cyber weak spots in multiple companies or ships. Targeted attacks are directed toward a specific company or ship and can be harder to deter. As discussed earlier, there are many ways (such as social engineering, tampering, phishing, hijacking, jamming, and spoofing, etc.) cybercriminals may attack your ship or company's systems. These methods share a focus on compromising communication and navigation systems. Cyber attackers have different reasons for trying to access your company or ship data and systems, ranging from identity theft to defamation of your company. Figure 7 shows stages of a cyber attack [17], while Figure 8 shows how to create a ship cybersecurity plan [17]. In an attempt to reduce cybersecurity threats, the United States Coast Guard has paired with the Transportation Security Administration to fight potential cyber risks in the shipping industry and prepare mariners with the knowledge to combat them.
- *Port Cybersecurity:* Ports and shipping lanes are ripe for adversaries' exploits. Cybersecurity is one of the growing challenges facing ports since ports are at the center of the country's supply chain. The need for advanced cybersecurity in ports is gaining momentum in the maritime sector. The proliferation of technology in maritime operations has profoundly impacted ports worldwide, leading to increased efficiency and the emergence of "smart" port operations. However, these advancements have also introduced new cyber threats, making risk assessment at ports a topic of critical importance U.S. ports are vital to the flow of imports and exports; however, the entire maritime transportation system's cybersecurity is exceedingly vulnerable. The August 2024 ransomware attack at the Port of Seattle resulted in significant cargo delays and a data breach of 90,000 individuals. The Coast Guard wants to help ports and others meet cybersecurity requirements, but it is also hampered by resourcing challenges. A typical port is shown in Figure 9 [14].
- *Coast Guard:* On January 17, 2025, the US Coast Guard published a new final rule that establishes baseline cybersecurity requirements to protect the marine transportation system (MTS) from cyber threats. This final rule addresses current and emerging cybersecurity threats in the MTS by adding minimum cybersecurity requirements to help detect risks and respond to and recover from cybersecurity incidents. This final rule also includes a solicitation for comments on a potential delay for the implementation periods for US-flagged vessels. In collaboration with Congress, state and local leaders, and the private sector, the administration must properly support

and modernize the US Coast Guard. Congress and the administration should increase cyber-specific Coast Guard personnel and automated digital tools to gain visibility across thousands of miles of coastline.

- *National Maritime Cybersecurity*: The National Maritime Cybersecurity Plan states that the US will work to "produce cybersecurity specialists in port and vessel systems." The plan highlights three areas of focus for the US government to help meet the challenge of growing maritime cyber risk: risk and standards, information and intelligence sharing, and workforce development. It proposes better risk modeling to inform standards and best practices. Shipowners and operators must ensure that third-party vendors and suppliers meet cybersecurity standards.

BENEFITS

Cyber incidents can damage the reputation of shipping companies and lead to financial losses. Cyber attacks can lead to operational disruptions, financial losses, environmental damage, and even endangerment of life. Cybersecurity in maritime has a huge potential to affect the safety of the crew, vessel, cargo, and even ports. Other benefits of maritime cybersecurity include the following [18]:

Enhanced Resilience: Maritime cyber security training can help enhance the industry's resilience against cyber-attacks. Employees can learn how to respond to cyber incidents, recover from them, and prevent similar incidents in the future. By enhancing resilience, the industry can ensure that it can continue its operations even in the face of cyber-attacks.

Protection of Reputation: Maritime cyber-attacks can have severe consequences to both company and industry reputations. Customers and stakeholders can lose trust, resulting in lost business. Maritime cyber security training can help employees to protect the industry's reputation by preventing cyber-attacks and responding appropriately in case of a cyber-incident.

Data Security: Data security has been identified as a critical area of advancement. There is the necessity of protective measures to maintain the confidentiality, integrity, and accessibility of data. This is achieved through the application of various controls, such as access restrictions, cryptographic techniques, and data backup procedures, designed to fend off unauthorized access, unintended alterations, or unintentional data loss.

CHALLENGES

The threat landscape to the maritime industry is expanding as the threat actors increase. Regularly assessing vulnerabilities and potential threats to both onboard systems and shore-based operations is crucial. The maritime industry faces cybersecurity challenges when it comes to investment, regulation, supply chains, organizational culture, and access to talent. Other challenges of maritime cybersecurity include [19,20]:

- *Addressing IT and OT systems:* Maritime cybersecurity integrates both Information Technology (IT) and Operational Technology (OT) to secure vessels from unauthorized access, data breaches, and other cyber threats. Recognizing that both Information Technology (IT) and Operational Technology (OT) systems on ships are vulnerable and require specific cybersecurity measures. As shown in Figure 10, cyber systems for ships and mobile units are classified as either IT (standard information systems) or OT (operation and control systems) [19]. While IT systems are generally more mature in terms of cybersecurity, OT systems (like those controlling navigation and engine functions) are often less secure and pose a greater risk to ship safety.
- *Sensitive Data:* Maritime operations involve handling sensitive information like cargo details, port schedules, and financial data, which can be vulnerable to theft or loss through cyberattacks.
- *Increasing Connectivity:* More interconnected systems and the use of cloud-based technologies increase the potential attack surface for cybercriminals.
- *Geopolitical Tensions:* State-sponsored cyberattacks targeting maritime infrastructure are on the rise, aiming to disrupt global trade and exert influence.
- *Collaboration:* There is a pressing need for increased collaboration between public and private partnerships to enhance system security, identify threats, and effectively mitigate risks. While smaller regional maritime groups are already collaborating, establishing larger, more comprehensive coalitions is essential. Effective maritime cybersecurity requires collaboration between governments, industry stakeholders, and technology providers. Sharing information about cyber threats and best practices among stakeholders is crucial for building a resilient maritime industry.
- *Regulations:* Regulation is another factor that is changing the maritime cybersecurity landscape. The maritime industry is subject to various regulations, and compliance is essential to avoid penalties and other legal consequences.

Compliance with international regulations and standards, such as those developed by the International Maritime Organization (IMO), is essential for ensuring a baseline level of security across the industry. The IMO and other regulatory bodies are tightening cybersecurity requirements to address the growing threat landscape. There is limited access to major ports for ships that fail to meet cybersecurity requirements.

- *Continuous Improvement:* Maritime cybersecurity is an ongoing process, requiring continuous monitoring, assessment, and adaptation to emerging threats and technologies.
- *Risk Management:* Cyber risk management means the process of identifying, analyzing, assessing and communicating a cyber-related risk and accepting, avoiding, transferring or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders. Maritime organizations need to take appropriate steps to identifying, analyzing, assessing, and communicating cybersecurity risks, and accepting, avoiding, transferring, or mitigating them to an acceptable level. This requires an overall organizational approach of risk management,
- *Fraud:* Another risk that arises due to the advancement of digitalization is fraud. Fake content has never been easier to create – or harder to catch. It has now become more difficult to spot potential frauds and tell the difference between what is real and what is not, as fraudsters use generative AI to create convincing phishing and spear phishing emails.
- *Vulnerability of Onboard Systems*: Ships rely on various digital systems for navigation, engine control, communication, and cargo management, making them potential targets for cyberattacks.

CONCLUSION

The maritime sector relies heavily on interconnected networks, communication systems, and sophisticated technologies for its operations, making it an attractive target for cybercriminals, nation-states, and other threat actors. Cybersecurity in the maritime industry is becoming increasingly crucial due to the growing reliance on digital systems for ship operations and the rise in cyber threats. Implementing robust cybersecurity management systems, as mandated by the International Maritime Organization (IMO) and other regulatory bodies, is essential. More information about maritime cybersecurity can be found in the books [21-25] and the following related journals:

- Journal of Marine Science and Engineering
- International Journal of Information Security

REFERENCES

[1] "Maritime cybersecurity," https://www.maritime-cybersecurity.com/

[2] P. Singh, "A layered approach to cybersecurity: People, processes, and technology- explored & explained," July 2021, https://www.linkedin.com/pulse/layered-approach-cybersecurity-people-processes-singh-casp-cisc-ces

[3] M. Loi et al., "Cybersecurity in health – disentangling value tensions," *Journal of Information, Communication and Ethics in Society,* June 2019, https://www.emerald.com/insight/content/doi/10.1108/JICES-12-2018-0095/full/html

[4] M. Adams, "Unlocking the benefits of ethical hacking: The importance of ethical hackers in cybersecurity," April 2023, https://www.businesstechweekly.com/cybersecurity/network-security/ethical-hacking/

[5] M. N. O. Sadiku, S. Alam, S. M. Musa, and C. M. Akujuobi, "A primer on cybersecurity," *International Journal of Advances in Scientific Research and Engineering*, vol. 3, no. 8, Sept. 2017, pp. 71-74.

[6] M. N. O. Sadiku, M. Tembely, and S. M. Musa, "Smart grid cybersecurity," *Journal of Multidisciplinary Engineering Science and Technology*, vol. 3, no. 9, September 2016, pp.5574-5576.

[7] "FCC Small Biz Cyber Planning Guide," https://transition.fcc.gov/cyber/cyberplanner.pdf

[8] "The 8 most common cybersecurity attacks to be aware of," https://edafio.com/blog/the-8-most-common-cybersecurity-attacks-to-be-aware-of/

[9] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports,* vol. 7, November 2021, https://www.sciencedirect.com/science/article/pii/S2352484721007289

[10] Y. Zhang, "Cybersecurity and reliability of electric power grids in an interdependent cyber-physical environment," *Doctoral Dissertation,* University of Toledo, 2015.

[11] "Maritime cyberthreats reflect expansion of vulnerable systems, shifting focus to boosting cybersecurity posture," August 2023, https://industrialcyber.co/features/maritime-cyberthreats-reflect-expansion-of-vulnerable-systems-shifting-focus-to-boosting-cybersecurity-posture/

[12] "Recent cybersecurity incidents and regulatory developments in the maritime industry (March 2025)," March 2025, https://shipip.com/recent-cybersecurity-incidents-and-regulatory-developments-in-the-maritime-industry-march-2025/

[13] "The U.S. Coast Guard new cybersecurity regulations for the marine transportation system," https://www.uscg.mil/MaritimeCyber/

[14] J. Le, "Rebuilding maritime cybersecurity resilience: Charting an America first course to secure the U.S. Homeland," April 2025, https://cyberscoop.com/us-maritime-cybersecurity-challenges-opportunities-2025/

[15] A. Dimakopoulou and K. Rantos, "Comprehensive analysis of maritime cybersecurity landscape based on the NIST CSF v2.0," *Journal of Marine Science and Engineering,* vol. 12, no. 6, 2024.

[16] A. King and M. Gallagher, "A rising tide lifts all boats in maritime cybersecurity," October 2021, https://cyberscoop.com/maritime-cybersecurity-rising-tide/

[17] "Guide to ship cybersecurity," March 2024, https://www.mitags.org/guide-ship-cybersecurity/

[18] "Why is cyber security so important to mariners?" May 2024, https://www.mitags.org/why-is-cyber-security-so-important-to-mariners/

[19] "Maritime cyber security," https://www.dnv.us/maritime/insights/topics/maritime-cyber-security/

[20] "Maritime cyber security: Piecing the puzzle together," June 2024, https://safety4sea.com/maritime-cyber-security-piecing-the-puzzle-together/

[21] G. C. Kessler and S. D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers.* Independently Published, 2022.

[22] J. DiRenzo III, N. K. Drumhiller, and F. S. Roberts (eds.), *Issues in Maritime Cyber Security.* Westphalia Press, 2017.

[23] S. Bauk (ed.), *Maritime Cybersecurity*. Springer, 2025.

[24] G. Blokdyk, *The Operational Excellence Library; Mastering Maritime Cybersecurity.* 5STARCooks, 2024.

[25] F. S. Roberts, J. DiRenzo, and N. K. Drumhiller (eds.), *Issues in Maritime Cyber Security*. Amazon Digital Services LLC, 2017.

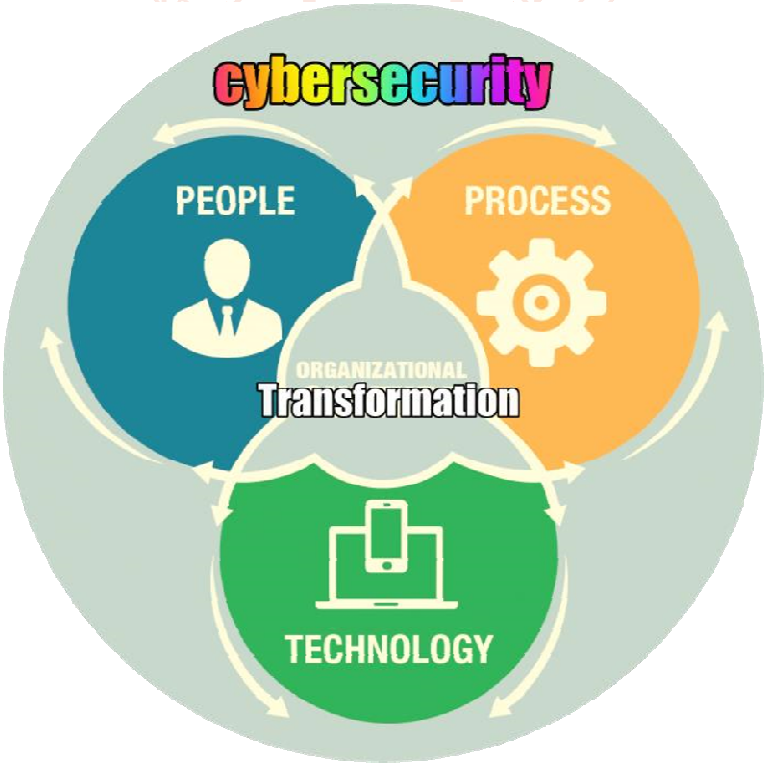

Figure 1 Cybersecurity involves multiple issues related to people, process, and technology [2].

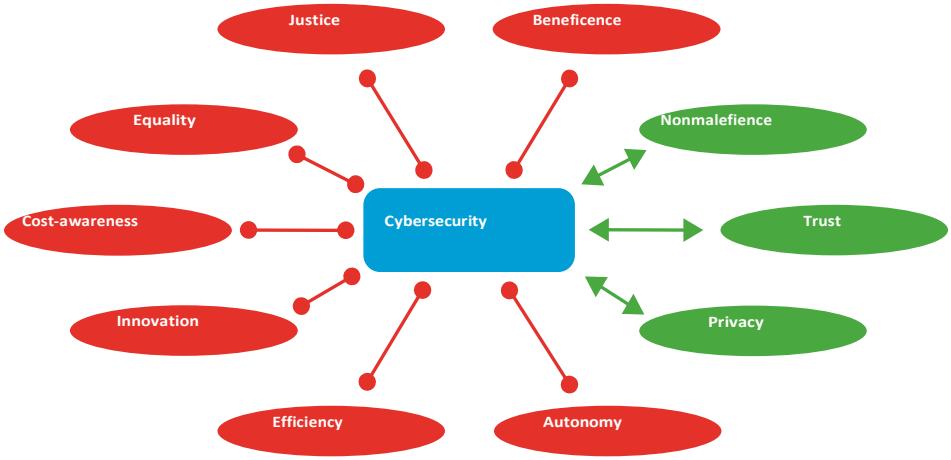

Figure 2 Different components of cybersecurity [3].(Green: supportive; red: in tension)

Figure 3 A typical cybercriminal [4].

Figure 4 Common types of cybersecurity threats [8].

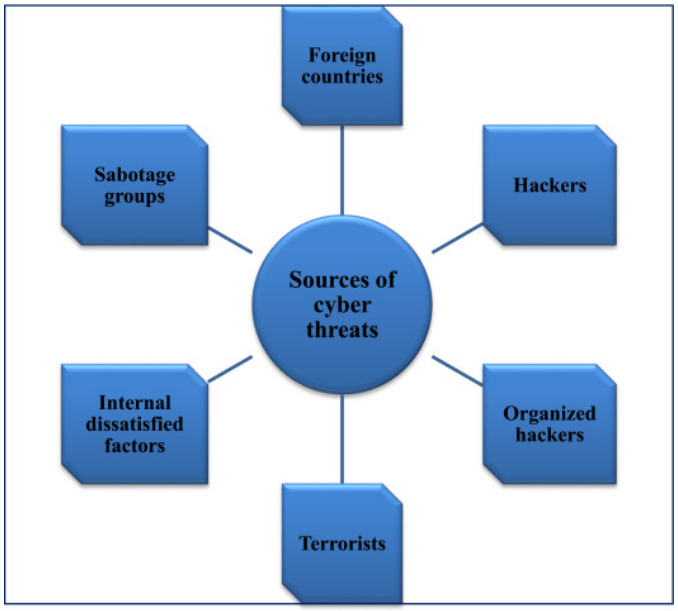

Figure 5 Sources of cyber threats [9].

Figure 6 A representation of maritime cybersecurity [12].

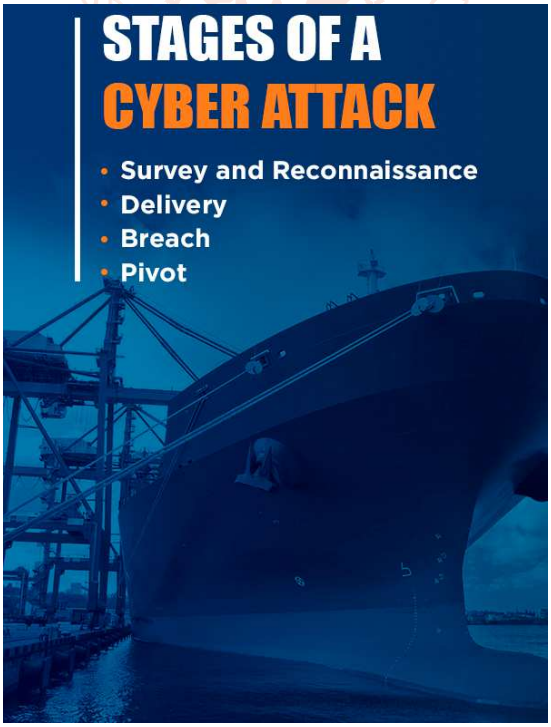

Figure 7 Stages of a cyber attack [17].

Figure 8 How to create a ship cybersecurity plan [17].

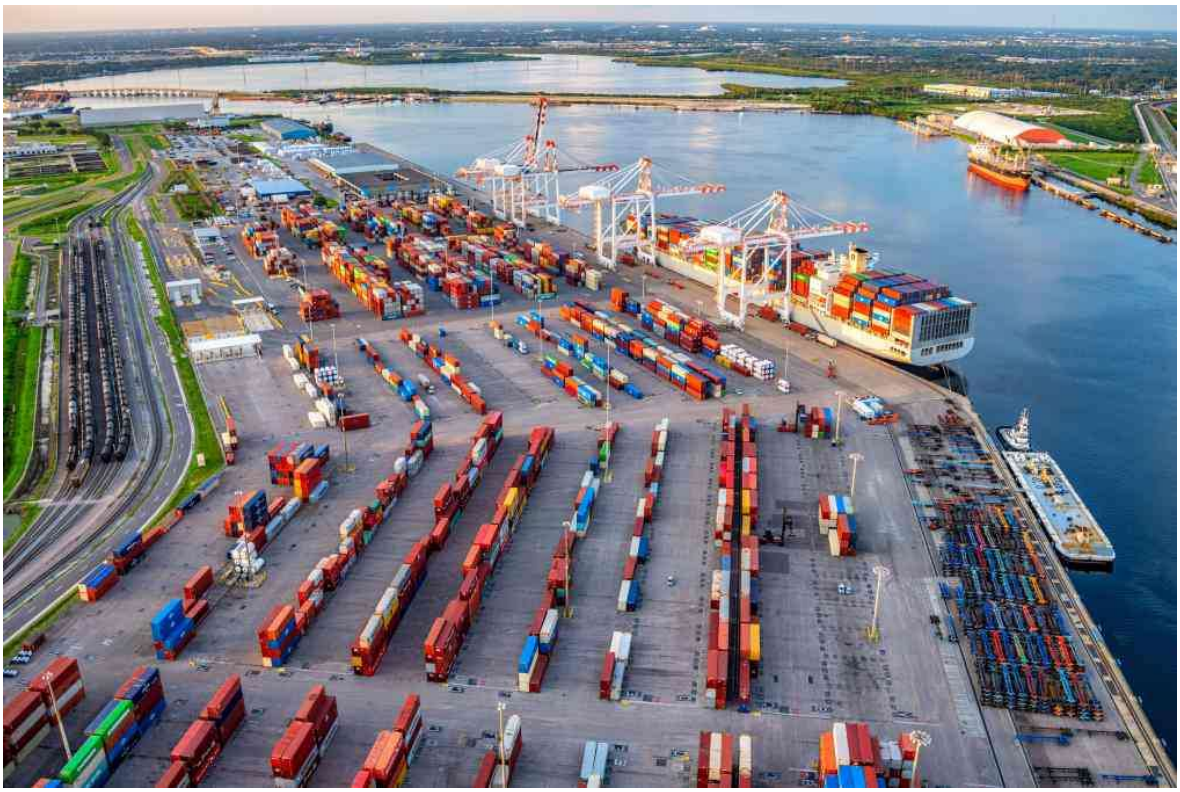

Figure 9 A typical port [14].

Figure 10 Cyber systems for ships and mobile units are classified as either IT or OT [19].