https://doi.org/10.26219/heal.aueb.5426

Διπλωματικη Εργασια

Enhancing Operational Technology (OT) Cybersecurity in the Maritime Sector: Risk Mitigation Strategies and Resilience Frameworks

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ ΣΤΗΝ ΑΝΑΠΤΥΞΗ ΚΑΙ ΑΣΦΑΛΕΙΑ ΠΛΗΡΟΦΟΡΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

Συγγελάκης Ιωάννης

(p3312214)

Επιβλέπων καθηγητής: Ντούσκας Θεόδωρος

Οικονομικό Πανεπιστήμιο Αθηνών

https://doi.org/10.26219/heal.aueb.5426

Περιεχόμενα

https://doi.org/10.26219/heal.aueb.5426

List of Figures

List of Tables

https://doi.org/10.26219/heal.aueb.5426

Συγγελάκης Ιωάννης

Enhancing Operational Technology (OT) Cybersecurity in the Maritime Sector: Risk Mitigation Strategies and Resilience Frameworks

Περίληψη

Η αυξανόμενη ψηφιοποίηση της ναυτιλιακής βιομηχανίας απαιτεί την ενσωμάτωση των τεχνολογιών πληροφορικής στο επιχειρησιακό τμήμα, μετασχηματίζοντας τον τρόπο λειτουργίας πλοίων, λιμένων και δικτύων εφοδιαστικής αλυσίδας. Αυτή η σύγκλιση σημαίνει ότι η σύγχρονη επιχειρησιακή τεχνολογία στη ναυτιλία βελτιώνει την αποδοτικότητα, τον αυτοματισμό και τη συμμόρφωση με τους κανονισμούς. Παράλληλα, όμως, εισάγει σημαντικούς κινδύνους κυβερνοασφάλειας. Η παρούσα μελέτη παρέχει μια ολοκληρωμένη ανάλυση των συστημάτων επιχειρησιακής τεχνολογίας στη ναυτιλία, εστιάζοντας στα πλεονεκτήματα που προσφέρουν, καθώς και στις ευπάθειες που παρατηρούνται. Επιπλέον, παρουσιάζεται η εξελισσόμενη απειλή στον κυβερνοχώρο, με παραδείγματα από σημαντικά πραγματικά περιστατικά κυβερνοεπιθέσεων, όπως η επίθεση NotPetya στη Maersk, καθώς και βέλτιστες πρακτικές στον χώρο, όπως η αποδοτικότητα του λιμένα της Σιγκαπούρης και οι αυτόνομες λειτουργίες του πλοίου Yara Birkeland. Παράλληλα, εξετάζονται τα ρυθμιστικά πλαίσια που αφορούν τη σύγχρονη επιχειρησιακή τεχνολογία στη ναυτιλία, συμπεριλαμβανομένων των IMO MSC.428(98), IEC 62443, IACS Unified Requirements και της Οδηγίας NIS2 της ΕΕ, προκειμένου να αξιολογηθεί η αποτελεσματικότητά τους στη μείωση των κινδύνων στον κυβερνοχώρο.

Λέξεις-κλειδιά

Ναυτιλιακή βιομηχανία, επιχειρησιακή τεχνολογία (ΟΤ), κυβερνοασφάλεια, σύγκλιση IT-OT, πρότυπα κυβερνοασφάλειας, κανονισμοί κυβερνοασφάλειας, διαχείριση κινδύνων κυβερνοασφάλειας στη ναυτιλιακή ΟΤ.

https://doi.org/10.26219/heal.aueb.5426

Abstract

The increasing digitalization of the maritime industry demands integration of informational technologies into the operational part, transforming the way vessels, ports, and supply chain networks operate. This convergence means that modern maritime operational technology enhances the industry's efficiency, automation, and regulatory compliance. With it, however, it also introduces significant cybersecurity risks. This study provides a comprehensive analysis of maritime operational technology systems, focusing on the advantages it brings, as well as vulnerabilities observed. What is more, the paper outlines the evolving threat landscape, drawing insights from major real-world cyber incidents such as the NotPetya attack on Maersk as well as best practices in the sphere, such as the port of Singapore efficiency and the Yara Birkeland autonomous ship operations. Additionally, the research examines regulatory frameworks relevant for modern maritime OT, including IMO MSC.428(98), IEC 62443, IACS Unified Requirements, and the EU's NIS2 Directive, to assess their effectiveness in mitigating cyber risks.

Keywords

Maritime industry, operational technology (OT), cybersecurity, IT-OT convergence, cybersecurity standards, cybersecurity regulations, cybersecurity risk management for maritime OT.

 https://doi.org/10.26219/heal.aueb.5426

Introduction

With the maritime industry with its vast networks of shipping lanes, ports, and logistics hubs, being the backbone of global trade through, its rapid and profound digitalization emerging as a crucial aspect of the global economic stability. Changes introduced by the digitalization encompass, among other active integration of Operational Technology (OT) into the sector operation. Operational Technology in the said context refers to hardware and software systems that control and monitor physical processes in shipboard and portside settings, directly interacting with their critical aspects, including navigation (ECDIS), cargo handling, ballast water management, satellite communication, etc. (Pfaff, 2022). These OT systems are becoming increasingly complex, with multiple networks being integrated to enable remote diagnostics, predictive maintenance, and real-time decision-making.

With multiple benefits that such integration brings, there are also significant challenges, with some of the main of them being related to new cybersecurity vulnerabilities, which maritime operators had never been concerned with before. As digitalization in the domain has accelerated the deployment of smart ship technologies, IoT sensors, autonomous systems, and AI-driven analytics within OT environments, the cyber threat issues as well as technical ones, including system failures are becoming the center of concerns not only for vessels, but also for ports and wider marine logistic networks. Finally, there is also demand for enhanced efficiency, fuel optimization and other aspects of OT integration, which all should be accounted for with the observance of stringent regulatory, safety and environmental compliance. Thus, the issue has become pressing concerns for shipowners, classification societies, marine regulatory bodies, and cybersecurity experts worldwide.

Research Objectives

The primary objective of this study is to analyze the role of Operational Technology (OT) in the maritime industry. This includes examination of its cybersecurity challenges, as well as analysis of the regulatory frameworks designed to mitigate risks. Thus, identified objectives of the research include:

https://doi.org/10.26219/heal.aueb.5426

1) Examination of the architecture and functionality of maritime OT systems. This will include navigation, propulsion, cargo management, both in vessels and port operations.

2) Identification and assessment of cybersecurity vulnerabilities in maritime OT. The focus here is made on IT-OT convergence risks, real-world cyber incidents, and emerging threats.

3) Evaluation of international cybersecurity regulations and standards with particular focus on their facilitation of cyber risks prevention and mitigation.

4) Exploration of cybersecurity strategies and risk management frameworks, adopted by leading shipping companies and port authorities.

5) Assessment of future trends in maritime OT security. In this respect issues associated with autonomous ships, IoT applications, and AI-driven cybersecurity solutions will be given particular attention.

Insights gained from the investigation of the outlined issues will provide valuable information for all the involved stakeholders, shipowners and policy makers included. With the increasing digitalization and automation of the maritime industry, it is crucial to ensure the resilience and security of OT systems to foster safe operations in the sector, economic stability, and environmental protection.

To achieve the outlined objectives, the study starts with the exploration of the maritime environment, its key stakeholders, and OT's role in modern shipping, which sets a stage for the research. After that the paper moves onto the discussion of main cybersecurity threats, exemplifying them with the real-world case studies. Further on, the study delves into the technical aspects of maritime OT to highlight the importance of each of its aspects. To do so, the study provides an in-depth analysis of maritime OT systems, their vulnerabilities, and IT-OT integration challenges. After the technical aspects of OT integration into maritime operations are discussed, the study will move into the regulatory issues, related to it. In this, the paper will examine cybersecurity standards and regulations (including IEC 62443, IMO, IACS, NIS2) and their implications for maritime security. The main aim of the analysis of the outlined regulations is

https://doi.org/10.26219/heal.aueb.5426

identification of their limitations regarding cybersecurity (and/or other) concerns in OT in the maritime industry. After that, exploration of practical solutions will be done to address the identified cybersecurity challenges. In this paper will focus on risk management frameworks and cybersecurity strategies for securing OT in ships and ports. Looking ahead into the future of maritime OT, the paper will touch upon the emerging trends and future challenges, including autonomous ships, IoT risks, and AI-driven cyber threats. Case studies will be presented along with the discussion, illustrating successful cybersecurity implementations in maritime OT as well as lessons learnt from the unsuccessful examples from the sector.

Thus, this study aims to provide a holistic analysis of maritime OT, covering its structure, cybersecurity risks, regulatory challenges, and emerging trends, illustrated by real-world examples of and best practices relevant to the issue. Results from the research will offer valuable insights for shipping companies, port authorities, cybersecurity experts, and policymakers.

Chapter 1: The Maritime Environment and the Role of OT Systems

1.1 Introduction

The maritime industry is a crucial component of global trade. According to estimations of United Nations Conference on Trade and Development, the sector is responsible for transportation of almost 90% of goods worldwide (Al-Enazi et al., 2021). Such a gigantic part in the global economy is only possible to be played by a highly complex conjunction of multiple stakeholders, including shipping companies, port operators, regulatory bodies, and technology providers. All of these stakeholders contribute to the sector's proper functioning, ensuring the seamless movement of cargo, passengers, and energy resources. As it has been historically traced, the operational efficiency and safety of this industry have, until recently, depended on manpower and mechanical systems. As of recently, however, increasing digitalization of the domain, introduced integration of information technologies (IT) into operational ones, profoundly transforming maritime operations.

 https://doi.org/10.26219/heal.aueb.5426

As it has already been briefly mentioned, operational technology (OT) in the maritime industry refers to hardware and software systems that control and monitor physical processes on ships and within port environments (Simola et al., 2024). These processes within vessels and port facilities have become increasingly interconnected, which means that OT has significantly evolved. If only 20 years ago, maritime operations required significant human input, with many equipment components being standalone devices with limited connectivity (Butler et al., 1998), now it includes IoT sensors, AI-driven predictive maintenance, and real-time monitoring, all of which not only significantly improve operational efficiency, but also regulatory compliance.

This chapter explores the global maritime ecosystem. The focus of the discussion will be on the key entities and stakeholders involved. What is more, the role of vessels as the primary component of maritime trade will also be examined. Finally, the evolution of OT from traditional manual operations to digitalized, data-driven processes will be traced.

1.2 The Global Maritime System: Key Entities and Stakeholders

The global maritime industry is composed of various stakeholders, each of which plays a crucial role in ensuring smooth and secure operations. These entities include shipping companies, port authorities, regulatory agencies, classification societies, and technology providers. All of them contribute to the industry's efficiency and cybersecurity.

1.2.1 Key Stakeholders in the Maritime Industry

Shipping companies are the primary drivers of global trade with more than 50,000 merchant vessels operating worldwide (Olsen, 2023), transporting almost 90% of global trade (Al-Enazi et al., 2021). Their responsibility includes owning, operating, and managing fleets that transport goods across international waters. Several of the biggest players in this domain, including Maersk, Mediterranean Shipping Company (MSC), COSCO, and CMA CGM, have already integrated IoT-driven predictive maintenance and real-time vessel monitoring into their operations, all of which brought them significant benefits (e.g. enhanced navigation, increased fuel efficiency, and automated cargo handling), but also exposed them to significant cybersecurity threats (Paridaens & Notteboom, 2022).

Moving on, port operators also are very important in the sphere as they ensure that vessels are efficiently loaded and unloaded. Also, they facilitate logistical and environmental regulations maintenance. With over 3,700 commercial ports operating globally (Rodrigue & Notteboom, 2024), major of them being the Port of Singapore, the Port of Rotterdam, and the Port of Los Angeles have already begun to incorporate such smart technologies, as automated cranes, AI-based traffic management, as well as digital twin simulations in their operations. Just like shipping companies, ports, due to their increasing digitalization, are highly vulnerable to cyber threats. One of the main targets there is critical infrastructure such as container terminal management systems and automated gate controls (Progoulakis et al., 2023).

After that it is crucial to mention cybersecurity organizations, as they develop frameworks for protecting OT infrastructure against cyberattacks. Organizations such as BIMCO, the European Union Agency for Cybersecurity (ENISA), and the U.S. Coast Guard Cyber Command are several of main players in the sphere. They actively contribute to policy formulation, incident response coordination, and the development of cybersecurity best practices. Their role includes addressing emerging threats such as ransomware attacks on shipboard networks, GPS spoofing, and unauthorized access to automated control systems. Classification societies (e.g. Lloyd's Register, Det Norske Veritas (DNV), and the American Bureau of Shipping) enforce technical standards for ship construction, maintenance, and operational safety. Increased digitalization of the industry introduced new factors to be taken into account by the said entities, main of them being cybersecurity resilience assessments (Drazovich et al., 2021). The said standards are developed by international organizations such as the International Maritime Organization (IMO), the International Association of Classification Societies (IACS), and the European Union Maritime Safety Agency (EMSA). These organizations set cybersecurity guidelines, including IMO's Resolution MSC.428(98) etc. to address the growing sophistication in cyber threats (Ngana et al., 2022).

Last but not list stakeholder to be mentioned are technology providers, who play a crucial role in designing and implementing OT solutions, that are to be integrated by

https://doi.org/10.26219/heal.aueb.5426

ship companies and ports. Noteworthy players in the field include Wärtsilä, Kongsberg, and ABB Marine, as they are responsible for provision of cutting-edge shipboard automation systems, cyber risk assessment tools, and AI-driven maintenance analytics. As of recently, the main issue of concern here is the increasing interconnectivity of the mentioned above systems because it introduces new attack surfaces, making cybersecurity measures a top priority for technology providers (Makkonen et al., 2022).

1.2.2 The Importance of Operational Technology in the Maritime Industry

The integration of OT in maritime operations, besides improving efficiency, safety, and regulatory compliance, also introduced new cybersecurity challenges (due to the widespread digitalization). In particular, when speaking of the benefits of modern OT systems, real-time monitoring and automation of vessel operations should be mentioned first as they significantly reduced human errors and optimized cargo handling processes. More specifically, automated cranes, AI-driven vessel traffic management systems, and remote diagnostics contribute to minimizing operational delays and increasing cost-efficiency (Okumus et al., 2023). The adoption of blockchain technology in maritime supply chains has further enhanced transparency, reducing fraud risks and improving data security (Liu et al., 2023). In the Port of Singapore, for example, AI-enhanced scheduling algorithms and predictive maintenance analytics increased the port's operational efficiency to such a degree that it proudly maintains its status as one of the world's most advanced maritime hubs (Sotirov et al., 2024).

What is more, as the maritime industry operates under strict international regulations, OT systems facilitate compliance with frameworks such as the IMO's Ballast Water Management Convention and the MARPOL environmental standards (Kara Balci et al., 2024). OT also facilitates safer and more efficient navigation, with the help of such tools as electronic navigation systems such as the Electronic Chart Display and Information System (ECDIS). Finally, OT is crucial in maintaining environmental regulations. In this, eco-friendly retrofitting technologies are worth to be mentioned as they ensure the transition toward a circular maritime industry (Kolios, 2024).

While OT digitalization has led to operational improvements, it has also expanded the potential for cyberattacks. The increased connectivity of shipboard and portside OT networks makes them susceptible to ransomware attacks, data breaches, and system

https://doi.org/10.26219/heal.aueb.5426

hijacking. A notable incident that illustrates such vulnerability in the cyberattack on Maersk in 2017. It resulted in an estimated loss of $300 million due to disrupted logistics operations, highlighting the urgent need for robust cybersecurity measures (Ahmed et al., 2024). Additionally, IT-OT convergence introduces new risks. This happens because cyber threats targeting IT systems can now compromise operational control systems, which in its turn leads to potential disruptions in navigation, cargo handling, and propulsion systems (Liu et al., 2023).

1.3 Vessels as Critical Components of Maritime Trade and Logistics

Though this paper addresses the maritime industry OT in a broader sense, it is vital to acknowledge that maritime OT discussions often prioritize vessels because they are the primary assets of moving goods and integrating advanced OT systems (Progoulakis et al., 2021, Kapalidis et al., 2022). Ports OT, in the present paper, will be examined within the broader maritime ecosystem, as well as dissected case studies, creating thus a holistic picture of the maritime OT. In the present subchapter, the focus of our attention is on vessels, their function, size, and technological sophistication, with many leveraging advanced OT to enhance navigation, automation, and energy efficiency.

Different vessel types fulfill specific roles within the maritime transportation sector, each integrating various OT systems for better performance and/or increased security. Container ships, which transport large volumes of goods in standardized containers, are equipped with automated cargo stowage systems, real-time remote monitoring, and smart loading/unloading cranes to increase efficiency (Pasha et al., 2021). Tanker ships use leak detection sensors, automated valve control, and ballast water management systems to enhance safety and prevent environmental hazards (Maljković et al., 2022). Bulk carriers utilize real-time cargo weight monitoring and automated loading/unloading systems to maximize efficiency and reduce turnaround times (Kapalidis et al., 2022). Ferries, cruise liners and other passenger ships benefit from such OT as smart navigation, real-time passenger tracking, and Electronic Chart Display and Information Systems (ECDIS) (Chen et al., 2024). Finally, the most recent introduction to the category is the group of autonomous vessels. They represent an embodiment of digital OT integration with fully automated operations. Equipped with

https://doi.org/10.26219/heal.aueb.5426

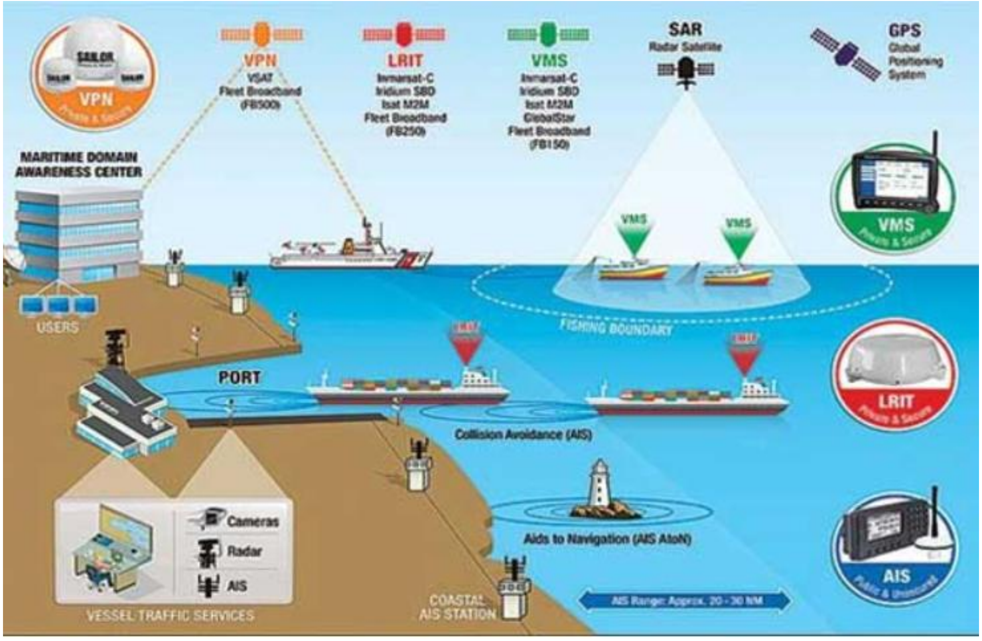
AI-based navigation, predictive maintenance, and cyber-physical security measures to enhance resilience against cybersecurity threats (Riyadh, 2024).

OT components integral to modern ship functions include engine monitoring and control systems, cargo handling automation, Automatic Identification System (AIS) and Electronic Chart Display and Information System (ECDIS). More specifically, ECDS, which is a digital replacement of navigation charts, improves accuracy and situational awareness for vessel operators (Sullivan et al., 2021). AIS provides real-time vessel tracking. It is useful in collision avoidance. Also, it enhanced communication between ships and ports (Progoulakis et al., 2021). Engine monitoring and control systems automate fuel efficiency optimization. They also reduce emissions and improve overall energy consumption (Alghanmi et al., 2024). Finally, cargo handling automation, through the integration of robotics and AI, ensures seamless container movement within ports and onboard vessels. (Pasha et al., 2021). For example, CMA CGM's fleet utilizes Wärtsilä's Smart Marine Ecosystem to optimize fuel efficiency through AI-driven analytics. Machine learning algorithms, employed by the systems, enables predictive maintenance, fuel demand estimation, and proactive decision-making, significantly reducing operational costs and carbon footprints (Alghanmi et al., 2024).

When speaking of OT in vessels, it is also crucial to mention digital twin technologies, used by vessels to simulate and optimize their operations in virtual environments. Digital twins help reducing maintenance costs and increasing sustainability (Werbińska-Wojciechowska et al., 2024). Furthermore, as vessel technology continues to evolve, blockchain-based solutions are also important to mention as they improve supply chain transparency and security. The integration of blockchain into vessel OT ensures tamper-proof data records, enhances cybersecurity resilience, and facilitates efficient cargo tracking (Kapalidis et al., 2022).

https://doi.org/10.26219/heal.aueb.5426

Figure 1: Interconnectedness of Modern Maritime OT (source: Sravani (2023).



1.4 Evolution of Maritime OT: From Manual Operations to Digitalization

The maritime industry has undergone significant digital transformation over the past few decades. Moving from manual operations in the pre-1990's to complex, interconnected digital systems of the present time. Before digitalization became a widespread trend, maritime operations were largely manual. Navigation relied on paper charts and mechanical instruments and communication was limited to radio transmissions (Stoddart, 2022). The risk of human error was high, and vessels lacked real-time monitoring capabilities, making operations less efficient and more vulnerable to accidents (Butler et al. 1998).

The evolution of OT in the maritime sector has been shaped by advancements in automation, AI, and cyber-physical security systems (Kechagias et al., 2022). The first of them was the introduction of GPS and electronic navigation systems, the maritime industry saw the first wave of digital transformation, which significantly enhanced navigational accuracy (Progoulakis et al., 2023). However, legacy systems from this era often lacked robust cybersecurity measures, which still made them susceptible to emerging cyber threats (Stoddart, 2022).

 https://doi.org/10.26219/heal.aueb.5426

After 2010, a shift toward fully integrated smart ship technologies was observed. Modern vessels integrated IT and OT, adopting IoT-enabled sensors, AI-driven predictive maintenance, and real-time fuel optimization systems (Verkoelen, 2022), which in its turn, introduced new vulnerabilities, requiring sophisticated cybersecurity frameworks to protect critical systems (Wilson et al., 2024). Fully autonomous vessels and blockchain-based supply chain solutions signify a new step forward in maritime OT development (Symes et al., 2024), with AI-driven automation, as it is expected, further enhancing operational efficiency. What is more, as of currently, quantum cryptography is being explored as a method for securing maritime communications (Drazovich et al., 2021). However, as vessels become more connected, the potential for cyberattacks on navigation, propulsion, and cargo handling systems increases, necessitating advanced cybersecurity strategies (Wilson et al., 2024).

Such profound transformation had its impact on the role of maritime industry in the global trade. In the Figure 2, it can be seen how transformation the change was, with, as it has been stated by STATISTA, the total volume of goods loaded worldwide increasing from 4 billion tons in 1990 to over 11 billion tons in 2019 (Richter, 2021)

Figure 2: Total Volume of International Maritime Trade: Increase through the years (Source : Richter (2021).

https://doi.org/10.26219/heal.aueb.5426

Despite the numerous benefits of OT digitalization in maritime operations, there are several challenges that must be mentioned. One of the most significant in this respect is the continued reliance on legacy systems that lack modern security features. Many vessels still operate with outdated hardware and software. This makes them easy targets for cyberattacks (Stoddart, 2022). Upgrading these systems is costly and logistically complex, and if not addressed this issue might create gaps in security preparedness (Verkoelen, 2022). What is more, as it has already been mentioned before, the integration of IT and OT (administrative with operational networks controlling navigation, fuel management, and cargo handling) has created more opportunities to taken advantage of by cybercriminals, which may lead to not only to disruption of vessel operations, but also jeopardizing of cargo security, or even endanger human lives (Wilson et al., 2024, Kechagias et al., 2022).

Additionally, regulatory landscape for maritime cybersecurity, as it seems, is lagging the rapid advancement in maritime OT development (Karim, 2022, Drazovich et al., 2021). It is not only the development of regulations per se that is an issue, but also the enforcement mechanisms as well. While organizations such as the International Maritime Organization (IMO) have introduced cybersecurity guidelines, compliance enforcement varies across regions (Progoulakis et al., 2023). Finally, the transition to digitalized maritime operations requires a workforce skilled in OT cybersecurity, but, unfortunately, many maritime professionals seem to lack cybersecurity training (Symes et al., 2024).

Chapter 2: The Cybersecurity Threats in Maritime Operations

Digitalization of the maritime industry impacted the development of OT systems, is increasing their dependence on IT. Such interconnectedness increased the maritime industry's efficiency, automation, and operational control. With it, however, it also increased its exposure to numerous cybersecurity threats, which may lead to financial losses, operational disruptions, and reputational damage. This chapter examines the prevalent cyber threats in maritime operations, and the economic and functional consequences of cyber breaches. Challenges in regulatory frameworks and industry responses to cyber incidents will also be examined as they are essential for, among others, identification of vulnerabilities in maritime OT.

2.1 Common Cyber Threats in Maritime IT and OT SystemsUnlike generic cyber threats, targeted cyberattacks in maritime OT exploit their unique vulnerabilities, targeting real-time control systems, industrial automation, and ship-to-shore communications (Progoulakis et al., 2021). One of the most widespread threats in maritime cybersecurity is ransomware, which is basically a malicious software that is developed by cybercriminals to encrypt critical data and demand ransom payments. If a malicious software is introduced to maritime OT it can compromise systems that control and monitor physical devices and processes on ships, leading to disrupting logistics, delaying cargo movement, and, ultimately, substantial financial losses (Akpan et al., 2022). Ransomware often is introduced to shipboard OT systems via phishing emails, malicious USB devices, or compromised software updates (Ben Farah et al., 2022).

The next types of cyber threat are often referred to as belonging to one group. Though related to one and the same issue (manipulation of navigation systems), they still are different in some ways from one another. They are Global Positioning System (GPS) spoofing and Automatic Identification System (AIS) manipulation. GPS poofing, involves interfering with a vessel's Global Positioning System (GPS) by transmitting false location data, casing the ship's navigation systems to believe it's in a different location. Such manipulation may lead to collisions, groundings, or other accidents. AIS manipulation, in contrast, involves altering the information transmitted by the Automatic Identification System (AIS), a system that allows ships to broadcast their identity, location, and other vital information (Soner et al., 2024). These cyber threats have been increasingly documented in geopolitical conflict zones where adversarial actors attempt to interfere with maritime navigation (de la Peña Zarzuelo, 2021).

Besides those there are also Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) cyberattacks, which overload maritime IT and OT systems with a flood of traffic making unavailable for the original/legitimate users (Kechagias et al., 2022). This type of attack may disrupt navigation, communication channels as well as crucial operational systems such as cargo handling, vessel traffic management, and port security systems (Ben Farah et al., 2022). DoS can occur through rogue or compromised

https://doi.org/10.26219/heal.aueb.5426

IoT/IIoT Devices, which, when insecure, can act as entry points for cyberattacks. Through this, hackers can manipulate fuel sensors, temperature controls, or security cameras, as it happened during the Mirai botnet attack, when compromised IoT devices were to launch massive DDoS attacks (Tushir et al., 2021). What is more, compromised Wi-Fi may lead to cybercriminals intercepting communication between two parties, such as a ship and a shore-based facility. This type of cyberattack is known as Man-in-the-Middle (MITM) attacks, during which is possible not only to intercept but also modify, or even replace the data being transmitted (Aşan, 2023).

Phishing is also a common type of cyberattacks, which aims at tricking individuals into revealing sensitive information. They target crew members and port employees to gain unauthorized access to OT networks, compromising them and controlling them (Haugli-Sandvik, 2024). In maritime context, exploitation of human error may come from fake port/customs agents, who manipulate authorized agents to open infected with malware e-mails, programs, attachments etc. Besides these two, there is also another type of social engineering cyberthreat, which may come from the within of the company. Insider threats insider threats come from employees or contractors who have access to shipboard IT and OT systems. These actors may unknowingly or maliciously facilitate cyberattacks through social engineering tactics, credential theft, or unauthorized system access (Haugli-Sandvik, 2024).

Supply chain cyberattacks are cyber threats introduced through the software of third-party vendors (e.g. hardware providers). This way, malware hidden in legitimate updates can bypass security controls, infecting multiple systems laterally, moving from one system to another. They infiltrate cargo tracking systems, steal sensitive data or cause malfunctions in critical systems, such as propulsion, steering, and safety systems. They can also introduce backdoors for prolonged access because they are hard to detect and remediate among seemingly legitimate components (Odimarha et al., 2024). The 2017 NotPetya attack on Maersk is a perfect example of such an attack, the impact of which caused widespread operational disruptions and economic losses exceeding $300 million (Afenyo & Caesar, 2023).

https://doi.org/10.26219/heal.aueb.5426

Firmware attacks is another type of cyber-attack, threatening maritime OT systems, particularly those relying on satellite communications, navigation, and remote monitoring technologies. Firmware is the embedded software that controls hardware functions. In maritime OT it refers to navigation systems, propulsion controllers, and communication devices, which means that when firmware is compromised, it can lead to attackers being able to disable, manipulate, or destroy shipboard systems without the possibility of remote recovery (Kim et al., 2022).

A combination of cyber and physical attacks poses a significant threat to maritime OT, particularly regarding propulsion control, ballast and power management systems. Their main aim being manipulation of automation processes on ships (e.g. engine power, steering controls, or fuel flow), attackers target the vulnerabilities in SCADA (Supervisory Control and Data Acquisition) and Industrial Control Systems (ICS). Unauthorized access to these systems may lead to catastrophic operational failures (Pfaff, 2022).

2.2 Financial, Operational, and Reputational Impact of Cyber Breaches in Maritime Operations

The financial consequences of cyber breaches in maritime operations are substantial. The impact often spreads over direct monetary losses, legal fees, regulatory fines, and ransomware payments. For instance, the cyberattack on COSCO in 2018 led to significant disruptions in their U.S. operations. Initially, the company attributed the issue to a "local network breakdown". However, evidence suggests it was likely a ransomware attack (Senarak, 2024). The company was forced to forsake the automated processes and manual ones. This increased operational costs, as well as caused delays in shipments, which also had a negative financial effect (Mohsendokht et al., 2024).

Moving onto the discussion of operational consequences, it is important to note that operational downtime caused by cyberattacks affects cargo handling, navigation, and port operations. Analyzing further impact of COSCO cyber incidents, the following aspects can be mentioned. First of all, the attack severely impacted COSCO's U.S. systems, including its website and phone and email systems. This disrupted communication with the company’s customers and partners. Secondly, the already mentioned manual operation caused a strain on the company’s work, as well as global

 https://doi.org/10.26219/heal.aueb.5426

international trade (Baştuğ & Yetgin, 2024). Finally, the resulting from the compromised operating systems paralyze container movement, lead to congestion, revenue loss, and heightened safety risks (Kechagias et al., 2022). Autonomous and AI-driven vessels are particularly vulnerable, as cyberattacks on navigation systems could lead to ship collisions or grounding (Symes et al., 2024).

Beyond financial and operational consequences, cyber incidents significantly erode public trust and damage the reputation of maritime organizations. Turning, yet again, to COSCO cyber incident, it could be said that it negatively impacted the brand image, as it planted a strong concern in customers and other involved stakeholders, regarding their data security and the ability of the company to ensure robust cybersecurity measures (Wang, 2024). What is more, this also increased scrutiny from regulators and insurers (Ashraf et al., 2022). High-profile cybersecurity breaches, such as the attack on COSCO, can also lead to declining stock prices (Edwards et al., 2021), further exacerbating financial instability (Ben Farah et al., 2022).

2.3 Regulatory Failures and Industry Response to Cyber Incidents

Despite the growing cybersecurity threats, regulatory frameworks have struggled to keep pace with evolving risks, leading to gaps in enforcement and compliance, with one of the key reasons for this being rooted in fragmentation of regulatory oversight. In particular, while the International Maritime Organization is actively working in the sphere, introducing relevant cyber regulations (e.g. Resolution MSC. 428 (98) (IMO, 2017) still, the implementation of these guidelines varies significantly across countries. Many operators have yet to fully comply with the mandate (Karim, 2022). In particular, countries which are more economically well off and thus, having more advanced digital infrastructure and a higher level of technological sophistication are more likely to have more robust cybersecurity regulations to protect their critical maritime infrastructure (Afenyo & Caesar, 2023). This inconsistency creates legal ambiguities and hinders effective enforcement.

Furthermore, as it has already been mentioned before, existing regulations often lag behind the rapidly evolving cyber threat landscape (Karim, 2022, Drazovich et al., 2021). Many regulations were developed before the current wave of digitalization and

 https://doi.org/10.26219/heal.aueb.5426

lack specific provisions addressing modern cyber threats, such as ransomware, advanced persistent threats (APTs), and supply chain attacks (Safitra et al., 2023). What is more, there are simply not enough resources and expertise within regulatory bodies to enforce effective oversight and timely investigations (Wang, 2024). Sadly, this gap leaves the industry inadequately-equipped to deal with emerging vulnerabilities and exploit new attack vectors. Finally, IMO guidelines provide broad recommendations rather than specific technical measures, limiting their effectiveness in preventing cyber incidents (Soner et al., 2024) leaving non-compliant operators get away with minimal consequences (Haugli-Sandvik et al., 2024).

In response to the challenges outlined above, the maritime industry is implementing proactive steps to enhance its cybersecurity situation. For example, the International Chamber of Shipping (ICS) and the Global Industry Alliance (GIA) are developing and promoting cybersecurity guidelines for the industry (Afenyo & Caesar, 2023). These initiatives aim to create and promote the culture of cybersecurity awareness among the industry stakeholders, encouraging their voluntary adoption of comprehensive security measures, such as multi-layered defense systems, AI-powered threat detection, and Zero Trust security models to mitigate cyber risks (Akpan et al., 2022).

Cybersecurity investments are another important trend. Shipping companies are investing in cybersecurity technologies, such as intrusion detection systems, firewalls, and anti-malware software, as well as working on the development of access and monitoring measures. They are also implementing robust access control measures and conducting regular security audits and penetration testing (Kechagias et al, 2020). In addition to the above, training programs are being developed to educate crew members, engineers, and other personnel on cybersecurity threats and best practices. This includes raising awareness about the increasingly more sophisticated social engineering tactics, and the importance of strong encryption methods (Dave et al., 2023).

The development of robust cyber risk insurance measures to mitigate financial exposure is another important step in fostering cybersecurity culture in the sector. Insurers are now offering specialized policies tailored to the specific needs of maritime industry. Parametric insurance policies covering losses from cyberattacks, business interruptions, and data breaches are being key trends in the sphere (Mohsendokht et al., 2024).

https://doi.org/10.26219/heal.aueb.5426

However, the effectiveness of such policies depends on accurate risk assessments and proactive cybersecurity measures by insured parties.

Chapter 3: Understanding Maritime OT Systems and Their Security Challenges

3.1. Overview of OT in Maritime Operations (ECDIS, Engine Control, Cargo Handling, Fuel Management)

Operational technology in maritime operations enables automation of various working processes, including real-time monitoring, and optimization of various shipboard and portside activities. As the said industry is responsible for approximately 90% of global trade transportation (Al-Enazi et al., 2021), the seamless integration of OT into its critical systems is essential for efficiency, safety, and regulatory compliance. This section provides an in-depth examination of key OT components in maritime operations, with the main focus on electronic chart display and information systems (ECDIS), engine control systems, cargo handling automation, and fuel management technologies. These elements collectively enhance navigational accuracy, operational efficiency, and environmental sustainability. Besides the advantages that automation of these systems brings, cybersecurity and maintenance challenges will be discussed as well.

3.1.1. Electronic Chart Display and Information System (ECDIS)

Electronic Chart Display and Information System is a vital element of modern maritime navigation as it plays a key role in ensuring the safety of navigation, optimizing routes and reducing operating costs. This happens because of the integration with the Global Navigation Satellite System (GPS) and the Automatic Identification System (AIS). It is with the help of these technologies that ECDIS enables real-time position tracking, as well as reduction of potential navigation errors due to the human factor (Kayisoglu et al., 2022).

Another technological advancement of ECDIS is automatic route optimization, enabled through advanced calculation algorithms. They allow for precise analysis of

https://doi.org/10.26219/heal.aueb.5426

meteorological conditions, shipping restrictions and water features, and suggest the safest and most efficient route. Such automatization not only increases the safety of the vessel, but also reduces fuel consumption. In the long term this also leads to both significant reduction in operating costs and environmental benefits. In addition, ECDIS integrates with other ship systems, (e.g. radars, weather services, engine management systems, etc.), which is highly convenient and increases the situational awareness of the crew (Kechagias et al., 2022).

Despite the obvious advantages, there are also a number of vulnerabilities and challenges associated with ECDIS operation, with the main of them being cybersecurity threat (e.g. GPS signal spoofing, data manipulation etc.). Consequences of these threats being actualized include changing the ship's course and even collisions (Kayişoğlu, et al., 2024). In addition, the use of this technology requires regular software updates, in line with standards set by the International Maritime Organization (IMO). Failure to comply with these standards has serious consequences, including loss of certificates and administrative sanctions (Neumann, 2024).

Finally, the need for high-quality crew training should also be mentioned as despite the automation of navigation processes, potential inconsistencies in human work (e.g. incorrect interpretation of data or insufficient understanding of ECDIS functionality) must be accounted for too, as they might cause serious navigation errors. Personnel training programs is one of the most effective strategy to mitigate these risks as it enables providing them with up-to-date knowledge of the system's operation and possible threats (Kayisoglu et al., 2022).

3.1.2. Engine Control and Automation Systems

Modern ships are equipped with advanced engine control and automation systems, main benefits of which include optimization of fuel consumption, reduction of harmful emissions, and overall increase of the ship's power plant efficiency. By continuously monitoring engine parameters in real time and automatically adjusting operating modes, these systems increase vessels' performance all while meeting environmental standards. All of these benefits are achieved through integration of sensors and intelligent algorithms into engine systems, which enable real-time diagnostics (Yu et

 https://doi.org/10.26219/heal.aueb.5426

al., 2021). Installed sensors monitor fuel consumption, engine temperature, and emissions, ensuring compliance with international environmental regulations such as MARPOL (Neumann, 2024). Predictive maintenance systems, based on artificial intelligence, are also crucial as they analyze equipment condition data and detect early signs of wear, helping prevent sudden breakdowns and reduce repair costs (Durlik et al., 2023). Finally, remote monitoring and control of a ship's engine should also be mentioned as it allows shore operators to track the vessel's operation in real time and promptly respond to possible malfunctions, increasing the efficiency of maintenance (Mellqvist & Jacobo, 2021).

With it, engine control systems are also vulnerable to cybersecurity threats and operational risks. In particular, integration with the ship's IT networks means that any failure in the automated engine control systems can lead to serious consequences, including loss of control of the vessel. What is more, strict compliance with IMO and classification societies requires constant software updates and maintenance. Thus, to ensure effectiveness of these technologies, a comprehensive approach to their maintenance is a must. This includes ensuring reliable cybersecurity measures, strict monitoring of technical condition and professional training of the crew (Neumann, 2024).

3.1.3. Cargo Handling Automation

Cargo handling systems, both onboard ships and in ports, are also exhibiting a remarkable digitalization with the integration of various types of robotics (equipped with sensors of diverse manner), artificial intelligence, and IoT technology to improve efficiency and safety.

One of the key examples of such is the introduction of automated cranes and forklifts, which reduces human intervention. Reduction of manforce leads to increased operational efficiency due to the minimization of the risk of accidents and reduction of vessel turnaround times at ports (Kuznetsov et al., 2021). Smart container tracking is another example of digital automatization. Enabled through IoT devices, this technology provides real-time data on cargo status, including temperature and humidity, which is very important for sensitive cargo like perishable goods (Bauk & Dzankic,

https://doi.org/10.26219/heal.aueb.5426

2024). Blockchain integration is also a valuable addition to improving supply chain security by preventing data tampering and providing transparency in cargo documentation (Elmay et al., 2021).

Challenges and risks of automation in cargo handling system include also cyberthreats vulnerabilities, which can lead to operational failures and financial losses due to hacker attacks (Elmay et al., 2021). What is more, there are also compatibility issues, which may arise when integrating legacy port infrastructure with modern digital systems (Merz et al., 2023). Mitigation of this particular challenge requires significant upgrades (Makkonen et al., 2022). What is more, differences jurisdictions regarding various shipping and safety regulations are also an issue that standardization difficult (Gattuso, D., & Pellicanò, D. S., 2023). Thus, automation of cargo handling, while opening new prospects for improving the efficiency and safety of maritime transport, still poses some challenges and thus requires a comprehensive approach for full potential of it to be enjoyed (Bauk & Dzankic, 2024)

3.1.4. Management Systems

Fuel consumption is a critical aspect of maritime operations, not only because it accounts for operational costs, but also due to the regulatory demands. Thus, the integration of advanced fuel management technologies has become essential for maritime operation optimization. In this respect automated fuel monitoring, utilizing sensors to track fuel consumption in real-time should be mentioned. Allowing for precise monitoring of fuel usage, this technology provides operators with up-to-date information (e.g. inefficiencies identification) valuable for optimization of efficiency. (Yan et al., 2021). As these systems can be integrated with other onboard technologies, they can also enhance overall operational performance and reduce costs (Aakko-Saksa et al., 2023).

Another factor worth mentioning is artificial intelligence (AI) and machine learning, used in fuel consumption patterns analysis. Data on weather conditions, sea state, vessel speed etc., are processed by AI algorithms, predicting fuel needs with utmost accuracy, and, subsequently, enabling for more efficient speed and course adjustment in real-time

(Zhang et al., 2024) ultimately leading to cost savings and reduced environmental impact.

In continuation of the environmental line of discussion, emission reduction technologies, such as advanced filtration and fuel-blending techniques should also be mentioned. These technologies play a critical role in ensuring compliance with evolving environmental regulations and improving the industry's sustainability (Aakko-Saksa et al., 2023).

Among challenges, associated with the integration of more advanced fuel management systems cybersecurity vulnerabilities should be mentioned. Because of the increased reliance on remote access and data connectivity, digital platforms for fuel monitoring and optimization might expose vessels to potential cyberattacks (e.g. data breaches, manipulation of fuel supply metrics etc.) (Śliwiński & Piesik, 2019). What is more, regulatory compliance also is challenging, particularly in the view of the growing more and more stringent emission reduction targets. This means that vessels must constantly adapt their systems to remain compliant, which often necessitates substantial investment in new technologies, crew education and training etc. (Yan et al., 2021).

Upon analyzing all the said above information, it could be concluded that the integration of OT with IT not only has revolutionized maritime operations through enabling real-time data collection, predictive maintenance, and enhanced automation, but also exposes maritime infrastructure to an expanded cyber threat landscape.

In particular, the advantages of the IT-OT convergence include enhanced operational efficiency, predictive maintenance benefits with the subsequent cost reduction and improved safety and regulatory compliance (Kechagias et al., 2022) as well as significant environmental benefits (Progoulakis et al., 2023). For example, such aspects of maritime operations as communication is very much improved because of the IT-OT integration resulting in optimized fleet management, reduced downtime, and improved vessel turnaround times (Skok et al., 2024). Predictive maintenance, as another example, can help reduce unexpected failures and, yet again, costly downtime. Machine learning algorithms in this sphere has become a most invaluable component of digitized

https://doi.org/10.26219/heal.aueb.5426

operation as by analyzing historical data from engine monitoring systems it predicts vessels' parts wear and schedule proactive maintenance, which is crucial for preventing breakdowns (Molęda et al., 2023). Such pro-active culture in the operation fosters not only operational safety but also compliance with regulatory standards (e.g. with IMO's MARPOL Annex VI standards in regards to the emission rates) (Simola et al., 2024). Finally, remote access and increased autonomy in operation is another benefit of IT-OT integration that not only is beneficial, but also sets a trend for future operational standards. As it has been seen from the industry practice, automated navigation, collision avoidance systems, and AI-driven fuel optimization with the reduced reliance on men work-force and increased reliability, made it possible for autonomous ships to become part of world fleet (Munim et al. 2022).

Despite the operational benefits, there are also cybersecurity challenges associated with IT-OT convergence. First of all, there is expanded cyber risk, which did not exist with the traditional OT systems. These include not only cyberattacks, ransomware, unauthorized access risk (Ben Farah et al., 2022), with all the physical security consequences, such as vessel hijacking, cargo theft, or environmental disasters (Soner et al., 2024) and supply chain vulnerability (Odimarha et al., 2024).

3.2. Critical OT Components and Their Vulnerabilities

Maritime operations depend on a range of OT systems to manage navigation, propulsion, cargo handling, and environmental monitoring and each of them have their vulnerable points, that threaten their security and reliability.

As it has already been mentioned above, ECDIS is crucial for modern maritime navigation. Because it is integrated with GPS, AIS, and radar, ECDIS becomes vulnerable to cyberattacks and data manipulation**.** As GPS signals are susceptible to spoofing attacks, it makes ECDIS a target for malignant manipulation regarding data on vessel positions. Consequences of such negative manipulation may be navigational errors or collisions (Durlik et al., 2023). What is more, as many vessels operate outdated ECDIS software, insufficient security updates might lead to malware infections and unauthorized access (Neumann, 2024). Also, besides cybersecurity issues, there are

https://doi.org/10.26219/heal.aueb.5426

also technical issues related to redundancy might occur. Specifically, failure in the ECDIS system (e.g. software glitch) can result in a complete loss of navigational capability. Thus, it is highly important to provide adequate back up such as regular software maintenance and update is necessary to avoid the risk of accidents (Visky et al., 2024).

In the engine control and automation systems there is a threat of remote exploits and unauthorized access in case authentication protocols are weak or insufficient. This may lead to cyberattacks targeting engine automation, which may lead to propulsion failure or manipulation of fuel systems (Progoulakis et al., 2023). What is more, as modern shipping companies often utilize fleet management systems, which enable centralized monitoring, data exchange, and remote control of certain functions, they expand cyberattack surface and in case malware infections occur, they spread across multiple vessels (Setiawan et al., 2024).

Cargo handling systems, as they involve port operations, in their vulnerability, might jeopardize the entire supply chain. Potential issues may arise in the following areas. First of all, there is the possibility of hacking of automated cranes which may lead to disruption of loading and unloading processes, delaying supply chains and causing economic losses (Weaver et al., 2022). Also, as cargo tracking systems rely on IoT sensors, in case of insufficient encryption, there could be data breaches and location spoofing, leading to cargo loss due to theft/misplacement and subsequent delays or even lost shipments, and increased costs for businesses (Ashraf et al., 2022). Finally, with the increasingly fast technological development, there are often interoperability issues with the existing infrastructure being unable to adopt modern digital systems. Issues like hardware and software incompatibility, proprietary systems and connectivity limitations, and even integration costs might stand in the way of new technology integration, not only hindering optimization of operations per se, but also leaving significant gaps in cybersecurity of maritime operations (Papastergiou et al., 2021).

Fuel management vulnerabilities may have both economic, environmental and human safety implications. More specifically, remote fuel management should have highly secured access points otherwise, without adequate authentication protocols (e.g. multi-

https://doi.org/10.26219/heal.aueb.5426

factor authentication, encryption etc.) such issues as manipulation of fuel consumption data, fuel efficiency, or even automated fuel controls may occur potentially leading to significant financial losses for shipping companies. In worst case scenarios involve fuel theft or fraudulent billing (Dimakopoulou & Rantos, 2024). Besides economic consequences, cyber vulnerabilities in fuel management systems also may result in regulatory compliance risks. In accordance with international maritime regulations, ships must maintain accurate records of fuel consumption and emissions. If due to cyberattacks, data of a vessel's fuel management system are compromised it may result in severe penalties for shipowners/operators, which may include fines, loss of operational licenses, and increased regulatory scrutiny (Neumann, 2024). Finally, safety risks could also be an issue with the compromised fuel management system as in extreme cases, there could be engine failures, power loss, or even hazardous situations such as collisions due to loss of propulsion (Stoumpos et al., 2022).

Chapter 4: Cybersecurity Standards and Regulations for Maritime OT

4.1. IEC 62443 and Its Relevance to Maritime OT

IEC 62443 is a set of cybersecurity standards Developed by the International Electrotechnical Commission (IEC) to address the security of industrial automation and control systems (IACS), IEC 62443 consists of several parts, each addressing different aspects of cybersecurity for IACS, including general requirements, policies and procedures, system-level security, and component-level security. The standard is built upon the principles of deep defense (involving multiple layers of security control), risk-based security management, which ensures that vulnerabilities are identified and mitigated based on their potential impact, and role-based access control, limiting unauthorized access to critical systems (Leander et al., 2019).

As it has already been mentioned, the maritime industry heavily relies on OT systems to support various operational aspects, including navigation, propulsion control, cargo management, as well as port logistics. Due to the integration of IT in maritime OT, they

 https://doi.org/10.26219/heal.aueb.5426

are susceptible to cyber threats, which makes IEC 62443 highly applicable for ensuring operational security and efficiency. In particular, IEC 62443 provides a framework for identifying and mitigating various cybersecurity risks through security development lifecycle processes, risk assessments, and continuous monitoring (TÜV SÜD, 2021).

There are several important introductions, made by IEC 62443, for mitigation of cybersecurity risks problem. First of them is the concept of security zones which involves segmenting OT networks into defined areas in accordance with each zone's security requirements and risk levels. As IT-OT convergence presupposes interconnectedness of systems, security zones, maritime operators can limit the impact of cyber incidents. Communication between security zones is ensured through conduits, which enforce access controls and ensure data integrity (Śliwiński & Piesik, 2019). In line with IEC 62443, there are multiple steps that should be taken for ensuring cybersecurity in maritime OT, which start with security risk assessments, definition of security policies, and integration of cybersecurity measures into the OT lifecycle (Verkoelen, 2022). This means that in line with IEC 62443-3-3 system security requirements, role-based access control (RBAC) should be implemented to prevent unauthorized personnel from manipulating key ship functions such as autonomous navigation or ballast water management systems. Integrating the Perdue Model into implementation of this requirement ensures that lower-level PLCs and sensors do not have direct internet connectivity (preventing cyber intrusions), while also limiting external access to fleet-wide ship management systems through designated demilitarized Zones (TÜV SÜD, 2021).

Another important aspect of IEC 62443 is that it helps establish Security Levels (SLs) according to potential threats, which may range from casual (at SL1) to significant (e.g. sophisticated, state-sponsored cyber threats) with SL4 (Progoulakis et al.,2021). Additionally, in line with IEC 62443, design and deploying OT systems should align with security development lifecycle (SDL), which includes security threat modeling, secure coding practices, rigorous testing, regular security updates and, secured identity and access management (IAM) solutions. The latter ensurs that only authorized personnel can access sensitive control systems. Finally, IEC 62443 also requires

https://doi.org/10.26219/heal.aueb.5426

continuous security monitoring, development of incident response mechanisms and regular cybersecurity training for the staff (crew members and shore-based personnel included) (Kavallieratos et al., 2020).

Maritime operators often use the Perdue Model as a guideline when they want to implement the IEC62443 standards as it offers a highly useful and handy map of the maritime OT industrial control system (ICS) network. Belev (2022) highlights the value of the Perdue model used to implement IEC 62443 in shipping control systems to segment and secure OT networks aboard vessels and in ports as it ensures hierarchical cybersecurity and functional isolation of shipboard OT systems. Application of the Perdue model allows for effective separation of core vessel control functions from administrative and external IT networks, preventing unauthorized access, reducing attack surfaces, as well as enhancing monitoring of shipboard automation systems.

More specifically, shipboard OT systems can be mapped to the six-layer Purdue Model, with each of them corresponding to specific ship control systems. The core ship operations components directly interacting with the vessel's physical processes, including sensors, actuators, propulsion systems, ballast control, and fuel monitoring, in this hierarchy will be positioned at Level 0. At Level 1 systems that manage ship automation and execute control commands are positioned. These include Control, comprises the Programmable Logic Controllers (PLCs) (responsible for fuel injection timing and cargo crane automation), engine automation, and navigation control. Level 2 will be responsible for PLC supervision operations and safety mechanisms. They will include Supervisory Control and Data Acquisition (SCADA) systems, engine monitoring systems, and alarm systems. Critical shipboard OT networks positioned on these lower levels are isolated from upper ones (from 3 and up) with firewalls and air-gapped configurations. High-level monitoring and decision-making (e.g. cargo weight distribution optimization via the SMS) will be positioned at Level 3, while Level 4 will host the business network, connecting through IT-OT interface (including shore-based fleet management and remote condition monitoring) the vessel with the shipping company. Finally, at the highest fifth level, responsible for strategic business decisions and global fleet operations, the Enterprise IT is positioned. Comprised of Maritime Logistics, Cloud-based Predictive Maintenance, and Regulatory Compliance Systems,

https://doi.org/10.26219/heal.aueb.5426

this level represents the highest point in the hierarchy, as all the information from the lower levels is directed up here to further be used in the global decision-making (Belev, 2022, TÜV SÜD, 2021).

Such hierarchical segmentation ensures that only authorized traffic is allowed between Purdue levels, safeguarding the entire network of a maritime operator from being overwhelmed by a potential cyberattack (Belev, 2022). This means that not only the low-level malware entrance is confined in the said segment, but also that the external sources cannot overwrite critical OT data. This protection is ensured by data diodes, which restrict communication between the levels to a one-way direction (Onshous et al., 2022).

While IEC 62443 provides a comprehensive cybersecurity framework, it is not without its limitations, with one of the major ones related to the challenges it poses in implementation of older infrastructures lacking modern security features. As retrofitting such systems requires substantial investment, both in terms of financial resources and technical expertise, they find it hard to comply with IEC 62443. Another challenge is the lack of standardized cybersecurity regulations across the maritime industry, with guidelines introduced by the International Maritime Organization (IMO) and the International Association of Classification Societies (IACS) not always aligning with IEC 62443 requirements. This has significant implication for compliance among shipowners and port operators. Finally, there are issues with interoperability when implementing IEC 62443 due to the complexity of maritime OT ecosystems, which differ in security protocols and vulnerabilities. This means that it is highly difficult to ensure consistency of security practices across various systems without coordinated efforts among stakeholders, including shipbuilders, equipment manufacturers, and cybersecurity (Simola et al., 2024).

Despite the said limitations, IEC 62443's and the Perdue Model's structured security framework offer invaluable advantages for security of maritime OT. With technological advancement in the sphere, integration of global strategies, like AI-driven threat detection, blockchain for secure data exchange, and zero-trust security models (Jhanjhi & Shah, 2024), as well as lesser ones, such as virtual patching with external firewalls

https://doi.org/10.26219/heal.aueb.5426

(Belev et al., 2022) implementation of IEC 62443's principles in maritime OT is expected to become less challenging, enhancing OT's defenses against evolving cyber threats (Progoulakis et al,. 2023).

4.2. International Maritime Organization (IMO) Guidelines

The International Maritime Organization (IMO) plays a fundamental role in establishing global safety and risk management standards for the maritime industry, including the aspects related to cybersecurity. The guidelines developed by the IMO integrate cybersecurity measures into existing safety and risk management frameworks, support shipping companies, port operators, and regulatory authorities in mitigating cyber risks and enhancing the resilience of maritime operations. The key guidelines include IMO Resolution MSC.428(98) on maritime cyber risk management, and the IMO's International Safety Management (ISM).

The IMO's International Safety Management (ISM), being a mandatory international regulation adopted under Chapter IX of the SOLAS Convention, provides a structured framework for the safe operation of ships and pollution prevention. With the introduction of the Resolution MSC.428(98) (which will be discussed later), cyber risk management becomes integrated into the ISM Code. The ISM code requires ship operators to develop a Safety Management System, which must include risk assessment procedures to identify and mitigate operational hazards, incident response plans for emergencies, crew training programs to ensure compliance with safety protocols and continuous improvement through audits and reviews. The ISM Code is enforceable. This means that maritime organizations operating ships and vessels must comply with it to obtain and maintain their Safety Management Certificate (SMC) and Document of Compliance (DOC), which necessary for legal operation (Tjahjono & Gemilang, 2023).

This strengthens maritime safety and operational resilience through several critical steps: risk identification through vessels and ports operational vulnerability assessments, risk mitigation through network segmentation, multi-factor authentication, and real-time monitoring of cyber threats and crew training and awareness programs implementation. Also, a crucial part of ISM code is the

https://doi.org/10.26219/heal.aueb.5426

development of incident response planning with provisions for procedures for detecting, responding to, and recovering from cyber incidents. Finally, ISM code also demands the industry representative to provide compliance audits and continuous improvement initiatives to adapt to evolving threats and regulatory changes (Verkoelen, 2022). The approach to cybersecurity that the ISM Code adopts ensures that cyber threats are addressed as operational risks and not just purely technical concerns, thus promoting cybersecurity practices to be integrated into daily ship operations (Rinaldy, 2022).

In regards with the IMO Resolution MSC.428(98), the following should be said. First of all, it emphasizes proactive measures to safeguard critical shipboard and portside infrastructure because it perceives cyber risk management as an integral part of existing safety protocols. With it, however, while mandating the integration of cyber risk management into the ISM Code and demanding documented compliance evidence during audits, the Resolution MSC.428(98) still lacks specific enforcement measures. To address these inconsistencies, some flag states (e.g. the USA) have introduced additional national cybersecurity regulations, complementing IMO requirements. Others, however, did not proceed with such additional measures. Such discrepancy creates disparities in how maritime cybersecurity is managed globally. What is more, despite the fact that the resolution also aligns with other cybersecurity frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001, which could enhance the universal nature of the signified by its provisions approach to maritime cyber resilience (Martínez et al., 2024), still the inconsistencies result in limited fulfilment of its potential. Finally, since MSC.428(98) does not impose penalties for non-compliance, enforcement remains weak and inconsistent across the industry (Fenton & Chapsos, 2023). Some suggest that stronger auditing and additional enforcement of penalties for non-compliance could enhance the effectiveness of IMO’s cybersecurity mandate (Kanwal et al., 2024).

In line with the IMO guidelines, cybersecurity strategies should include five functional elements for cyber risk management (Identification, Protection, Detection, Response and Recovery) (Rajaram et al., 2022). The first element, Identification, involves an asset

https://doi.org/10.26219/heal.aueb.5426

examination to determine which IT and OT systems require protection. The results of this examination are analyzed focusing on risk assessments to prioritize cybersecurity investments. The second element, Protection, requires implementing security measures (e.g. firewalls, intrusion detection systems, endpoint security solutions etc.) (Kathayat, 2022) to ensure that access control mechanisms prevent unauthorized access to critical maritime infrastructure. The third element, Detection, introduce continuous monitoring and anomaly detection systems to identify suspicious activities in real time. The fourth element, Response, involves developing incident response plans for procedures that could mitigate cyberattacks, as well as cybersecurity drills to ensure crew preparedness. The fifth and final element, Recovery, focuses on implementing disaster recovery solutions (e.g. data backup) to restore systems in case of a cyberattack, as well as to update risk management policies to prevent future breaches (Rajaram et al., 2022).

The NotPetya ransomware attack on Maersk, can be used as an example of inadequate asset identification and inventory management in maritime OT and IT networks. The incident was caused by a rapid spread of the malware, which entered Maersk's global network during the update of a tax software, installed on Maersk's administrative IT systems, resulting in disruption of port operations, ship scheduling, and logistics tracking. This shows that critical shipboard and port systems lacked proper segmentation, allowing the malware to spread uncontrollably (Jhanjhi & Shah, 2024). Another example of the highest relevance of the 5-element framework that the IMO demands from maritime operators is the prolonged cyberattack on the terminal operation system of port of Antwerp, leading to criminals taking advantage of the port's infrastructure to smuggle drugs. The incident was discovered by chance, when a minor anomaly regarding a container displacement was observed. After that, a security information and event management system with intrusion detection and a behavioral analytics tool was installed to analyze traffic logs, login attempts, and container handling patterns, which eventually detected the unauthorized database access (May & Holcova, 2023).

4.3. IACS Unified Requirements (UR) E26 and E27

https://doi.org/10.26219/heal.aueb.5426

Next in our discussion of guidelines, fostering cybersecurity resilience in the maritime industry are Unified Requirements (UR) E26 and E27 developed by the International Association of Classification Societies (IACS), responding to growing concerns about the vulnerability of shipboard systems to cyber threats. Also, UR E26 and E27 respond to the increase of regulatory expectations from the IMO, IEC 62443, and the EU's NIS2 Directive, aiming to enhance cyber resilience of ships by ensuring that digital systems onboard are protected against cyber threats, to integrate cybersecurity measures into ship design, operations, and maintenance and, finally, to ensure compliance with global cybersecurity frameworks by providing structured guidelines for shipowners, operators, and classification societies (IACS, 2023a, b).

In respect to UR E26, it should be said that it focuses on cyber resilience of shipboard systems helping them develop solid protection against unauthorized access and cyberattacks through mandatory integration of security measures such as intrusion detection systems, secure authentication mechanisms, and robust communication protocols. UR E26 is all about protection of onboard digital systems of vessels and maintenance of operational integrity throughout a ship's lifecycle (IACS, 2023 b). UR E27 expands the area of concern, including operational networks into the cybersecurity focus. For it, UR E27 requires implementing risk assessment methodologies, continuous monitoring, and network segmentation hardening techniques so that vessels were protected from potential cyber threats. What is more, UR E27 provisions for incident response & recovery planning, which include backup systems, emergency shutdown protocols, and post-incident investigations (IACS, 2023 a).

A lifecycle approach to cybersecurity is a must and thus should be incorporated from the design phase through to operational deployment (Ungureanu et al., 2024). Combined provisions of UR E26 and E27 ensure that cyber risk management is embedded into ship design, operation, and maintenance, influencing both ship design and daily operational procedures (Kayisoglu et al., 2024). In particular, in line with the provisions of UR E26 and E27, shipbuilders must integrate cybersecurity measures during vessel design, including, accounting for network segmentation architecture (isolating IT-OT networks), secure hardware installations (tamper-proof communication systems) and pre-installed cybersecurity software (firewalls, endpoint

https://doi.org/10.26219/heal.aueb.5426

protection). What is more, new ships must undergo cybersecurity risk assessments before classification societies grant certification. In respect to operational security, ship operators must conduct mandatory cybersecurity training for all personnel, regular vulnerability scanning and penetration testing, strict access control enforcement (e.g., disabling default passwords) and routine software updates and patching schedules. Finally, mandatory cyber incident response plans must ensure automated backups and failover systems, emergency shutdown procedures in case of cyberattack and immediate reporting to classification societies (IACS, 2023, a, b). Implementation of a risk-based cybersecurity framework, on the other hand is not mandatory, but is encouraged, as cyber risk assessments, response plans and personnel cybersecurity training are all key aspects of pro-active protection against cyberthreats (Verkoelen, 2022).

Classification societies like DNV, Lloyd's Register, and ABS ensure that vessels meet cybersecurity requirements before certification, enforcing the vessels undergo cyber risk assessment (for newly built ships) and regular cybersecurity audits for all, as well as provide verification of OT security compliance in accordance with IACS UR standards, with E26 and E27, being among top priority ones. The provided certification establishing the security of vessels in accordance with the level of robustness of their cybersecurity controls (DNV, 2024). For example, In July 2020, ClassNK, a leading classification society, released the second edition of its Guidelines for the Design of Cybersecurity on Board Ships for Newbuilds, intended for shipyards and shipowners. The publication defines controls and a framework for implementing such controls, which have been supplemented by the IEC62443 series of international cybersecurity standards for industrial control systems and the latest recommendations on cyber resilience for new ships published by IACS. In addition, ClassNK introduced requirements for the addition of class notations to classification codes related to cybersecurity. The guide also includes current best practices for shipyards and shipowners in identifying computer systems that should be protected from cyber incidents and building networks to protect them. Just recently, the classification society Korean Register of Shipping carried out the world's first cyber security class assignment (CS Ready) to a large gas carrier, after completing documentary and field inspections.

https://doi.org/10.26219/heal.aueb.5426

The CS Ready class is assigned to newly built ships and requires successful completion of 49 inspection points in a total of 12 categories, including risk and asset management, cyber incident response and recovery. The Korean Register of Shipping also provides maritime cyber security certification for a company or vessel with a cyber security management system. Cybersecurity compliance for a company or an existing vessel is divided into three levels (CS1, CS2 and CS3) according to cybersecurity maturity and consists of 35 zones and 144 inspection points. In addition, KR conducts cybersecurity compliance equipment inspections (Fukuto, 2021, Kim et al. 2022).

4.4. The European Union's NIS2 Directive and Global Regulations

NIS2 directive builds upon the NIS (original directive) expanding its scope and strengthening its security measures. With strict reporting and collaboration demands NIS2 is to ensure that maritime entities remain resilient against cyber threats that could disrupt important maritime domains such as port operations, vessel management, and maritime logistics (Singh, 2023).

NIS2 directly impacts not only large shipping firms (like it was mandated previously by NIS) but also mid-sized operators, including port authorities, shipping companies, and logistics providers within the EU, (Avramidou et al., 2023), legally binding them to comply with its cybersecurity measures (Progoulakis et al., 2023). In particular, the directive requires all the said entities to implement risk-based approach, with cybersecurity risk assessments to identify vulnerabilities in their IT and OT systems. What is more, it also mandates strict reporting obligations (with major incidents being firstly reported within 24 hours, and then secondly within maximum of 72 hours of the occurrence to the relevant authorities), as well as business continuity and disaster recovery plans provision, to enhance threat detection and response. Moreover, it also enforces mandatory cybersecurity measures. Incident response planning, network segmentation, and data protection strategies are all part of mandatory cybersecurity requirements of NIS2. A critical aspect of NIS2 is its emphasis on board-level accountability. This part ensures that executive management actively participates in cybersecurity governance and decision-making processes (Ruohonen, 2024).

https://doi.org/10.26219/heal.aueb.5426

While directly affecting multiple stakeholders, NIS2 also focuses on the entire supply chain security. In this, NIS 2 requires maritime operators to provide cybersecurity assessment of third-party vendors and external IT/OT service providers. Post-incident analysis with forensic investigations and detailed mitigation reports are also part of mandatory cybersecurity actions. Non-compliance with NIS2 requirements carries penalties, which besides substantial financial costs also imply increased regulatory scrutiny (Singh, 2023).

Within the EU, the directive fosters international cooperation and information sharing through initiatives such as the EU Cybersecurity Incident Response Teams (CSIRTs) (Nowikowska, 2022). The initiative facilitates the exchange of threat intelligence and coordinate responses to cyber incidents in maritime infrastructure. To promote further collaboration and continuous learning, NIS2 mandates that maritime operators participate in cross-sector information-sharing forums. As maritime trade is largely international, the directive also influences cybersecurity practices beyond the EU (Progoulakis et al, 2023) forging partnerships with other stakeholders, including the IMO, the IACS and other non-EU maritime authorities. These cooperative measures enhance the global maritime sector’s ability to detect, prevent, and mitigate cyber threats while promoting regulatory harmonization (Ruohonen, 2024).

However, despite all of this, there are some uncertainties in regulatory alignment with maritime standards such as IMO MSC.428(98) and IACS UR E26/E27. In particular, the provision of the Article 2(6) of NIS2 stating that sector-specific laws are to be applied if these laws’ security requirements are "at least equivalent" to NIS2 are highly confusing because without clear definition of what constitute the equivalency, the exact scope of the law’s application remains uncertain. This means that there are bound to be potential gaps in cybersecurity of maritime operators particularly for vessels operating under weaker cybersecurity frameworks such as older IMO MSC.428(98) (Avramidou et al., 2023).

What is more, there is a certain clash between the theoretical applicability and the practicality of NIS2. In theory NIS2 applies to critical infrastructure, essential service providers. Passenger ships and European port organizations are also within the NIS2 scope. In practice, however, its impact on the commercial shipping industry (which is

https://doi.org/10.26219/heal.aueb.5426

a major player not only in the industry but in the worldwide economics (Al-Enazi et al., 2021) is somewhat limited due to the jurisdiction issues because many commercial cargo vessels are registered under non-EU flags of convenience (e.g., Panama, Liberia, Marshall Islands). This means they are not subject to EU regulations like NIS2 (IIcus, 2023). Also, due to the highly fragmented nature of maritime industry, different entities might be responsible for management of vessels, cargo, and IT systems and thus do it separately. This fragmented structure complicates even more direct enforcement of NIS2 on individual cargo ships. Finally, there is the issue of the limitation regarding the targeting scope of the NIS2 applicability (medium and large maritime enterprises) as the directive does not provide clear guideline for the size categorization. If one take into account specific provisions regarding smaller ports being treated as essential but high-security-risk entities or the one regarding the demands that EU cargoes pose, this size-related uncertainty of NIS2 complicates cybersecurity compliance even more (Avramidou et al., 2023).

Chapter 5: Risk Management and Cybersecurity Strategies for Maritime OT

5.1. Vulnerability Assessments and Penetration Testing in Maritime OT Environments

Vulnerability assessments in maritime OT environments involve systematic identification of security weaknesses within critical infrastructure, which should be tailored to specific needs of different types of maritime assets, viewed against a wide range of modern cyberthreats. With it, a holistic risk assessment framework should be applied, accounting for both cyber and physical security considerations, to proactively identify vulnerabilities and implement effective mitigation measures. For example, in case of port OT vulnerability assessment, key cyber-attack scenarios could include attacks on terminal operating systems, unauthorized access to port communication networks, distributed denial-of-service attacks, and the compromise of industrial control systems. Areas of concern, identified through the analysis of these scenarios would include operational disruptions, financial losses, and significant security breaches (Gunes et al., 2021). For digitalized ships, on the other hand, cybersecurity risks stem from both administrative and technical weaknesses in maritime IT and OT systems, with the major concern being the vulnerability of the Ship Management System, which oversees various onboard operations (Yoo & Park, 2021). It is important to account for the cyberthreats described, particularly in regards to the covering potential vulnerabilities in the critical OT systems described in Table 1, as, crucial to the safe and efficient operation of a vessel (BIMCO, 2024).

Table 1: Potential cyberthreats in maritime OT systems (shipboards) (Source: BIMCO (2024)

Systems	Description of the system's functions	Potential threat/vulnerability
Bridge Systems	Digital navigation systems (ECDIS, AIS, Radar/ARPA)	Malware infection, GPS spoofing, unauthorized remote access, AIS manipulation, firmware exploitation, MITM attacks
Propulsion & Machinery Control	Monitors engine power, steering, and fuel management	Remote hijacking, malware, firmware attacks, cyber-physical attacks (SCADA exploitation), unauthorized remote system access, lateral movement from infected IT systems
Cargo & Loading Systems	Manages cargo loading, stowage, and stability	Data manipulation, unauthorized access, supply chain attacks, insider threats leading to unauthorized cargo modifications
Access Control Systems	Controls crew and visitor access, security alarms	Physical security breaches, unauthorized control, social engineering (fake port/customs agents), insider threats
Passenger Management Systems	Boarding, ticketing, and security databases	Data leaks, identity fraud, phishing-based credential theft, ransomware attacks targeting personal data
Communication Systems	VSAT, GMDSS, and onboard wireless networks	Hacking, jamming, data interception, firmware-based attacks on satellite communications (e.g., Viasat incident), MITM attacks
Ship-to-Shore Interfaces	Remote monitoring and diagnostics	Supply chain attacks, unauthorized access, lateral movement from infected IT devices to OT systems, MITM attacks on remote monitoring connections

https://doi.org/10.26219/heal.aueb.5426

Supervisory Control and Data Acquisition (SCADA) Systems	Controls shipboard automation, including power and stability management	Remote hijacking, firmware manipulation, data spoofing, cyber-physical attacks targeting automation systems, unauthorized firmware updates
Ballast Water Management Systems	Automated systems for managing ballast water intake and discharge	Unauthorized access, system override leading to stability risks, malicious remote configuration changes, lateral movement of malware from other OT networks
Fire Detection and Suppression Systems	Monitors and controls fire response onboard	Sensor spoofing, remote disabling of alarms, DoS attacks on safety system alerts, ransomware-induced sensor malfunctions
Environmental Monitoring & Emission Control (e.g., EGCS, BWTS)	Monitors emissions and ensures MARPOL compliance	Data tampering, unauthorized shutoff, IoT vulnerabilities, supply chain malware injection into monitoring systems

Penetration testing, also known as ethical hacking (Baloch, 2017) can be valuable for establishing cybersecurity of maritime OT environments. Penetration testing is a tool, simulating real-world cyberattacks and exploiting all the potential weaknesses of the system to assess the effectiveness of existing security measures. It helps to evaluate the resilience of maritime networks and helps organizations refine their incident response strategies.

Depending on the type of information, penetration testing methods can be divided into the following types: black box, white box, and gray box testing, physical penetration tests, and social engineering tests (Tauqeer et al., 2021). Black box testing is performed with a minimum amount of information about the security control system or the company's infrastructure provided to the pen tester. When testing using the white box method, the tester is provided with all the information and detailed documentation on the infrastructure, applications, equipment, and security control system. For example, a description of the system architecture, source code, and much more. This is a comprehensive assessment method that allows you to identify both external and internal vulnerabilities. When using the gray box method, the tester is provided with the information necessary to assess the effectiveness of the security control system at the

https://doi.org/10.26219/heal.aueb.5426

user level. Limited access and some knowledge of web applications and internal network infrastructure are also provided. Physical penetration tests include finding unprotected areas through which it will be possible to access the object, Eavesdropping. These are techniques in which a hacker closely monitors and listens to employees or workers who have access to the site. Social engineering testing (phishing, pretexting) involves assessing the organization's personnel. Such testing helps to identify an attack from within the organization from an employee who either initiates the attack themselves or has compromised their credentials (Baloch, 2017).

Network Penetration Testing. This is the most common and sought-after method that helps to discover and exploit vulnerabilities in a network system or infrastructure. There are three types of network penetration tests: external, internal, and wireless. External Penetration is the process of testing the security of networks, servers, and systems that are accessible from the Internet. Testing will help to check how reliably the system responds to threats from the outside. Internal Penetration involves identifying security weaknesses in your internal systems or infrastructure. These vulnerabilities are then used for attacks to analyze how internal systems respond to them. An internal penetration test mainly evaluates the attack potential of an employee of an organization, such as potential unauthorized access and leakage of personal data or information. (Tauqeer et al., 2021).

Wireless penetration testing allows testers to demonstrate the possible consequences of a security breach in a wireless network. Web applications are an integral part of organizations. Therefore, a hacked web application can also lead to the leakage of confidential information. Web application penetration testing is a method in which applications on the network are tested for vulnerabilities or security issues caused by security-ignorant development, weak architecture, or coding errors (Baloch, 2017)

Conducting vulnerability assessments and penetration testing in maritime OT environments is highly challenging because of the complexity of integrating IT and OT systems. Major challenge in these highly intertwined systems includes potential disruption of critical workflows of some critical parts of a system, while testing other ones (Harish et al. 2024). To avoid the said challenge, adherence to the requirements of

https://doi.org/10.26219/heal.aueb.5426

IMO MSC.428(98), IEC 62443 is a must, as they provide valuable structured frameworks for the risk-based security strategies implementation.

5.2. Other strategies

5.2.1. Third-party risk management

Third-party risk management (TPRM) regards external actors, including external vendors, suppliers, contractors, and service providers who have access to or interact with a vessel's OT environment. TPRM is basically an assessment and mitigation of risks introduced by these external actors. As any maritime OT components (e.g. navigation systems, propulsion controls, and communication networks) working on either third-party software or hardware, or their maintenance is depended on them, this strategy is highly crucial for the cyber resilience of maritime organizations. Key strategies for TPRM include vendor risk assessment, supply chain security protocols development, continuous monitoring and audits implementation and, finally, security of remote access control. In all the strategies adherence to maritime cybersecurity standards (IEC 62443, ACS UR E26/E27) is a must (Keskin et al., 2021).

5.2.2. Patch Management

Patch management is regular updating and changing software to keep the technology up to date with new advances in order to fix performance issues. Basically, it identifies potential issues and deploys software patches to address security vulnerabilities in maritime OT systems. In contrast to traditional IT environments, ensuring continuity of maritime OT could be challenges because of the long lifecycle of equipment, real-time operational requirements, and regulatory constraints. In particular, if patches are deployed during active ship operations, continuity of work of critical systems can be jeopardized, leading to safety hazards, navigational errors, or failures in essential machinery. Such issues directly contradict the safety objectives of IMO MSC.428(98), making effective and efficient patch management essential to ensure system integrity and compliance with international standards. This means patch management should not only adopt risk-based approach, prioritizing updates based on risk assessment and Common Vulnerability Scoring System scores, but also implement testing in controlled

https://doi.org/10.26219/heal.aueb.5426

environment. What is more, the deployment of patches should be strictly scheduled with fallback mechanisms provisioned in case of failures. Finally, in unpatchable systems, network segmentation should be implemented with an option of virtual patching of the segments (Revuru, 2024).

5.2.3. Logging and monitoring

Logging and monitoring presuppose continuous surveillance of OT systems, done to detect unauthorized activities, anomalies, as well as potential cyber threats. In maritime OT, due to the reliance on real-time data in operations, real-time monitoring is essential for early threat detection and provision of timely response. Being part of organizations' cyberthreat detection and response policy, this strategy ensures compliance with IEC 62443. This pro-active measure involves implementation of centralized log management system with automated analysis and behavior-based anomaly detection (with possibility of integration of AI for enhanced outcomes), real-time alert system as well as capability to securely store logs for extensive periods of time for forensic investigation (Kechagias et al., 2022). The advantages of such measures are undeniable, but due to the limitations in resources, physical and digital infrastructure, its integration in maritime OT can be of significant challenge (Progoulakis et al., 2021).

5.2.4. Zero Trust Architecture

Another advanced cybersecurity strategy worth mentioning is the implementation of Zero Trust Architecture (ZTA), which, unlike the traditional model, that, once authenticated, assumes a safe working mode, eliminates this assumption. Instead, ZTA requires that every user, device, and system undergo continuous verification before being granted access. This approach is critical for maritime OT, where, due to the interconnectedness of various OT systems, compromised access to one of them (e.g. engine controls, cargo systems, or navigation data) could result in catastrophic failures of larger scale. Key aspects of ZTA include: micro-segmentation, which ensures containment of the threat within the compromised system, least privilege access and multi-factor authentication (MFA). MFA is crucial for protecting remotely operated systems, as it ensures a higher level of security for unauthorization (Sindiramutty et al., 2024).

5.2.5. Firmware integrity validation

Firmware integrity validation & secure update mechanisms are also important for maritime OT cybersecurity. Controlling critical shipboard OT systems, including ECDIS, propulsion control, and satellite communication firmware must be verified and validated before installation. Such a level of security can be achieved if each firmware update is cryptographically (digitally) signed by the manufacturer to ensure authenticity. Another strategy that helps achieve this is whitelisting of approved update servers. Practically it means that only trusted firmware sources are allowed to be used/updated, with all unauthorized downloads are blocked. Finally, continuous monitoring is needed to detect any unauthorized firmware modifications, ensuring that all changes are legitimate (Marchand et al., 2023).

5.2.6. Threat intelligence

Before drawing the line, threat intelligence, a general strategy safeguarding maritime OT needs to be discussed. It is basically the identification and analysis of cyber threats specific to the maritime industry OT, such as ransomware attacks on port infrastructure or GPS spoofing affecting navigation. By monitoring the situation with these threats, how they evolve and are being used, maritime organizations can implement timely countermeasures to mitigate risks before they escalate into significant security breaches (Kumar et al., 2021). Threat intelligence information regarding maritime industry can be provided by organizations such as BIMCO, ENISA, and the U.S. Coast Guard Cyber Command. Collaborative initiatives where ship operators, port authorities, and cybersecurity agencies share valuable information, such as forums organized by Maritime Cyber Security Working Group (MCSWG) as well as Class Societies, further enhance cybersecurity awareness (Roshanaei, 2023). Finally, technological advancement (e.g. AI-enhanced threat analysis platforms) also play an important role in the promotion of cybersecurity resilience in maritime OT (Progoulakis et al., 2021).

https://doi.org/10.26219/heal.aueb.5426

5.3. Developing a Cybersecurity Risk Management Framework for Ships and Ports

Mitigation of cyber threats to maritime OT systems requires a structured cybersecurity risk management framework, which, in the view of IT-OT convergence, should account for securing critical assets through adoption of a risk-based approach This includes threat identification, risk assessment, mitigation strategies, and continuous monitoring (Neumann, 2024).

First of all, pro-active measures should be taking in regards to risk identification and assessment. To accomplish these, maritime operators must conduct asset inventories, perform threat modeling, and prioritize risks as they help in detection of potential security gaps in OT environments (Progoulakis et al., 2021). Pro-active measures are necessary for resource allocation optimization and timely implementation of targeted countermeasures. Next, access control and network segmentation should be taken care of. To achieve this step, the Perdue Model is oftentimes used, due to its efficient hierarchical structure that effectively segments networks into distinct levels, thereby reducing the risk of cyber threats. Each of these levels represent a specific operational domain, which, in case of a cyberattack incident, will contain the damage within specific zones, preventing widespread system compromise (Belev, 2022).

What is more, it is also necessary to account for monitoring which detects potential threats. Modern technologies, such as AI-driven intrusion detection systems allow for most effective analysis of network traffic and, real-time identification of anomalies that may indicate cyberattacks (Ben Farah et al., 2022). In case the identified anomalies indicate cyberattack, response and recovery plan should be developed to be implemented, ensuring business continuity (Soner et al., 2024). Finally, regulatory compliance should be an integral part of a proper risk management framework. Aligning the framework’s components with IMO MSC.428(98), IEC 62443, and IACS Unified Requirements helps effective cyber risk mitigation along digital and physical assets of maritime operators.

https://doi.org/10.26219/heal.aueb.5426

5.4. Regulatory Frameworks Applicability in Maritime OT: SOA

In the view of such complex, oftentimes overlapping and yet, not completely clearly defined applicability of the regulatory frameworks, maritime organizations are guided by the State of Applicability (SOA) of various cybersecurity strategies. SOA is basically a framework that systematizes cybersecurity governance, ensuring cyber resilience of maritime operations because appropriate security controls are applied to specific maritime OT systems depending on their vulnerabilities and regulatory requirements. SOA in maritime OT is determined on the basis of the following factors: a) the nature of the OT system, b) the identified cyber threats, c) applicable regulatory frameworks and d) the level of risk posed by a security gap as high-risk systems require stricter controls (BIMCO, 2023). Building upon the information from the Table 1 (presented above) SOA in the maritime OT is represented in Table 2 (presented below).

Table 2: Maritime OT Cybersecurity: State of Applicability (SOA) Table

Control	Description	Systems Targeted	Threats Addressed	Rationale
Access Control & Authentication	Restricts unauthorized access through multi-factor authentication (MFA) and role-based access control (RBAC).	Bridge Systems, Propulsion & Machinery Control, Cargo Systems, SCADA, Ship-to-Shore Interfaces	Unauthorized access, Insider threats, Phishing, Lateral movement	Prevents unauthorized personnel from accessing and manipulating shipboard OT systems.
Network Segmentation	Separates IT and OT networks to	Propulsion, Ballast, Cargo,	Ransomware, Lateral movement,	Ensures malware in IT systems cannot

https://doi.org/10.26219/heal.aueb.5426

n & Air-Gapping	prevent malware spread.	SCADA, Ship-to-Shore Interfaces	Supply chain attacks	spread into critical OT networks.
Firmware Integrity & Secure Updates	Ensures only verified, signed firmware updates are installed.	Communication Systems (VSAT, GMDSS), Bridge Systems, Propulsion & SCADA	Firmware attacks (e.g., Viasat case), Supply chain malware, Remote hijacking	Prevents unauthorized firmware modifications that could disable shipboard systems.
Intrusion Detection & Prevention Systems (IDPS)	Detects and blocks unauthorized access attempts.	Ship-to-Shore Interfaces, SCADA, Propulsion, Cargo & Loading	Ransomware, Cyber-physical attacks, DoS attacks	Provides real-time monitoring to detect anomalies before major failures occur.
Encryption for Ship-to-Shore Communications	Ensures encrypted communication between ships and shore-based systems.	Communication Systems, Ship-to-Shore Interfaces	MITM attacks, Data interception, Supply chain breaches	Protects operational data against interception/manipulation
Whitelisting & USB Device Control	Blocks unauthorized external devices from	SCADA, Bridge Systems, Cargo & Loading	Malware infections, Supply chain backdoors, Insider threats	Prevents malware from being introduced via infected/

 https://doi.org/10.26219/heal.aueb.5426

	connecting to OT systems.			unauthorized devices.
Role-Based Access Control (RBAC) & Least Privilege	Limits system access based on job responsibilities.	Cargo Systems, SCADA, Bridge Systems	Insider threats, Phishing, Unauthorized control	Authorized access only to specific personnel->less human error risks.
Incident Response & Recovery Plan	Defines procedures for cyber incident containment, mitigation,recovery.	All OT Systems	Ransomware, DoS attacks, Cyber-physical attacks	Ensures a structured response to cyber incidents.
Zero-Trust Security Model	Continuous verification for network and device access.	Ship-to-Shore Interfaces, SCADA, Cargo Management	Phishing, Insider threats, lateral movement.	When data compromised, prevents unauthorized access.
Real-Time Monitoring & Anomaly Detection	Uses AI and machine learning to detect abnormal activity.	SCADA, Bridge Systems, Propulsion & Machinery Control	Cyber-physical attacks, Ransomware, DoS attacks	Detect cyber threats before they escalate into full-scale attacks.
Secure Configuratio	Ensures that OT devices	Propulsion, Cargo, SCADA,	Firmware, Malware infections,	Disables unnecessary system features->reduced

https://doi.org/10.26219/heal.aueb.5426

n of OT Systems	have minimal vulnerabilities.	Bridge Systems	Unauthorized system overrides	exposure to cyber threats.
Backup & Disaster Recovery Planning	Implement regular backups and system recovery strategies.	All OT Systems	Ransomware, Data corruption, Supply chain attacks	Ensures recovery of critical systems.

Elaborating more on the Table 2, it should be said that the Maritime OT SOA reflects the unique characteristics of the industry's demands to ensure compliance with the relevant frameworks by indicating which control is most applicable in each particular case. The relevant frameworks, the SOA builds upon include: IEC 62443, IACS UR E26/E27, IMO MSC.428(98), NIS2. With it, it is important to note that applicability of some of the frameworks is limited. For example, as it has already been discussed in 4.4. section of the present paper, NIS2 has limited applicability to certain segments of the maritime industry, particularly in onboard OT systems. However, when ship-to-shore communication systems are managed by entities that are considered Operators of Essential Services (OES) or Important Entities under NIS2, then cybersecurity provision requires implementation of NIS2 as well. Further each control measure will be discussed in detail.

Access Control and Authentication should be implemented across all OT systems, as it is required by IEC 62443, IACS UR E26 and E27, and IMO MSC.428(98). In particular, applicability of IEC 62443 is justified as it emphasizes the importance of identity and access management to prevent unauthorized access, while IACS UR E26 and E27 mandate secure access controls for onboard systems. IMO MSC.428(98) is equally applicable as well as it requires risk-based access management. On the other hand, NIS2 applicability is limited here (as it has been mentioned above) but, whenever it is applicable it also enforces stringent access control measures. For bridge systems MFA is necessary to ensure the security of access to ECDIS, radar, and navigation

https://doi.org/10.26219/heal.aueb.5426

systems, while for propulsion system MFA is used in engine control systems and steering mechanisms. Cargo management can be secured if MFA is integrated into cargo loading and monitoring systems. All types of remote and local access (SCADA, Ship-to-Shore interfaces) should also be protected by MFA. Role-Based Access Control (RBAC) can also be used to restrict access based on the officer's role (e.g., captain, watch officer), protecting sensitive data of each system. RBAC and Least Privilege is applicable to all OT systems and it is required by IEC 62443, IMO MSC.428(98) and, in certain cases, by NIS2.

Network Segmentation and Air-Gapping controls are critical to propulsion, ballast, and cargo controls as their networks should be physically or logically separated, and in some cases completely disconnected, to prevent malware spreading onto other networks. This can be achieved by creating separate VLANs or physical networks for critical OT systems and, where feasible, air-gapping the most critical components of engine control systems. When physically disconnecting components of the latter, data transfer is to be done using controlled and scanned removable media, as it mandated by IACS UR E27. This control is also applicable to safe proofing SCADA, where it is achieved through installation of firewalls to control traffic flow between the SCADA network and the IT network, allowing only necessary communication. Network segmentation is an essential requirement of IEC 62443 as it helps limit the impact of security breaches. IACS UR E26 also mandates network zoning because this measure helps isolate critical systems. Segmentation of Ship-to-Shore communication is also done, and it is achieved through implementation of DMZs, isolating shipboard networks from external networks, in line with IMO MSC.428(98)' emphasis on network security in risk mitigation.

Firmware Integrity and Secure Updates should be digitally signed and verified before installation in line with IEC 62443 requirement of firmware management to prevent malicious modifications. Besides installation, each update should also be digitally verified as it is mandated by IACS UR E27. Risk assessment for firmware updates should be done (IMO MSC.428(98)), with mechanisms for secure remote updates implemented where necessary, with rollback capabilities.

https://doi.org/10.26219/heal.aueb.5426

Intrusion Detection and Prevention Systems (IDPS) are placed at network perimeters, within critical OT segments. They detect and block unauthorized access attempts, as it recommended by IEC 62443. This control method is also part of continuous monitoring requirements, imposed by IACS UR E26 and IMO MSC.428(98). NIS2 is also applicable here, but with the restrictions discussed.

Encryption for Ship-to-Shore Communication channels is necessitated by IEC 62443, with remote access stipulation being specifically recommended by IACS UR E26 and IMO MSC.428(98) to ensure secure data transmission. This control is done with the help of cryptographic protocols, strong enough to protect data confidentiality and integrity. The applicability is spread on all maritime organizations as, due to the complexity of the maritime communication, which might involve multiple stakeholders and thus, is enforced by NIS2.

Whitelisting and USB Device Control is required by IEC 62443 and refers to the use of only authorized software and USB or other external devices on maritime OT systems (as it is stated by IACS UR E27) to avoid introduction of malware via removable media. This measure is also in line with IMO MSC.428(98) and its warnings regarding potential threats, associated with malware introduction via removable media.

Incident Response and Recovery Plan should be developed to enhance maritime organizations' cyber resilience. This measure aligns with all the mentioned frameworks and presupposes establishing cohesive flow of the necessary procedures, including the following parts of the plan: detection, containment, eradication, recovery, and analysis of the learnt lessons (IMO MSC.428(98), IACS UR E27/T26). Specific procedures should be included for reporting activities, as it is mandated by NIS2. In order for the measure to be successfully implemented, regular incident response exercises should be conducted. What is more, here it is also necessary to mention the value of backup and incident recovery planning, as in case any of OT systems malfunctioning, it is crucial to recover the critical data for the reboot of the compromised segment in proper time (IEC 62443). As IACS UR E27 requires data backup and recovery capabilities, organizations need to provision those before the incident happens, which make this measure legitimate part of cyber risk management practice (IMO MSC.428(98), NIS2).

https://doi.org/10.26219/heal.aueb.5426

Zero-Trust Security Model adoption (presupposing the use of micro-segmentation, MFA, and continuous monitoring) aligns with the IEC 62443' recommendations of defense-in-depth approach and IMO MSC.428(98) requirements for risk-based access management. This measure primarily focuses on systems with network connectivity and data access, including Ship-to-Shore Interfaces, SCADA Systems, Cargo and Passenger Management Systems and, of course, Communication Systems.

Real-Time Monitoring and Anomaly Detection as a cybersecurity measure is crucial for systems where real-time operational data is critical. These include SCADA, Bridge, Cargo management systems, Propulsion and Machinery Control and Ship-to-Shore Interfaces. It can be implemented through the deployment of real-time monitoring tools and anomaly detection systems, which identify suspicious activities, as well as potential security breaches. All the discussed regulatory frameworks advocate this kind of vigilance both in the form mandatory network monitoring for anomalies (IACS UR E26), and general monitoring for cyber threats (IMO MSC.428(98)) for all the maritime organizations, ships and ports included (NIS2)

Control for Secure Configuration of OT Systems presupposes following security best practices in configuration of all OT devices, with unnecessary services and ports being disabled. The measure is relevant to all hardware/software components of maritime OT systems, onboard and shore-bound ones included. Regulatory documents advocating such measure include IEC 62443, which recommends secure configuration management; IACS UR E27, which requires secure configuration of onboard systems, and IMO MSC.428(98), which emphasizes the importance of secure system configurations.

Chapter 6: Emerging Trends and Future Challenges in Maritime OT Cybersecurity

As technological and informational advancements continue to evolve, digital transformation of maritime OT is expected to proceed along, integrating newest

https://doi.org/10.26219/heal.aueb.5426

technologies such as autonomous ships, satellite communications, the Internet of Thing, Artificial Intelligence, blockchain, and even quantum cryptography (Luchenko et al., 2023). By automating navigation and propulsion, autonomous vessels can optimize routes and speeds. In its turn, such optimization leads to significant fuel savings and reduced operational costs. Additionally, prevailing automation of operations means if not complete reduction, then at least drastic elimination of crew members, leading to lessening of labor expenses and minimization of human error (Issa et al., 2022). With the benefits that this progress offers, however, there are expected to increase the challenges related to cyber security of the sector that require innovative mitigation strategies (Neumann, 2024).

6.1. Autonomous ships

In recent years, new developments in autonomous ships have highlighted the cost savings and logistical efficiencies. Firstly, autonomous ships offer significant financial benefits, as crews account for around 30% of the current costs of shipping. Secondly, “human error” accounts for up to 96% of accidents at sea (Hilden et al., 2023). Combined with increased energy efficiency and environmental considerations, this makes autonomous ships an inevitable direction for shipping. The International Maritime Organization has defined a four-stage development path for autonomous surface ships: 1) automated processes; 2) remotely operated ships with crews on board; 3) remotely operated ships without crews on board; 4) fully autonomous ships (Pietrzykowski et al., 2022).

The United Nations has already called for updated legal frameworks and regulations to support the development of new ships and systems. But despite the international attention and enormous potential benefits, the future of fully autonomous ships poses even more safety risks. According to the European Directive “EU 2016-679”, cyber-enabled ships are among the most critical infrastructures that already rely heavily on digital services, and malicious disruption of their operation could result in financial and environmental damage or even endanger human safety. Cybersecurity of modern ships is becoming an increasingly important area due to its increasing potential to impact people, the ship, cargo and the environment (Munim et al., 2022).

Among the challenges that are associated with the new autonomous trend in maritime operations, high complexity of IT-OT integrated systems should be mentioned (Ziajka-Poznańska & Montewka, 2021). In particular, high dependence on digital control systems and remote communications should be mentioned, which means that autonomous ships' OT systems are highly susceptible to remote hacking and control hijacking, leading to compromised navigation, propulsion, or cargo systems (Munim et al., 2022). Other types of cyber threats that are of pressing concern include GPS spoofing, navigation manipulation, as well as communicating jamming which may lead to sabotaged critical ship-to-shore coordination and vessels deviating from planned courses, increasing the risk of collisions or enabling hijackings. (Issa et al., 2022). In the view of such highly complex and integrated systems, identification of potential vulnerabilities, as well as development of strategies that could mitigate these risks could pose significant challenges (Thotokatos et al., 2023). One of relevant practical issues, associated with that is the liability and insurance gaps, exposing autonomous vessels yet unaddressed legal issues in case of cyberattacks (Islam, 2024).

Additionally, there is also a shortage of cybersecurity professionals with the relevant expertise in maritime autonomous systems (Munim et al., 2022). What is more, one should not forget about the ethical considerations that autonomous technology implies, with its inherent parts, such as AI, machine learning etc., raising issues with bias in algorithms and the potential for unintended consequences (Veitch & Alsos, 2022). Finally, cybersecurity issues associated with autonomous ships presuppose regulatory hurdles as existing maritime laws and regulations are primarily designed for manned vessels. Admittedly, the guidelines and regulations discussed above (e.g. IACS UR E26 & E27), do have provisions requiring shipowners to integrate cybersecurity measures into vessel design, operation, and maintenance, still, adjustment of those provisions will be required to account for decreased human involvement in the OT (Issa et al., 2022).

6.2. Satellite Communication Systems

Maritime Satellite communications have become an indispensable technology of the maritime operations, connecting vessels to shore and facilitating essential ship-to-ship

 https://doi.org/10.26219/heal.aueb.5426

communications. As the maritime industry undergoes digital transformation, the maritime satellite communications market is witnessing a profound shift in operational trend, with the following seven key trends shaping the industry's communication.

First of all, High-Throughput Satellites (HTS) trend should be mentioned as it offers increased data rates and higher throughput, meeting the growing demand for higher connectivity and bandwidth-intensive applications on maritime vessels. This trend ensures that ships can access faster and more reliable communication links, supporting real-time data exchange, video conferencing, and other bandwidth-intensive maritime applications (Dizaj & Shishvan, 2024). Secondly, as maritime operations become more digitalized, there is a growing trend in the demand for broadband connectivity at sea. Vessels require high-speed internet access for navigation, weather monitoring, crew welfare, and operational efficiency. Maritime satellite communications providers are responding to this trend by offering scalable and cost-effective broadband solutions that meet the various connectivity needs of the maritime industry (Niknami et al., 2023).

The third trend is integrating the IoT into the maritime satellite communications market. Ships are increasingly equipped with IoT devices and sensors to monitor and optimize various operational aspects, from engine performance to cargo conditions. This trend requires robust satellite communications networks that can handle the increased data traffic generated by IoT devices, enabling intelligent and data-driven decision-making processes on maritime vessels (Chaudhry et al., 2021). Another trend is marked by the migration to flat panel antennas. Traditional parabolic antennas are giving way to the trend towards the adoption of flat panel antennas in maritime satellite communications. Flat panel antennas offer a more compact and aerodynamic design, making them suitable for maritime applications. This trend helps improve vessel aesthetics, reduce wind resistance, and increase fuel efficiency, while still providing high-performance satellite communications capabilities (Weng et al., 2022). The fifth point in the list is the shift to software defined networks (SDN) architectures, which has its impact on satellite communications solutions. Network management can be made more flexible and efficient using software-defined networking, allowing maritime operators to dynamically allocate bandwidth, prioritize traffic, and respond to changing

https://doi.org/10.26219/heal.aueb.5426

communications requirements. At the same time, this trend is happening as the industry seeks communications solutions that are flexible and adaptable (Alqurashij et al., 2022).

Besides those, there is also a global tendency to further developments being done in the sphere of cybersecurity, translated into the maritime satellite communications market integrating advanced cybersecurity measures to protect sensitive data and communications channels. Besides issues with digital cybersecurity, which may include satellite signal interception, signal jamming and denial-of-service (DOS) attacks, malware infiltration via satcom networks, there are also physical security threats to the ground stations. The former issues require advanced solutions, including strong encryption, threat detection systems, and secure network protocols are becoming standard features, ensuring that maritime communications remain resilient to cyber threats. The latter, on the other hand, in addition to cyber protection, require safeguarding from physical security breaches unauthorized access to the facility or sabotage of equipment, can have equally disruptive effects (Carlo & Obergfaell, 2024).

Another major trend, which basically, represents the urgent demand of the maritime industry, the need for global coverage and seamless mobility. Vessels navigating international waters and remote regions, as well as the autonomous technology being increasingly integrated, require continuous and reliable communications links. Satellite communications providers are responding to this trend by offering services that provide continuous connectivity, regardless of vessel location or mobility (Xylouris et al., 2024).

6.3. Newest Technological Advancements: AI, IoT, Predictive Analytics

The maritime sector is embracing a wave of technological advancements, with IoT being already actively used for real-time tracking and monitoring, and AI being employed for predictive analytics and automation. These technologies promise to revolutionize maritime operations, increasing their efficiency and improving decision-making (Setiawan et al., 2024).

https://doi.org/10.26219/heal.aueb.5426

IoT devices are now being actively employed across ships and ports. Onboard vessels, IoT sensors monitor engine performance, fuel consumption, cargo conditions, and environmental parameters, while in ports, the technology is used to track container movements, monitor berth availability, and manage traffic flow. The real-time data collected by these devices provides a well-rounded view of operations, and thus enabling better control and optimization. This technology works with vast amounts of data related to vessel performance, cargo status, and environmental conditions (Ashraf et al.,2022). Such bigdata are better processed with AI algorithms, that enable predictive maintenance, optimized routing, fuel consumption, and autonomous navigation. AI-powered systems also are used to predict equipment failures both on vessels and on-shore maritime objects, allowing for timely repairs and preventing costly breakdowns. In ports, AI-driven technology can optimize container yard operations and predict vessel arrival times. This is helpful in improving efficiency and reducing turnaround times (Paraskevas et al., 2024). Predictive analytics, possible through integration of AI technology into IoT data processing, is profoundly transforming decision-making in the maritime industry (Setiawan et al., 2024). On ships, predictive analytics can optimize voyage planning, as, for instance, AI can process vast amounts of historical data on such factors as weather conditions, fuel prices, and port congestion. In ports, these predictions are used forecast cargo volume and thus optimize resource allocation, and predict potential delays, enabling better planning, reducing costs, and improving overall operational efficiency. Integration of AI and IoT is expected to bring into reality fully automated maritime units (Sotirov et al., 2024). Some of them (e.g. autonomous ships), are currently being employed in their testing voyages. A good example of such is the Yara Berkenland autonomous ship, that will be discussed in further chapter. Besides ships, however, there is a possibility of "smart ports" that, through AI, IoT and Blockchain integration, will allow for fully automated and interconnected operational systems.

Finally, digital twins (virtual ships), are also needed to be mentioned. This technology represents virtual replicas of physical assets (vessels), used to simulate and optimize ship and port operations. In theory, there is an infinite variety of operations that can benefit from a digital twin, and these have expanded to include system design, efficient

 https://doi.org/10.26219/heal.aueb.5426

verification and validation services, simulator testing, training and integration with a virtual system, and the generation of deep insights and predictions. The operations and ideas of a digital twin lead the first steps towards autonomy - the creation of efficient algorithms for components and operations with remote control and self-monitoring. A digital twin vessel equipped with an integrated data link is fundamental to the expansion and development of autonomy (Neugebauer et al., 2024).

Smart ports and digital twins are part of Industry 4.0 and Internet Plus enable the transformation and renewal of digital, automated and intelligent work only with the development of broadband communication systems (today this is already equal to 5G systems) as a condition for their implementation. With 5G, they will collaborate to advance this transformation and modernization to build efficient and environmentally friendly smart ports and digital twins of ships. Smart ports require communication systems to support low-latency, high-bandwidth and high-reliability communication services to process control data and multi-channel video data of port equipment. Using traditional fiber-optic and Wi-Fi-based communication, the deployment, operation and maintenance of the network is expensive, and the network performance for such data processing is often suboptimal due to poor stability and low reliability. 5G is expected to address these issues with its low latency, large bandwidth and capacity, and high reliability, as well as support for private network solutions and end-to-end (E2E) application performance assurance (Potter et al. 2024).

The said benefits, however, come with significant security challenges as many IoT are resource-constrained and lack robust security protocols. This makes them susceptible to various cybersecurity risks, which could not only disrupt operations, steal data, but even take control of the vessel. The IoT integration into maritime OT is numbered, but so are the vulnerabilities they bring into the operation. To illustrate this, the example of the Port of Antwerp cyberattack can be given, when IoT-based cargo tracking devices were cyber attacked to monitor container movements and cargo status for the purpose of illegal substances smuggling (May & Holcova, 2023)

https://doi.org/10.26219/heal.aueb.5426

6.4. Quantum computing technology

Another trend that is worth exploring when discussing maritime OT development is the implantation of quantum computing, which can perform complex calculations at the highest speeds, offering an unprecedented pathway for optimization of operational processes and increased efficiency (Li et al., 2024). While not yet widely implemented, quantum computing has the potential to revolutionize data processing, cybersecurity, and operational efficiency of the maritime industry. Despite the fact that the trend belongs to the future in its actualization, research into quantum optimization algorithms suggests enormous benefit from real-time decision-making capabilities, such as adaptive navigation based on dynamic weather and traffic conditions (Phillipson, 2024), ultra-efficient fuel management, enhanced cargo logistics, including vessel wait times and improving quay crane utilization (Li & Li, 2024). The segment of autonomous shipping and AI-driven fleet management will likely be the first to explore quantum-enhanced solutions (Li & Li, 2024).

Despite its potential benefits, quantum computing also introduces significant cybersecurity risks. For example, when used as a tool for cyberattacks, quantum computers could break currently existing encryption standards, leaving maritime OT systems vulnerable to cyberattacks (Singh & Kumar, 2024), increasing the risk of hijacking, cargo manipulation, and GPS spoofing (Li et al., 2024). Thus, with the advancement of the technology, quantum computing' role in both enhancing and disrupting maritime OT is expected to become more and more evident. If the technology to be integrated into the industry's operation with safety, it is vital to ensure a balanced approach not only uses its potential but also provision for ways of mitigating potential risks (Phillipson et al., 2024).

Chapter 7: Case Studies and Best Practices

7.1. Case Study: OT and the Port of Singapore efficiency

The Port of Singapore stands as one of the perfect examples of how modern OT transforms and elevates maritime logistics. As one of the world's busiest ports, handling

https://doi.org/10.26219/heal.aueb.5426

over 37 million TEUs annually, the Port of Singapore showcase major advantages that integration of smart port technologies, blockchain, artificial intelligence, and cybersecurity frameworks have to offer.

To start the discussion, OT for efficiency enhancement should be discussed. In this respect, the Port of Singapore is known for implementations are AI-powered automated cranes, infrastructure with IoT technology, blockchain integration for supply chain transparency, as well as the use of AI-predictive analytics (Mba, 2024). AI-driven automated cranes allowed the Port of Singapore to significantly decrease container dwell time, streamlining port activities and reducing overall logistical delays. Fujitsu company has announced the results of a two-year study conducted with the Maritime and Port Authority of Singapore to evaluate AI-based risk analysis for shipping in the Singapore Strait. Using Fujitsu Human Centric Al Zinral, an AI technology developed by Fujitsu Laboratories, it is possible to identify vessel collision risks and dynamically predict hot spots. The technology can be deployed in a vessel traffic service (VTS) system to help dispatchers manage schedules and improve shipping safety. Fujitsu's risk detection technology has demonstrated the ability to quantify risks in more detail before they are detected by human operators, giving humans more time to take the actions needed to prevent collisions.

Beyond automation, the IoT-enabled smart port infrastructure plays a pivotal role in monitoring vessel traffic, container positioning, and environmental conditions. In October 2019, the Maritime and Port Authority of Singapore launched a dedicated information portal, digitalPort@SGTM, to enable seamless connectivity and information sharing across ports across the maritime transport chain. The portal digital-PORT@SGTM simplifies the process of checking ship, immigration and port requirements from multiple agencies in one app by consolidating 16 separate forms. Masters and ship agents from over 550 shipping companies can now submit, track and receive vessel arrival and departure clearances through the portal. In the next phase, digitalPORT@SGTM, by simplifying operations for optimal vessel passage planning at the Port of Singapore, will optimise port resources and improve efficiency through the use of artificial intelligence. The platform will act as a single digital window for

 https://doi.org/10.26219/heal.aueb.5426

booking maritime services. The Port of Singapore also employs IoT sensor data to facilitate predictive maintenance. This allows port authorities to address potential mechanical failures before they escalate into major disruptions (Chowdhury et al., 2023).

The Port of Singapore also employs Blockchain technology (TradeTrust) to improve its document verification. This helped reduce fraudulent activities, and accelerated customs clearance procedures. Due to the cybersecurity advantages of the Blockchain technology, the Port of Singapore increased its data integrity, while also fostering trust among stakeholders. Another innovative technology employed by the Port of Singapore, is predictive analytics, enabled by AI, which accounts for such factor as anticipated traffic congestion to recommend optimal berth allocations, and enable preemptive infrastructure maintenance (Lam et al., 2021). Finally, digital twin technology, which simulates port operations in a virtual environment, further enhanced the Port of Singapore decision-making by allowing authorities to test different operational scenarios (Karlsson et al., 2024).

Increased automation and connectivity, that the Port of Singapore takes advantage of requires accounting for significant cybersecurity risks. Acknowledging the potential vulnerabilities, the Port of Singapore introduced several security measures, including network segmentation, Intrusion Detection System (IDS), as well as regular cybersecurity monitoring and audits (Fenton, 2024).

7.2. The Yara Birkeland – Cyber Risks of the World's First Fully Autonomous Ship

The Yara Birkeland is the first ever emission-free, autonomous container ship, launched in 2021. Two Norwegian companies, Yara (a fertilizer manufacturer) and Kongsberg (a technology company), have joined forces to build a market-changing vessel. Once in service, the vessel will allow Yara to replace 40,000 transportation trips a year. It represents a groundbreaking advancement in maritime technology with a cutting-edge OT and AI-driven navigation system, which is expected to eliminate the need for a human crew while also significantly reducing greenhouse gas emissions. In short, key features of the Yara Birkeland include: ballast free, battery pack as ballast and fully battery powered operations. As it is a container transporting ship, in its work it relies on automated cargo handling technology that, when integrated into infrastructure of ports, allows seamless loading and unloading of goods, with fully digital cargo handling system and automatic electrified cargo unloading/loading system. It also has got automatic mooring/departure from the berth, potential for fully autonomous and unmanned vessel operation (which though possible, is currently not allowed due to the limitations in the regulations). The vessel operates at a distance of up to 12 nautical miles from the shore (Yara, 2024).

This system uses an array of sensors, cameras, radar, LiDAR, and sonar to collect real-time data on the ship's surroundings, while AI algorithms process the data in real time, optimizing operational efficiency and minimizing the risk of human error. IoT systems on board of the vessel, ensure shore-based operators have continuous monitoring of engine performance, cargo conditions, and environmental factors such as wind speed and wave height. (Fenton & Chapsos, 2023). All in all, the technological advancements that the Yara Birkeland boasts of, allow for enhanced operational efficiency, reduction of labor costs, while the emission-free status ensures environmental benefits. However, the ship is not yet fully autonomous, as it is still undergoing operational testing. What it can do now include the following: leaving the quay at Yara's Herøya facility, sailing to Brevik, and docking at the unloading quay. The navigator onboard is overlooking the voyage. Furthermore, on the return trip to Herøya, it can autonomously return and dock at its Birkeland quay. The mooring of the ship is still done manually, however, as soon as robotic mooring arms complete the testing, it is expected to become a fully autonomous ship (Yara, 2024).

Despite the expected operational and environmental benefits, the ship's innovative design also introduces a range of cybersecurity risks that may challenge the safety, reliability, and operational integrity of autonomous shipping. First of all, due to the reliance on remote control systems (accessible via satellite and shore-based infrastructure), there is a concern of remote hacking, which could jeopardize the

https://doi.org/10.26219/heal.aueb.5426

navigation system, disrupt communication links, or even take control of the vessel (Xing, 2024). Other cyberattacks, that the Yara Birkeland is potentially vulnerable to, include GPS spoofing as the vessel relies heavily on GPS for autonomous routing. More specifically, Astrov and Bauk (2024) note that a cyber-attack on an autonomous vessel's rudder controller can severely impact maneuverability. This can make the vessel vulnerable to collision, hijacking, and loss of operational control. Since Yara Birkeland relies on remote and AI-driven rudder adjustments, it is vulnerable to rudder signal manipulation and DoS attacks when, due to being altered by the unauthorized users, rudder command inputs change the vessel's course, which not only can steer it into different navigational zones, but also prevent it from making necessary course corrections (Astrov & Bauk, 2024).

Thus, despite the fact that Yara Birkeland does represent a pioneering step toward fully autonomous shipping, with a big number of operational and environmental benefits, still it is highly vulnerable to cyberattacks. AI-driven navigation, IoT connectivity, and remote monitoring of the ship are main vulnerable points that introduce significant cybersecurity challenges and they must be addressed. The existing regulations and protective guidelines (IMO MSC.428(98) and IEC 62443) allow for viable solutions that should be included to account for the mentioned issues. They may include (but not limited to) implementation of the end-to-end encryption, network segmentation, redundant navigation systems (Jhanjhi & Shah, 2024), virtual patching with external firewalls (Belev et al., 2022). However, due to the unprecedented nature that autonomous maritime OT brings into the discussion, mere compliance with the existing regulations and standards will not suffice as they simply do not account for all the implications and vulnerabilities that unmanned OT might imply. Thus, continuous monitoring and constant adjustment are necessary to enhance this type' of OT's defenses against evolving cyber threats (Progoulakis et al, 2023)

7.3. Lessons Learned from Past Cyber Incidents

https://doi.org/10.26219/heal.aueb.5426

According to a report prepared by HFW and CyberOwl, a company specializing in cybersecurity in the maritime industry, the average damage from an attack on one organization is already $550,000. A year ago, this amount was almost 3 times less - $182,000.

According to a survey conducted among 150 maritime sector specialists, in general, ransom demands have increased by 350%. The average ransom amount remains at around $3.2 million (in 2022, it was $3.1 million). It is also estimated that 24% of victim companies agreed to the attackers' terms. 25% of respondents said that their management does not have any insurance against cyber risks at all. Furthermore, a fleet of 30 ships experiences an average of 30 incidents per month and more than 80 per year. Although most of them do not cause serious damage, a lot of resources are spent on restoring systems. Experts are calling on shipping companies to pay increased attention to safety issues by attracting highly qualified specialists. Currently, the industry is experiencing an acute shortage of such personnel, and this is with an extremely low level of unemployment in the IT sector - less than 1%. Impressive financial investments, which not every carrier can afford, can save. The report is another warning for the maritime industry, since the introduction of autonomous shipping, modern communications at sea and artificial intelligence brings new risks, which, however, could be mitigated if lessons from past cyber incidents are accounted for (CyberOwl, 2023).

One of such lessons can be drawn from The NotPetya ransomware attack, which in 2017 was one of the most disruptive cyber incidents in maritime history, affecting Maersk, the world's largest shipping company, with, as it was reported, a complete shutdown of the entire computer system of the APM Terminals division, which operates terminals in 76 ports in 59 countries. Problems with Maersk's computer systems lasted a week. The virus entered the company's computer system through the Ukrainian program M.E.Doc, which is used to fill out tax reports in Ukraine. Within hours, 17 shipping terminals worldwide experienced operational disruptions, leading to widespread delays and financial losses estimated at $300 million. The impact of NotPetya was catastrophic for Maersk's operations as container logistic, and critical OT

https://doi.org/10.26219/heal.aueb.5426

systems, including cargo management platforms and port operations software were shut down (Kanellopoulos, 2024).

One of the main reasons NotPetya spread so quickly, was the lack of proper segmentation between the Maersk's IT and OT networks, leading to the malware quickly propagating to critical port and shipping operations. The incident showed that network segmentation between IT and OT environments is a must if similar incidents are to be avoided in future. Adoption of the Perdue Model, which fosters multiple layers of security in control systems can help preventing similar cyber-attacks. Next, the fact that Maersk was infected through third-party software (MeDoc) highlights a major weakness in supply chain security. To avoid such incident from happening it is vital to ensure third-party vendors for OT software undergo rigorous security testing before deployment (Kanellopoulos, 2024). This measure should be applied not only during the initial installation of the third-party software, but also before each programmed update, with digital signature and verification being provided. Zero Trust Architecture (ZTA) should be applied to vendor access too. This will ensure that external partners have restricted access to shipboard networks (Sindiramutty et al., 2024).

Furthermore, provisions for backup and recovery planning (preferably available offline) should be a must as well, as one of the few reasons Maersk was able to recover, was the unexpected (unplanned) backup that was provided by one of the company's domains, which, by sheer luck, was offline during the attack. Among other lessons learnt from the incident are the value of real-time monitoring, which allow for stopping cyber incidents before they escalate, as well as provisioning of comprehensive crew training in cybersecurity (Abbatemarco et al., 2024).

Finally, compliance with the relevant industry standards (IMO, IACS UR E26/E27, and NIS2) as well as development of cybersecurity-first culture in maritime operations can help preventing or/and mitigating of the cyber incidents negative impact. Maersk's experience showed how detrimental the impact of cybersecurity negligence can be. With the introduction of more advanced technology cyber risk management must be integrated into ship design, construction, and daily operations. By applying these

https://doi.org/10.26219/heal.aueb.5426

lessons, the maritime industry can significantly improve its resilience against future cyber incidents, while also ensuring secure and reliable maritime operations.

Learning from the past incidents is a viable strategy against future cyber attracts thus, researchers from the Netherlands have created a unique database that contains information on more than 160 cyber-attacks on maritime transport around the world, starting from 2001. The database is called the Maritime Cyber Attack Database (MCAD) and is available for public viewing online (https://maritimecybersecurity.nl). Among the incidents included in the database are such as the spoofing of the locations of NATO ships in the Black Sea in 2021. The aim of the database is to raise awareness of cybersecurity in the maritime industry and to provide further research and more accurate simulations in this critical area (NHL,n.d).

The MCAD database contains information about incidents involving not only ships, but also ports and other maritime facilities. The information is collected from open sources and covers various types of cyberattacks, such as hacking, blackmail, data tampering, system destabilization, etc. Some of the incidents had serious security and economic consequences. With more than 90% of the world's cargo transported by sea (equivalent to 70% of the value of global trade), maritime cybersecurity is a priority. However, much of the fleet and the technology it uses is aging and increasingly vulnerable to cyberattacks. According to the data collected for MCAD, 38% of operational oil tankers and 59% of general-purpose vessels have been in operation for more than 20 years. (David et al., 2024).

One of the applications of the database is to develop realistic simulations of cyber-attacks on maritime transport so that companies, organizations, ports and harbors can prepare for them in advance. The research group will also use MCAD to create reports and scientific papers showing trends and results of detailed analysis of subsets of the data. (NHL, n.d.).

Conclusion

Concluding the analysis, it could be definitively said that the increasing digitalization of the maritime industry has profoundly transformed shipboard and port operations.

https://doi.org/10.26219/heal.aueb.5426

The discussed optimization in all operational systems, owed to rapid and deep integration of OT with IT, however, comes at the cost of significant increase in cybersecurity challenges. With the wide range of cyberthreats, including ransomware, GPS spoofing etc., modern maritime OT seems to be vulnerable on a variety of levels. This study has conducted and provided a holistic assessment of maritime OT cybersecurity, addressing the technical, regulatory, and strategic dimensions of cyber risk management.

Key findings of the analysis highlight the growing impact that the evolving cyberthreats could have on the deepening convergence of IT-OT systems within the maritime industry. In particular, targeting critical OT systems (e.g., ECDIS, engine automation, cargo handling, fuel management) can not only endanger one part of a ship, but entire ships and the relevant marine infrastructure, disrupting entire supply chains, and causing financial losses in the hundreds of millions. Discussed examples of NotPetya attack on Maersk serve as perfect illustration to the level of impact. What is more, attacks such as GPS spoofing, AI-based manipulation, and port IT system breaches, like the one that happened when Port of Antwerp was cyberattacked, illustrate how different vulnerabilities such as insecure IoT devices, legacy systems, and poor network segmentation can be explored. Besides the cybersecurity limitations that are inherent to older systems, there are also challenges related to the uncovered gaps, that new technological advancements have. The rise of autonomous vessels, as it has been discussed on the example of Yara Birkeland, brings new risks such as remote hacking, AI poisoning, and communication jamming, necessitating enhanced cybersecurity frameworks.

In regard to the regulatory standards, the analysis shows that while the existing standards, like IMO's MSC.428(98), IACS Unified Requirements (UR E26 & E27), and the EU's NIS2 Directive provide quite a comprehensive regulatory framework that fosters cybersecurity awareness among the maritime operators, still gaps in their provisions remain, particularly in regard to the newest technological advancements (e.g. automated/unmanned vessels). What is more, with the latest trends being firmly rooted in the deeper digitalization, with AI-driven decision-making and quantum computing advancements the gaps seem to be largely unaddressed. As the said technologies are expected to redefine secure maritime communications, their safe

https://doi.org/10.26219/heal.aueb.5426

integration into the maritime OT remains one of the most pressing concerns. To do so and to improve maritime cyber resilience such aspects as the shortage of maritime cybersecurity professionals, regulatory fragmentation, and the slow adoption of AI-powered anomaly detection must be urgently addressed.

To mitigate the risks identified in this research and improve maritime cybersecurity, the industry must adopt a proactive, multilayered security approach. This includes enhancing IT-OT networks segmentation, with tools such as Purdue Model-based security zoning and Zero Trust Architecture being implemented consistently. What is more, AI-powered threat detection systems are now required as well, to ensure proper network traffic monitoring and real-time detection of anomalies. Additionally, it is vital to strengthen maritime operators' cyber resilience through regulatory compliance. In particular, shipowners must align cybersecurity policies with IMO, IEC 62443, IACS UR E26/E27, and NIS2 guidelines. This will ensure standardized global compliance. Classification societies, on their part, should expand cybersecurity auditing requirements to enforce stricter cyber hygiene measures on newbuild ships and already existing vessels.

Besides this, mandatory crew training programs should be developed to educate maritime professionals on the constantly evolving range of cyber risk, forging comprehensive cybersecurity culture within the industry members. Finally, in the view of the constantly evolving technology, the maritime industry should begin preparing for post-quantum cryptographic standards to safeguard shipboard communication systems and satellite navigation data against emerging threats.

Drawing the final line, it is necessary to highlight that autonomous shipping, AI-driven logistics, and blockchain-based port operations will shape the future of maritime OT. They will present both unparalleled opportunities but also expose the industry to constantly evolving cyber risks. To navigate this complex landscape, maritime organizations must embrace cybersecurity as a foundational pillar of digital transformation. Only in doing so could it be possible to ensure long-term operational resilience, regulatory compliance, ultimately removing the danger of disruption to global trade flows.

https://doi.org/10.26219/heal.aueb.5426

Bibliography

Aakko-Saksa, P. T., Lehtoranta, K., Kuittinen, N., Järvinen, A., Jalkanen, J. P., Johnson, K., ... & Timonen, H. (2023). Reduction in greenhouse gas and other emissions from ship engines: Current trends and future options. Progress in Energy and Combustion Science, 94, 101055.

Abbatemarco, N., Salviotti, G., D'Ignazio, C., & De Rossi, L. M. (2024). Understanding Leadership Competencies in Cyber Crisis Management: Insights from the Maersk Global Supply Chain Meltdown.

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. Ocean & Coastal Management, 236, 106493.

Ahmed, Y. A., Theotokatos, G., Maslov, I., Wennersberg, L. A. L., & Nesheim, D. A. (2024). Regulatory and legal frameworks recommendations for short sea shipping maritime autonomous surface ships. Marine Policy, 166, 106226.

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity challenges in the maritime sector. Network, 2(1), 123-138.

https://doi.org/10.26219/heal.aueb.5426

Al-Enazi, A., Okonkwo, E. C., Bicer, Y., & Al-Ansari, T. (2021). A review of cleaner alternative fuels for maritime transportation. Energy Reports, 7, 1962-1985.

Aşan, C. (2023). THE ROLE OF CYBER SITUATIONAL AWARENESS OF HUMANS IN SOCIAL ENGINEERING CYBER ATTACKS ON THE MARITIME DOMAIN. Mersin University Journal of Maritime Faculty, 5(2), 22-36.

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2677-2690.

Astrov, I., & Bauk, S. (2024, June). Simulating a cyber-attack on an autonomous sea surface vessel's rudder controller. In 2024 13th Mediterranean Conference on Embedded Computing (MECO) (pp. 1-7). IEEE.

Avramidou, M., Biasin, E., Kamenjasevic, E., Kun, E., & Nisevic, M. (2023, February). Cybersecurity and the NIS2 Directive: regulatory aspects and sectoral perspectives. In Consolidated Proceedings of the Second ECSCI Workshop on Critical Infrastructure Protection and Resilience (pp. 91-92). Steinbeis-Edition.

Baloch, R. (2017). Ethical hacking and penetration testing guide. Auerbach Publications.

Bauk, S., & Dzankic, R. (2024). Smart cargo container tracking and IT security management: Experimental results. Journal of Maritime Research, 21(2), 128-134.

Belev, B. C. (2022, May). Purdue Model Implementation in the Shipping Control Systems. In 2022 10th International Scientific Conference on Computer Science (COMSCI) (pp. 1-4). IEEE.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. Information, 13(1), 22.

BIMCO. (2024). The Guidelines on Cyber Security Onboard Ships. https://www.bimco.org/products/publications/titles/the-guidelines-on-cyber-security-onboard-

 https://doi.org/10.26219/heal.aueb.5426

ships/#:~:text=Ships%20and%20shipping%20are%20vulnerable%20to%20cyber%20attacks,incident%20response%20plan%20based%20on%20a%20risk%20assessment.

Butler, K. L., Sarma, N. D. R., Whitcomb, C., Do Carmo, H., & Zhang, H. (1998). Shipboard systems deploy automated protection. IEEE Computer Applications in Power, 11(2), 31-36.

Carlo, A., & Obergfaell, K. (2024). Cyber attacks on critical infrastructures and satellite communications. International Journal of Critical Infrastructure Protection, 46, 100701.

Chaudhry, S. A., Irshad, A., Khan, M. A., Khan, S. A., Nosheen, S., AlZubi, A. A., & Zikria, Y. B. (2021). A lightweight authentication scheme for 6G-IoT enabled maritime transport system. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2401-2410.

Chen, H., Wen, Y., Huang, Y., Xiao, C., & Sui, Z. (2024). Edge Computing Enabling Internet of Ships: A Survey on Architectures, Emerging Applications, and Challenges. IEEE Internet of Things Journal.

Chowdhury, M. M. H., Alshareef, M., Shaheen, M. M. A., & Majumdar, S. (2023). Smart port management practices and implementation: an interpretive structural modelling approach. Bangladesh Maritime J, 7(1).

CyberOwl. (2023, October 17). Maritime cyber risk report: Shipping industry remains “easy target”, pays average US$3.2m in cyberattacks. CyberOwl. Retrieved from https://cyberowl.io/maritime-cyber-risk-report-shipping-industry-remains-easy-target-pays-average-us3-2m-in-cyberattacks/

Dave, D., Sawhney, G., Aggarwal, P., Silswal, N., & Khut, D. (2023, November). The new frontier of cybersecurity: emerging threats and innovations. In 2023 29th International Conference on Telecommunications (ICT) (pp. 1-6). IEEE.

David, M., Gollasch, S., & Hewitt, C. (2024). Global maritime transport and ballast water management. Springer International Publishing.

de la Peña Zarzuelo, I. (2021). Cybersecurity in ports and maritime industry: Reasons for raising awareness on this issue. Transport Policy, 100, 1-4.

Dimakopoulou, A., & Rantos, K. (2024). Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2. 0. Journal of Marine Science and Engineering, 12(6), 919.

Dizaj, M. H., & Shishvan, S. C. (2024). Using High-Throughput Satellites-HTS in Direct Broadcast Satellite (DBS) communications to increase data transmission capacity and improve video quality, especially for high-resolution content such as 4K and 8K. J. Appl. Res. Electr, 2(5), 13-23.

DNV. (2024). Ship classification - Fleet in service: Cyber secure class notation. DNV. Retrieved from https://www.dnv.com/services/cyber-secure-class-notation-124600/#:~:text=Since%202018%2C%20DNV%E2%80%99s%20Cyber%20Secure%20class%20notation%20has,and%20to%20vessels%20and%20offshore%20units%20in%20operation.

Drazovich, L., Brew, L., & Wetzel, S. (2021, July). Advancing the state of maritime cybersecurity guidelines to improve the resilience of the maritime transportation system. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 503-509). IEEE.

Durlik, I., Miller, T., Cembrowska-Lech, D., Krzemińska, A., Złoczowska, E., & Nowak, A. (2023). Navigating the sea of data: a comprehensive review on data analysis in maritime IoT applications. Applied Sciences, 13(17), 9742.

Edwards, F., Szyliowicz, J., Goodrich, D., Medigovich, W., Lange, L., & Anderton, A. (2021). Surface Transportation supply chain security: Creating a blueprint for future research.

Elmay, F. K., Salah, K., Jayaraman, R., & Omar, I. A. (2022). Using NFTs and blockchain for traceability and auctioning of shipping containers and cargo in maritime industry. IEEE Access, 10, 124507-124522.

Fenton, A. J. (2024). Preventing Catastrophic Cyber–Physical Attacks on the Global Maritime Transportation System: A Case Study of Hybrid Maritime Security in the Straits of Malacca and Singapore. Journal of Marine Science and Engineering, 12(3), 510.

 https://doi.org/10.26219/heal.aueb.5426

Fenton, A. J., & Chapsos, I. (2023). Ships without crews: IMO and UK responses to cybersecurity, technology, law and regulation of maritime autonomous surface ships (MASS). Frontiers in Computer Science, 5, 1151188.

Fukuto, J. (2021). Automation levels of automated/autonomous ships. ClassNK technical journal, 2, 35-50.

Gattuso, D., & Pellicanò, D. S. (2023). Perspectives for ports development, based on automated container handling technologies. Transportation Research Procedia, 69, 360-367.

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. Computers & Security, 103, 102196.

Harish, A. V., Tam, K., & Jones, K. (2024). BridgeInsight: An asset profiler for penetration testing in a heterogeneous maritime bridge environment. Maritime Technology and Research, 6(1), 266818-266818.

Haugli-Sandvik, M. (2024). Cyber Risk Perception in Offshore Operations: An Exploratory Study of Deck Officers' Perceptions of Cyber Risks in Norwegian Shipping Companies.

Haugli-Sandvik, M., Lund, M. S., & Bjørneseth, F. B. (2024). Maritime decision-makers and cyber security: deck officers' perception of cyber risks towards IT and OT systems. International Journal of Information Security, 1-19.

Hilden, M. (2023). "Utopia at Sea" from the Captain's Chair: Are Autonomous Ships the Real Solution to Human Error?. In Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance (pp. 31-62). Cham: Springer International Publishing.

Ilcus, C. (2023). Revision of the EU's Integrated Maritime Policy: an Opportunity for Developing Maritime Power?. Available at SSRN 4662584.

International Association of Classification Societies (IACS). (2023):

a) UR E26 Rev.1: Cyber resilience of ships. International Association of Classification Societies.

https://doi.org/10.26219/heal.aueb.5426

b) UR E27 Rev.1: Cyber resilience of on-board systems and equipment. International Association of Classification Societies.

Islam, M. S. (2024). Navigating modern era at sea: legal challenges and opportunities of unmanned and autonomous shipping. AI and Ethics, 1-14.

Issa, M., Ilinca, A., Ibrahim, H., & Rizk, P. (2022). Maritime autonomous surface ships: Problems and challenges facing the regulatory process. Sustainability, 14(23), 15630.

Jhanjhi, N. Z., & Shah, I. A. (Eds.). (2024). Navigating Cyber Threats and Cybersecurity in the Logistics Industry. IGI Global.

Johnson, W., & Wisniewski, B. (2020, October). Cyber Security: Supply Chain Risk Management and Defense-in-Depth requirements for Maritime Systems. In Conference Proceedings of INEC.

Kanellopoulos, A. N. (2024). Enhancing Cyber Security and Counterintelligence in the Shipping Industry. National security and the future, 25(1), 137-154.

Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C. H. (2024). Maritime cybersecurity: are onboard systems ready?. *Maritime Policy & Management*, *51*(3), 484-502.

Kapalidis, C., Karamperidis, S., Watson, T., & Koligiannis, G. (2022). A Vulnerability Centric System of Systems Analysis on the Maritime Transportation Sector Most Valuable Assets: Recommendations for Port Facilities and Ships. Journal of Marine Science and Engineering, 10(10), 1486.

Kara Balci, Ö., Varan Samut, İ., & Ademuni-Odeke. (2024). An evaluation of cyber-worthiness and related factors in maritime safety and maritime security. Journal of International Maritime Safety, Environmental Affairs, and Shipping, 8(4), 2411180.

Karim, M. S. (2022). Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?. Marine Policy, 143, 105138.

Karlsson, M., Liu, M., Li, H., Haraldson, S., Lind, M., Mishra, M., ... & Lind, K. (2024, October). Digital twins for resource optimization in multi-purpose ports: A design

https://doi.org/10.26219/heal.aueb.5426

approach for data-driven decision making. In Journal of Physics: Conference Series (Vol. 2867, No. 1, p. 012055). IOP Publishing.

Kathayat, D. (2022). International Maritime Organization and Cyber Risk Management Framework. Supremo Amicus, 31, 67.

Kavallieratos, G., Diamantopoulou, V., & Katsikas, S. K. (2020). Shipping 4.0: Security requirements for the cyber-enabled ship. IEEE Transactions on Industrial Informatics, 16(10), 6617-6625.

Kayisoglu, G., Bolat, P., & Tam, K. (2022). Evaluating SLIM-based human error probability for ECDIS cybersecurity in maritime. The Journal of Navigation, 75(6), 1364-1388.

Kayisoglu, G., Duzenli, E., Bolat, P., & Bolat, F. (2024). Maritime Cyber Security: Adopting a Checklist Based on IACS UR E26 Standard. Turkish Journal of Maritime and Marine Sciences, (Özel Sayı Erken Görünüm Makaleler), 1-20.

Kayişoğlu, G., Güneş, B., & Bolat, P. (2024). ECDIS Cyber Security Dynamics Analysis based on the Fuzzy-FUCOM Method. Transactions on Maritime Science, 13(1).

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.

Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. International Journal of Critical Infrastructure Protection, 37, 100526.

Keskin, O. F., Caramancion, K. M., Tatar, I., Raza, O., & Tatar, U. (2021). Cyber third-party risk management: A comparison of non-intrusive risk scoring reports. *Electronics*, *10*(10), 1168.

Kim, D., Lee, C., Park, S., & Lim, S. (2022). Potential liability issues of AI-based embedded software in maritime autonomous surface ships for maritime safety in the Korean maritime industry. Journal of Marine Science and Engineering, 10(4), 498.

https://doi.org/10.26219/heal.aueb.5426

Kim, D., Lee, C., Park, S., & Lim, S. (2022). Potential liability issues of AI-based embedded software in maritime autonomous surface ships for maritime safety in the Korean maritime industry. Journal of Marine Science and Engineering, 10(4), 498.

Kolios, A. (2024). Retrofitting Technologies for Eco-Friendly Ship Structures: A Risk Analysis Perspective. Journal of Marine Science and Engineering, 12(4), 679.

Kumar, P., Gupta, G. P., Tripathi, R., Garg, S., & Hassan, M. M. (2021). DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems. IEEE Transactions on Intelligent Transportation Systems, 24(2), 2472-2481.

Kuznetsov, A., Kirichenko, A., & Zboinov, A. (2021). Influence of a cargo plan on the container ship port turnaround time. In E3S Web of Conferences (Vol. 244, p. 08011). EDP Sciences.

Lam, J. S. L., Li, Q., & Pu, S. (2021). Volatility and uncertainty in container shipping market. In New Maritime Business: Uncertainty, Sustainability, Technology and Big Data (pp. 11-32). Springer International Publishing.

Leander, B., Čaušević, A., & Hansson, H. (2019, August). Applicability of the IEC 62443 standard in Industry 4.0/IIoT. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).

Li, M. W., Lei, Y. Z., Yang, Z. Y., Huang, H. P., & Hong, W. C. (2024). An optimization method for maintenance routing and scheduling in offshore wind farms based on chaotic quantum Harris hawks optimization. Ocean Engineering, 308, 118306.

Li, Z., & Li, S. (2024, October). An Integrated Mathematical Model and an Enhanced Quantum-Computing Algorithm for the Berth and Quay Crane Optimization Problem. In Chinese Intelligent Systems Conference (pp. 666-674). Singapore: Springer Nature Singapore.

Liu, J., Zhang, H., & Zhen, L. (2023). Blockchain technology in maritime supply chains: applications, architecture and challenges. International Journal of Production Research, 61(11), 3547-3563.

https://doi.org/10.26219/heal.aueb.5426

Luchenko, D., Georgiievskyi, I., & Bielikova, M. (2023). Challenges and developments in the public administration of autonomous shipping. Lex Portus, 9, 20.

Makkonen, H., Nordberg-Davies, S., Saarni, J., & Huikkola, T. (2022). A contextual account of digital servitization through autonomous solutions: Aligning a digital servitization process and a maritime service ecosystem transformation to autonomous shipping. Industrial Marketing Management, 102, 546-563.

Maljković, M., Vukša, S., Vidan, P., & Pavić, I. (2022). Review of Cargo Operations on Crude Oil Tankers and Methods/Models Used for Optimisation and Improvement of Safety. Časopis Pomorskog fakulteta Kotor-Journal of Maritime Sciences, 23(1/2022), 153-164.

Malone, I., & Strouboulis, A. (2022). Emerging Risks in the Marine Transportation System (MTS), 2001-2021.

Marchand, A., Imine, Y., Ouarnoughi, H., Tarridec, T., & Gallais, A. (2023). Firmware integrity protection: A survey. IEEE Access, 11, 77952-77979.

Martínez, F., Sànchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernàndez-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. International Journal of Information Security, 23(2), 1429-1457.

May, P., & Holcova, P. (2023, November 7). Inside job: How a hacker helped cocaine traffickers infiltrate Europe's biggest ports. Organized Crime and Corruption Reporting Project (OCCRP). Retrieved from https://www.occrp.org

Mba, J. U. (2024). Advancing sustainability and efficiency in maritime operations: Integrating green technologies and autonomous systems in global shipping. Int J Sci Res Arch, 13(02), 2059-2079.

Mellqvist, J., & Jacobo, A. V. C. (2021). Best practice report on compliance monitoring of ships with respect to current and future IMO regulation. Retrieved from https://research.chalmers.se/en/publication/523049

https://doi.org/10.26219/heal.aueb.5426

Merz, M., Grøtli, E. I., Mørkrid, O. E., Tangstad, E., Fossøy, S., & Nordahl, H. (2023). A gap analysis for automated cargo handling operations with geared vessels frequenting small sized ports. Maritime Transport Research, 5, 100098.

Mohsendokht, M., Li, H., Kontovas, C., Chang, C. H., Qu, Z., & Yang, Z. (2024). Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades. Ocean Engineering, 312, 119078.

Molęda, M., Małysiak-Mrozek, B., Ding, W., Sunderam, V., & Mrozek, D. (2023). From corrective to predictive maintenance—A review of maintenance approaches for the power industry. Sensors, 23(13), 5970.

Munim, Z. H., Saha, R., Schøyen, H., Ng, A. K., & Notteboom, T. E. (2022). Autonomous ships for container shipping in the Arctic routes. Journal of Marine Science and Technology, 27(1), 320-334.

Neugebauer, J., Heilig, L., & Voß, S. (2024). Digital twins in the context of seaports and terminal facilities. Flexible Services and Manufacturing Journal, 1-97.

Neumann, T. (2024). Cybersecurity in Maritime Industry. TransNav: International Journal on Marine Navigation & Safety of Sea Transportation, 18(4).

Nganga, A., Lützhöft, M., Scanlan, J., & Mallam, S. (2022). Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment. CYBER 2022 : The Seventh International Conference on Cyber-Technologies and Cyber-Systems, ISBN: 978-1-61208-996-6

NHL Stenden University of Applied Sciences. (n.d.). Maritime Cyber Attack Database (MCAD). NHL Stenden. Retrieved from https://www.nhlstenden.com/en/maritime-cyber-attack-database

Niknami, N., Srinivasan, A., St. Germain, K., & Wu, J. (2023). Maritime Communications—Current State and the Future Potential with SDN and SDR. Network, 3(4), 563-584.

Nowikowska, M. (2022). The main tasks of the network of computer security incident response teams in the light of the act on the national cybersecurity system in Poland. Cybersecurity in Poland: Legal Aspects, 223-241.

Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies. World Journal of Advanced Science and Technology, 5(1), 026-030.

Okumus, D., Gunbeyaz, S. A., Kurt, R. E., & Turan, O. (2023). Towards a circular maritime industry: Identifying strategy and technology solutions. Journal of Cleaner Production, 382, 134935.

Onshus, T., Bodsberg, L., Hauge, S., Jaatun, M. G., Lundteigen, M. A., Myklebust, T., ... & Wille, E. (2022). Security and independence of process safety and control systems in the petroleum industry. Journal of Cybersecurity and Privacy, 2(1), 20-41.

Papastergiou, S., Kalogeraki, E. M., Polemi, N., & Douligeris, C. (2021). Challenges and issues in risk assessment in modern maritime systems. Advances in Core Computer Science-Based Technologies: Papers in Honor of Professor Nikolaos Alexandris, 129-156.

Paraskevas, A., Madas, M., Zeimpekis, V., & Fouskas, K. (2024). Smart ports in industry 4.0: A systematic literature review. Logistics, 8(1), 28.

Paridaens, H., & Notteboom, T. (2022). Logistics integration strategies in container shipping: A multiple case-study on Maersk Line, MSC and CMA CGM. Research in Transportation Business & Management, 45, 100868.

Pasha, J., Dulebenets, M. A., Fathollahi-Fard, A. M., Tian, G., Lau, Y. Y., Singh, P., & Liang, B. (2021). An integrated optimization method for tactical-level planning in liner shipping with heterogeneous ship fleet and environmental considerations. Advanced Engineering Informatics, 48, 101299.

Pfaff, M. (2022). Ship Operation Technology. Springer Fachmedien Wiesbaden.

Phillipson, F. (2024). Quantum computing in logistics and supply chain management an overview. arXiv preprint arXiv:2402.17520.

https://doi.org/10.26219/heal.aueb.5426

Pietrzykowski, Z., Wołejsza, P., Nozdrzykowski, Ł., Borkowski, P., Banaś, P., Magaj, J., ... & Nozdrzykowska, M. (2022). The autonomous navigation system of a sea-going vessel. Ocean Engineering, 261, 112104.

Potter, A., Wang, Y., & Naim, M. (2024). Scaling-up 5G adoption in smart ports: barriers and enablers. Maritime Policy & Management, 1-18.

Progoulakis, I., Nikitakos, N., Dalaklis, D., Christodoulou, A., Dalaklis, A., & Yaacob, R. (2023). Digitalization and cyber physical security aspects in maritime transportation and port infrastructure. In Smart Ports and Robotic Systems: Navigating the Waves of Techno-Regulation and Governance (pp. 227-248). Cham: Springer International Publishing.

Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. Journal of Marine Science and Engineering, 9(12), 1384.

Rajaram, P., Goh, M., & Zhou, J. (2022, July). Guidelines for cyber risk management in shipboard operational technology systems. In Journal of Physics: Conference Series (Vol. 2311, No. 1, p. 012002). IOP Publishing.

Revuru, S. (2024, November). Ensuring Maritime Cyber resilience. In *Conference Proceedings of INEC* (Vol. 2024).

Richter, F. (2021, March 26). The steep rise in global seaborne trade. Statista. Retrieved from https://www.statista.com/chart/24527/total-volume-of-global-sea-trade/

Rinaldy, D. Y. (2022, August). Reliability of International Safety Management (ISM) Code Implementation in Operational Risk Management of Shipping Industry. In Proceedings of International Conference on Economics Business and Government Challenges (Vol. 1, No. 1, pp. 56-64).

Riyadh, M. (2024). Transforming the Shipping Industry with Autonomous Ships and Artificial Intelligence. Maritime Park: Journal of Maritime Technology and Society, 80-85.

https://doi.org/10.26219/heal.aueb.5426

Riyadh, M. (2024). Transforming the Shipping Industry with Autonomous Ships and Artificial Intelligence. Maritime Park: Journal of Maritime Technology and Society, 80-85.

Rodrigue, J. P., & Notteboom, T. (2024). CONCEPT 3. PORT TERMINALS. The Geography of Transport Systems, 187.

Roshanaei, M. (2023). Cybersecurity Preparedness of Critical Infrastructure—A National Review. Journal of Critical Infrastructure Policy• Volume, 4(1).

Ruohonen, J. (2024). A Systematic Literature Review on the NIS2 Directive. Cornell University. arXiv preprint arXiv:2412.08084. https://doi.org/10.48550/arXiv.2412.08084

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. Sustainability, 15(18), 13369.

Senarak, C. (2024). Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases. Maritime Economics & Logistics, 26(1), 105-130.

Setiawan, A., Hasugian, S., Sri Wahyuni, A. A. I., Widyaningsih, U., Wiratno, D., Umasangadji, F., & AH Hammad, J. (2024). Maritime Fleet Management Transformation Using Big Data and IoT. Maritime Fleet Management Transformation Using Big Data and IoT (August 12, 2024).

Simola, J., Paavola, J., Satopää, P., & Vanharanta, J. (2024, June). The Impact of Operational Technology Requirements in Maritime Industries. In European Conference on Cyber Warfare and Security (Vol. 23, No. 1, pp. 516-525).

Sindiramutty, S. R., Jhanjhi, N. Z., Tan, C. E., Khan, N. A., Shah, B., & Manchuri, A. R. (2024). Cybersecurity measures for logistics industry. In Navigating Cyber Threats and Cybersecurity in the Logistics Industry (pp. 1-58). IGI Global.

Singh, C. (2023). The European Approach to Cybersecurity in 2023: A Review of the Changes Brought in By the Network and Information Security 2 (NIS2) Directive 2022/2555. International Company and Commercial Law Review, 5, 251-261.

https://doi.org/10.26219/heal.aueb.5426

Singh, S., & Kumar, D. (2024). Enhancing cyber security using quantum computing and artificial intelligence: A review. algorithms, 4(3).

Skok, S., Aksentijevic, S., Tijan, E., & Jardas, V. (2024, December). Enhancing Maritime Port Sustainability: The Impact of Smart Energy Management Systems-Review with Proposed Novel Solution. In 2024 25th International Middle East Power System Conference (MEPCON) (pp. 1-6). IEEE.

Skredderberget, A. (2017). The first ever zero emission, autonomous ship. Yara International. Retrieved from https://www.yara.com/knowledge-grows/game-changer-for-the-environment/

Śliwiwński, M., & Piesik, E. (2019). Integrated approach for functional safety and cyber security management in maritime critical infrastructures. Journal of Polish Safety and Reliability Association, 10(1).

Soner, O., Kayisoglu, G., Bolat, P., & Tam, K. (2024). Risk sensitivity analysis of AIS cyber security through maritime cyber regulatory frameworks. Applied Ocean Research, 142, 103855.

Sotirov, M. K., Petrova, V. M., & Dimitrov, D. P. (2024). Theoretical Framework for Future Developments: AI-Based Predictions and Risk Assessment for Coastal Ports in the Bulgarian Sector of the Black Sea.

Sravani, P. (2023, March 5).Maritime Cybersecurity: A Potential Threat to India's National Security. Modern Diplomacy, All Views, All Voices. https://moderndiplomacy.eu/2023/03/05/maritime-cybersecurity-a-potential-threat-to-indias-national-security/

Stoddart, K. (2022). Gaining access: attack and defense methods and legacy systems. In Cyberwarfare: Threats to critical infrastructure (pp. 227-280). Cham: Springer International Publishing.

Stoumpos, S., Bolbot, V., Theotokatos, G., & Boulougouris, E. (2022). Safety performance assessment of a marine dual fuel engine by integrating failure mode, effects and criticality analysis with simulation tools. Proceedings of the Institution of

https://doi.org/10.26219/heal.aueb.5426

Mechanical Engineers, Part M: Journal of Engineering for the Maritime Environment, 236(2), 376-393.

Sullivan, B. P., Arias Nava, E., Desai, S., Sole, J., Rossi, M., Ramundo, L., & Terzi, S. (2021). Defining Maritime 4.0: Reconciling principles, elements and characteristics to support maritime vessel digitalisation. IET Collaborative Intelligent Manufacturing, 3(1), 23-36.

Symes, S., Blanco-Davis, E., Graham, T., Wang, J., & Shaw, E. (2024). The survivability of autonomous vessels from cyber-attacks. Journal of Marine Engineering & Technology, 1-23.

Tauqeer, O. B., Jan, S., Khadidos, A. O., Khadidos, A. O., Khan, F. Q., & Khattak, S. (2021). Analysis of security testing techniques. Intelligent Automation & Soft Computing, 29(1), 291-306.

The International Maritime Organization (IMO) (2017) RESOLUTION MSC.428(98), (adopted on 16 June 2017), MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS. Retrieved from https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

Theotokatos, G., Dantas, J. L. D., Polychronidi, G., Rentifi, G., & Colella, M. M. (2023). Autonomous shipping—an analysis of the maritime stakeholder perspectives. WMU Journal of Maritime Affairs, 22(1), 5-35.

Tjahjono, A., & Gemilang, M. (2023, February). Implementation of regulation of the minister of transportation no. 7 of 2019 against the installation of automatic identification system (AIS) on ferriage ships operating in the Ketapang-Gilimanuk and Ketapang-Lembar. In AIP Conference Proceedings (Vol. 2675, No. 1). AIP Publishing.

Tushir, B., Sehgal, H., Nair, R., Dezfouli, B., & Liu, Y. (2021). The impact of dos attacks onresource-constrained iot devices: A study on the mirai attack. arXiv preprint arXiv:2104.09041.

TÜV SÜD. (2021). IEC 62443 industrial security standards: An introduction to the framework /White paper/. TÜV SÜD South Asia. Retrieved from

https://doi.org/10.26219/heal.aueb.5426

https://www.tuvsud.com/en-za/-/media/regions/in/pdf-files/resource-center/whitepapers/tuv-sud-iec-62443-industrial-security-standards.pdf

Ungureanu, M. A., Gavan, E., & Gasparotti, C. (2024). Securing innovation at sea: Cyber risk management for SMEs in ship design. Annals of" Dunarea de Jos" University of Galati. Fascicle XI Shipbuilding, 47, 89-100.

Verkoelen, C. (2022, September). Maritime cybersecurity. In Conference Proceedings of iSCSS (Vol. 2022). Retrieved from https://library.imarest.org/record/10734?p=%28+%28Conference+%2B+Proceedings+%2B+of+%2B+iSCSS%29%29&v=pdf

Visky, G., Šiganov, A., ur Rehman, M., Vaarandi, R., Bahşi, H., Bahsi, H., & Tsiopoulos, L. (2024, September). Hybrid Cybersecurity Research and Education Environment for Maritime Sector. In 2024 IEEE International Conference on Cyber Security and Resilience (CSR) (pp. 644-651). IEEE.

Wang, F. (2024). The role of insurance in regulating cyber risks in the shipping industry. In Research Handbook on Marine Insurance Law (pp. 306-332). Edward Elgar Publishing.

Wang, Q. (2024). Maritime law enforcement concerning offshore energy platforms: Navigating international law constraints and challenges. Marine Policy, 170, 106370.

Weaver, G. A., Feddersen, B., Marla, L., Wei, D., Rose, A., & Van Moer, M. (2022). Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach. Transportation Research Part C: Emerging Technologies, 137, 103423.

Weng, Z., Chi, L., Drewniak, J. L., de Paulis, F., Zhu, Y., & Qi, Y. (2022). An 1.7–2.7 GHz all-weather broadband High-gain antenna with W-shape reflector for maritime communications. AEU-International Journal of Electronics and Communications, 155, 154339.

Werbińska-Wojciechowska, S., Giel, R., & Winiarska, K. (2024). Digital twin approach for operation and maintenance of transportation system—Systematic review. Sensors, 24(18), 6069.

https://doi.org/10.26219/heal.aueb.5426

Wilson, A., Menzies, R., Morarji, N., Foster, D., Mont, M. C., Turkbeyler, E., & Gralewski, L. (2024). Multi-Agent Reinforcement Learning for Maritime Operational Technology Cyber Security. arXiv preprint arXiv:2401.10149.

Xing, W. (2024). Contemplating Maritime Autonomous Surface Ships (MASS) under the international law on ship-source pollution. Marine Pollution Bulletin, 207, 116884.

Xylouris, G., Nomikos, N., Kalafatelis, A., Giannopoulos, A., Spantideas, S., & Trakadas, P. (2024). Sailing into the future: technologies, challenges, and opportunities for maritime communication networks in the 6G era. Frontiers in Communications and Networks, 5, 1439529.

Yan, R., Wang, S., & Psaraftis, H. N. (2021). Data analytics for fuel consumption management in maritime transportation: Status and perspectives. Transportation Research Part E: Logistics and Transportation Review, 155, 102489.

Yara (2024, April 28), Yara Birkeland, two years on. Yara International. Retrieved from https://www.yara.com/knowledge-grows/yara-birkeland-two-years-on/?_gl=1*1agsh6j*_up*MQ..*_ga*NTA1MTk2NDU4LjE3NDAxMTIzNDk.*_ga_W5MJZ2GTWV*MTc0MDExMjM0OS4xLjEuMTc0MDExMzQyNS4wLjAuMA..*_ga_FJB1LTWP77*MTc0MDExMjM0OS4xLjEuMTc0MDExMzQyNS4wLjAuMTU3NDAzMjA3Mg..

Yoo, Y., & Park, H. S. (2021). Qualitative risk assessment of cybersecurity and development of vulnerability enhancement plans in consideration of digitalized ship. Journal of Marine Science and Engineering, 9(6), 565.

Yu, H., Fang, Z., Fu, X., Liu, J., & Chen, J. (2021). Literature review on emission control-based ship voyage optimization. Transportation Research Part D: Transport and Environment, 93, 102768.

Zhang, M., Tsoulakos, N., Kujala, P., & Hirdaris, S. (2024). A deep learning method for the prediction of ship fuel consumption in real operational conditions. Engineering Applications of Artificial Intelligence, 130, 107425.

Ziajka-Poznańska, E., & Montewka, J. (2021). Costs and benefits of autonomous shipping—a literature review. Applied Sciences, 11(10), 4553.

https://doi.org/10.26219/heal.aueb.5426