FINAL THESIS

CYBER SECURITY OF MERCHANT SHIPS

AUTHOR: SUMIT MEHAN

Acknowledgements

Completing this thesis has been a challenging yet rewarding experience. This past year brought significant growth, learning, and reflection. I owe much of this to the support of those around me. As I close this chapter, I want to thank everyone who contributed to this achievement. I extend my thanks to Professor Albert Veenstra, my thesis supervisor. Your guidance and feedback were crucial. You challenged me to think critically and inspired me to expand my understanding. Your expertise and patience formed the foundation of this thesis.

I also appreciate my professors and the academic staff for their dedication and passion for teaching. Your collective knowledge and insights have profoundly shaped my understanding of the maritime industry, and I look forward to applying what I've learned in my future career. A special thanks to the program office for always being there to address any concerns and for ensuring our journey was smooth and fulfilling.

To my family, words cannot fully express my gratitude for your love and support. To my wife, you have been my anchor through this journey. Your support and sacrifices allowed me to chase my dream while away from home. You took on many responsibilities so I could concentrate on my work. I will always appreciate that. Your laughter and joy are my greatest motivation, even from afar. Knowing I am working for a better future for us keeps me going during tough times.

Thank you to my friends and colleagues who stood by me this year. Your support and trust provided comfort and inspiration. Late-night calls, messages, and shared laughter reminded me of the importance of connection, even at a distance. To my classmates, now lifelong friends, sharing this journey has been a highlight. From intense discussions to shared meals, every moment has been better with you. Our diverse backgrounds united by a shared passion for this field created lasting memories. I believe we will continue to support and inspire each other as we move forward.

This thesis reflects my efforts and the incredible people who supported me throughout this journey. I appreciate all of you for making this possible.

Abstract

The maritime industry's rapid digital transformation has introduced advanced technologies, enhancing operational efficiency and safety. However, this progress has also exposed vessels to significant cybersecurity risks, such as phishing, ransomware, GPS spoofing, and malware attacks, threatening global supply chains and maritime safety. Despite regulatory frameworks like IMO Resolution MSC.428(98) and IACS Unified Requirements E26/E27, critical gaps remain in equipping crews to address real-world cybersecurity challenges effectively.

This thesis bridges these gaps by shifting the focus from compliance driven protocols to enhancing crew readiness through tailored training programs. Using a mixed-methods research approach, the study integrates semi-structured interviews with cybersecurity experts and thematic analysis to identify vulnerabilities, challenges, and limitations in current practices. Findings highlight the need for vessel-specific resilience assessments, proactive vulnerability testing, and scenario-based training to prepare crews for evolving cyber threats.

The research introduces a structured cyber resilience test protocol incorporating risk-based approaches, layered defence strategies, and real-world simulations. These protocols focus on improving crew preparedness by enabling early threat detection and effective incident response. By aligning with international standards like the ISPS and ISM Codes, the study ensures these measures are practical, scalable, and adaptable to diverse vessel types.

Furthermore, the study emphasises the integration of technical defences with human-centric solutions. By leveraging continuous learning models, predictive analytics, and iterative training exercises, the research aims to build genuine resilience within maritime operations. This work not only contributes to the academic understanding of maritime cybersecurity but also offers actionable solutions for the industry, safeguarding global trade and ensuring operational continuity in an increasingly digitised era.

Table of Contents

Chapter 1: Introduction

Section 1.1: Background

The maritime industry has undergone significant changes due to the adoption of advanced digital technologies. Automated and interconnected systems, such as the Electronic Chart Display and Information System (ECDIS) and the Automatic Identification System (AIS), have enhanced shipping safety and operational efficiency by reducing human error and enabling real-time decision-making. These advancements have transformed how ships manage navigation, traffic, and cargo logistics through integrated communication networks and advanced data analytics (Nikolov, 2024).

However, this digital transformation has also introduced heightened cybersecurity risks. Modern ships are increasingly vulnerable to threats such as GPS spoofing, ransomware attacks that paralyse systems, and unauthorised access to operational technologies. These threats jeopardise maritime operations' safety and pose significant risks to global supply chains and financial markets (M. Canepa, 1 March 2021)

In response to these challenges, the International Maritime Organization (IMO) mandated in 2017 that ships include cyber risk management in their Safety Management Systems by 2021. Furthermore, the International Association of Classification Societies (IACS) is implementing new standards starting in 2024, requiring cybersecurity measures to be integrated into ship design. The Unified Requirements E26 and E27 focus on critical elements such as protecting equipment from cyber threats, detecting cyber-attacks, and enabling efficient recovery processes (Iacs, 2023).

Despite these regulatory efforts, a critical gap remains in ensuring that maritime crews are prepared to identify, respond to, and recover from real-world cyber threats. While compliance with regulations addresses baseline security requirements, it does not guarantee that crew members possess the skills and knowledge needed to handle complex and evolving cyber incidents effectively. This gap underscores the need for practical, hands-on training programs that equip maritime professionals with the ability to recognise and mitigate cyber risks proactively (Divine C. Chupkemi, 2024).

This thesis aims to bridge this gap by developing a comprehensive framework for enhancing crew training in maritime cybersecurity. Through a combination of risk-based approaches, layered defence strategies, and real-world simulations, this research priorities crew preparedness as the cornerstone of cybersecurity resilience. While protocols for testing and assessing cyber defences are integral to this study, they are framed as tools to enhance the primary focus, building the capabilities of maritime crews to handle cybersecurity threats confidently and effectively (Louise Praestin Jepsen, 2024).

Section 1.2: Research Question, Sub-Research Questions, and Objectives

The shipping industry has increasingly adopted digital systems to enhance efficiency, but this shift has also made ships more vulnerable to cyber-attacks. To address these risks, classification societies, such as Lloyd's Register, have implemented cybersecurity rules based on the standards set by the International Association of Classification Societies (IACS) (Iacs, 2023). These societies are now aligning with IACS guidelines by developing specific auditing plans to ensure ships comply with basic cybersecurity requirements. However, there is still a critical gap. While these audits check whether ships meet minimum cybersecurity standards, they do not evaluate the readiness of crews to handle and recover from actual cyber-attacks. In other words, there is currently no standardised approach to assess or enhance crew preparedness for addressing real-world cybersecurity threats. This gap means that even compliant ships may lack the human readiness to withstand sophisticated attacks effectively (Androjna, 2020).

This thesis aims to fill that gap by developing a cyber resilience framework with a primary focus on enhancing crew training. The framework will provide structured methods to actively test and improve crew readiness, ensuring that maritime personnel are equipped with the knowledge, skills, and confidence to handle cybersecurity incidents. By emphasizing crew training and preparedness, this research intends to lay the foundation for stronger cybersecurity in the maritime industry, ensuring ships are not only compliant but also resilient against evolving cyber threats.

Main Research Question

How can effective test protocols be designed to evaluate and enhance crew readiness for addressing cybersecurity threats in the maritime industry?

Sub-Research Questions

1. **What are the current challenges faced by maritime crews in identifying and responding to cybersecurity threats?**
2. **What training methods and drills are currently used to enhance cybersecurity awareness and preparedness among maritime crews?**
3. **How can threat simulations and vulnerability tests be adapted to improve crew readiness for addressing cybersecurity threats?**

Section 1.3: Research Design and Methodology

In this study, we use a combination of expert interviews and training-focused case studies to develop a practical training program aimed at preparing ship officers to handle cyberattacks effectively, especially in remote maritime environments. The objective is to ensure these officers are not only equipped with theoretical knowledge but also possess the practical skills to confidently manage real-world cybersecurity challenges. The research begins with interviews conducted with maritime cybersecurity experts. These interviews aim to gather insights into the current gaps and challenges in cybersecurity training for ship officers. Experts will share their experiences and perspectives on what constitutes effective training, along with examples of training methods that have been successful in practice. These insights will form the foundation for understanding the current state of cybersecurity training in the maritime industry.

In parallel, the study will analyse case studies of existing training programs used in the maritime and related industries. These case studies will focus on the design, implementation, and outcomes of different training approaches, emphasising how they address the unique challenges of cybersecurity in a maritime context. By evaluating these case studies, the research seeks to identify best practices and strategies that can be adapted to develop a comprehensive training program tailored to the specific needs of maritime crews. By combining the expertise of industry professionals with lessons learned from training-focused case studies, this research ensures a robust and practical approach to enhancing cybersecurity preparedness in the maritime sector.

Section 1.4: Structure of Thesis

This thesis is organised into six chapters to provide a comprehensive exploration of the research topic. **Chapter 1: Introduction** sets the stage by presenting the background of the research, outlining the objectives, defining the research questions, and detailing the overall structure of the thesis. **Chapter 2: Literature Review** examines the current state of cybersecurity in the maritime industry, exploring the evolution of cyber threats and the role of international frameworks and standards. It also highlights critical gaps in current training practices and resilience-building measures. **Chapter 3: Research Methodology** describes the methods used in this study, including expert interviews and case study analysis, to assess crew training needs and guide the design of test protocols. **Chapter 4: Developing Test Protocols** outlines the framework for designing test protocols and training programs, with a focus on simulated drills and hands-on learning to enhance crew preparedness for cyber threats. **Chapter 5: Findings and Implications** summarises the key research findings, offering actionable recommendations for integrating training protocols within the maritime industry and addressing its cybersecurity challenges. Finally, **Chapter 6** concludes the study by addressing the research questions, emphasising the shift to a training-focused framework to enhance maritime crew readiness, and summarizing key contributions. It also highlights limitations and offers recommendations for future research to strengthen cybersecurity training and resilience.

Chapter 2: Literature Review

Section 2.1 - Cybersecurity Challenges and Resilience in Maritime Industry

The maritime industry has undergone a significant transformation in recent decades, shifting from traditional manual operations to a highly digitized environment. Advanced technologies across navigation, communication, and cargo management have created a more interconnected and efficient industry. Tools such as the Electronic Chart Display and Information System (ECDIS) and the Automatic Identification System (AIS) have become standard, improving navigation accuracy, reducing human error, and enhancing situational awareness (Marco Balduzzi, 2014; Tam & Jones, 2019). Additionally, integrated networks and real-time data analytics have streamlined logistics and cargo operations, enabling better tracking of vessel positions, weather conditions, and cargo status (Lund et al., 2021). However, this increased reliance on interconnected systems has also escalated cybersecurity risks, with threats such as GPS spoofing, ransomware attacks, and unauthorized access to operational technologies posing significant risks to the industry. High-profile incidents, such as the 2017 NotPetya attack on Maersk, which caused operational disruptions and financial losses of approximately $300 million (Greenberg, 2018), illustrate the growing threat of cyberattacks on maritime operations.

Despite regulatory efforts, such as the International Maritime Organization's (IMO) Resolution MSC.428(98), which mandates the inclusion of cyber risks in Safety Management Systems (SMS), and the International Association of Classification Societies (IACS) Unified Requirements E26 and E27 aimed at enhancing cyber resilience in ship design, a significant gap remains between compliance and active resilience (International Maritime Organization, 2020). Compliance with these regulations provides a baseline but does not ensure a ship's readiness to withstand sophisticated cyberattacks. Moreover, ships' reliance on third-party vendors for critical services, such as satellite communications and navigation, introduces additional vulnerabilities (Knapp & Sanquist, 2020). Older vessels, which often lack modern cybersecurity infrastructure, face heightened risks, making retrofitting both technically challenging and costly (Kessler & Shepard, 2020). These vulnerabilities underscore the need for active resilience measures that extend beyond regulatory compliance.

While regulations establish minimum standards, the preparedness of ship officers to detect and respond to threats often determines the effectiveness of cybersecurity measures. Training officers

for early detection and mitigation of cyber risks is a critical component of building resilience. Poorly trained crews may fail to identify threats such as phishing or GPS spoofing, resulting in delayed responses and escalated vulnerabilities. Early detection enables swift action, preventing minor risks from evolving into significant disruptions. However, there is currently no standardized protocol for training officers to handle cybersecurity threats effectively, leaving a critical gap in the industry's resilience strategies.

High-profile incidents such as the Maersk ransomware attack underscore this gap, as these events highlight the need for not only robust systems but also adequately trained personnel to manage and recover from such situations. A lack of comprehensive training combined with insufficient testing of shipboard systems creates vulnerabilities that can compromise global supply chains and financial markets.

This literature review aims to bridge this gap by exploring existing methods for assessing and encountering cyber threats in the maritime industry, with a specific focus on training as a critical component of resilience. By evaluating prevalent cybersecurity threats and assessing the effectiveness of regulatory frameworks, this review identifies the limitations of current practices and highlights the importance of integrating training into resilience strategies. This research proposes a structured cyber resilience test protocol that incorporates predictive analytics, comprehensive audits, and regular training exercises to address these challenges. By linking training with active testing, the proposed protocol aims to establish a robust framework for protecting the maritime industry—a cornerstone of the global economy from emerging cyber threats.

SECTION 2.2 - Background on Auditing, Protocols, Drills, and Mechanisms for Security

2.2.1 -Background on Auditing Procedures

Cybersecurity auditing plays a pivotal role in the maritime industry by identifying vulnerabilities in a ship's digital systems and ensuring compliance with industry standards**.** Frameworks like the NIST Cybersecurity Framework and IMO guidelines provide essential baselines for these audits, enabling ships to assess and enhance their resilience against cyber threats (Kessler, 2020). These frameworks guide maritime operators in establishing standardised practices for evaluating the

security posture of both operational and informational systems. By systematically identifying risks, audits ensure that even older vessels with legacy systems can achieve a level of cybersecurity that meets industry expectations. For instance, auditing can uncover risks such as reliance on outdated hardware, insufficient patching schedules, or the lack of multifactor authentication protocols, all of which are critical to maintaining the ship's operational integrity.

Vulnerability scanning acts as a continuous safety check, proactively identifying weak points such as outdated software, misconfigurations, or weak passwords. These scans provide maritime operators with a real-time view of their security posture, enabling them to prioritize and address critical issues. For example, a vulnerability scan might reveal unpatched ECDIS software or misconfigured network access controls that could allow unauthorised intrusion. Such insights are not only essential for securing the ship's digital ecosystem but also for designing effective training programs that address specific vulnerabilities (Elstial, 2024). Integrating automated tools for vulnerability scanning helps in identifying common weaknesses like default passwords or open ports, reducing the reliance on manual checks and improving accuracy.

Penetration testing, or simulated cyberattacks, complements vulnerability scanning by evaluating both technical and human defences. This involves mimicking real-world attack scenarios to determine how well the ship's systems and crew respond to potential threats. For instance, penetration tests may target critical systems like navigation controls, main engines, or cargo management networks to expose vulnerabilities in access controls or encryption protocols. In addition to testing technology, threat simulations such as phishing campaigns or social engineering attempts assess crew readiness and highlight gaps in cybersecurity awareness. The findings from such exercises provide actionable insights for both system upgrades and the development of scenario-based training modules, ensuring that personnel can effectively mitigate similar threats in real-world situations (Armstrong, 2018).

Audits also serve a critical function in maintaining compliance with regulatory standards. Industry frameworks like ISO/IEC 27001 and IMO’s Resolution MSC.428(98) require ships to regularly evaluate their cybersecurity measures as part of Safety Management Systems (SMS). Audits ensure that these requirements are not only met but also adapted to address evolving threats. For example, computational vulnerability scanning of systems like ECDIS and GNSS has revealed

specific weaknesses, such as outdated encryption methods or the susceptibility to jamming attacks, which can be remediated through targeted intervention (Sabillon, 2021).

By conducting comprehensive audits, maritime operators create a feedback loop where identified gaps in cybersecurity measures directly inform the design of training and drills, ultimately building a more robust defence system. For example, audit results can guide the creation of cybersecurity drills focused on phishing simulations or ransomware attack scenarios, equipping crews to handle incidents effectively. This process ensures continuous improvement, addressing both known vulnerabilities and emerging threats to strengthen the overall resilience of maritime operation (Dupont, 2019).

2.2.2 - Cybersecurity Protocols and Drills: Objectives and Impact

Cybersecurity protocols and drills are fundamental to a robust maritime cybersecurity strategy, addressing both technical vulnerabilities and human readiness. Protocols serve as detailed action plans to guide crews during cyber incidents, such as malware infections, GPS spoofing, or ransomware attacks (BIMCO, 2024). These plans typically include steps for isolating affected systems, switching to backup operations, and notifying relevant personnel. For example, protocols for ransomware might involve segregating compromised networks and alerting shoreside support, while GPS spoofing procedures could recommend switching to alternative navigation methods like manual plotting or inertial navigation systems (Sabillon, 2021).

Cybersecurity drills complement these protocols by testing and refining them under realistic conditions. Drills help the crew to familiarise themselves with their roles during specific cyberattacks, such as ransomware or malware disrupting navigation systems. These exercises emphasise quick decision-making, ensuring crew members can respond effectively to minimise operational disruptions (Armstrong, 2018).

Drills also play a critical role in identifying technical vulnerabilities and human response gaps. For instance, simulated phishing attacks can reveal the need for improved training on recognising social engineering tactics, while jamming simulations might highlight weaknesses in contingency plans for navigation systems (Dupont, 2019).

Beyond technical preparedness, these drills cultivate a proactive culture among crew members, reinforcing habits like reporting suspicious activities, using strong passwords, and securing

workstations. Regular exercises not only improve the crew's technical and psychological readiness but also help them remain composed and effective during high-pressure situations, such as coordinated ransomware attacks or system breaches (Kessler, 2019).

By integrating cybersecurity protocols and drills into broader safety training programs, maritime companies can enhance overall preparedness. Combining cyber drills with traditional emergency exercises, such as fire or collision simulations, creates a cohesive and practical training approach. Customising these exercises for ship-specific systems, like ECDIS or GNSS, further improves their relevance and effectiveness (Sabillon, 2021).

In summary, protocols and drills form the backbone of maritime cybersecurity, enabling crews to handle both known and emerging threats. Regular testing and auditing of these measures ensure continuous improvement, strengthening both technical defenses and human readiness across increasingly digitized maritime operations (Bimco, 2024).

Section 2.3 -Fundamental Cyber Security Principles

Introduction to Cybersecurity Models in Maritime Operations

In the maritime industry, where vessels increasingly rely on interconnected digital systems for navigation, communication, and operations, cybersecurity has become a critical focus. This dependence on digital networks exposes ships to vulnerabilities such as malware, GPS spoofing, and system jamming, which can disrupt operations, jeopardise safety, and lead to financial losses. To manage these risks, the maritime sector adopts structured models that offer systematic approaches to identifying, mitigating, and addressing cyber threats in shipboard systems. These models include the **CIA Triad**, the **Maritime Cyber Risk Assessment (MaCRA)**, **Bayesian Networks**, **Attack Graphs**, and **Markov Models**, each of which provides unique insights into the prevention and management of cyber risks.

The **CIA Triad** focuses on three core principles: confidentiality, integrity, and availability. These principles ensure that sensitive information, such as navigation data or crew details, remains protected from unauthorised access, tampering, or disruption. For example, a ship’s power management system monitored by SCADA (Supervisory Control and Data Acquisition) relies on the confidentiality of its data, the integrity of its operations, and the availability of its control functions to maintain safety and efficiency. (Silgado, 2018)

MaCRA (Maritime Cyber Risk Assessment) provides a maritime-specific framework for evaluating cyber threats. By assessing risks based on vulnerabilities, ease of exploitation, and potential rewards for attackers, MaCRA helps maritime operators to prioritise resources and protect high-risk systems. For instance, MaCRA can assess the risks of GPS spoofing in navigation systems or ransomware attacks on a ship's business networks, offering actionable insights to reduce exposure to these threats. (Jones, January 7,2019)

Complementing these models, **Bayesian Networks** offer a probabilistic approach to predicting the progression of cyberattacks. They are particularly valuable for assessing risks in complex, interconnected shipboard systems. For example, Bayesian models can estimate the likelihood of a phishing email leading to unauthorised access to operational technology (OT) systems, allowing operators to prioritise defences effectively. (Martina Pivarníková, November 2020)

Attack Graphs are another practical tool, providing visual representations of potential attack paths through a system's vulnerabilities. They help maritime operators understand how attackers exploit weaknesses, such as unpatched software in Integrated Bridge Systems (IBS), to compromise ship operations. Attack graphs are particularly useful in designing crew training exercises and refining cybersecurity protocols. (Martina Pivarníková, November 2020)

Markov Models address multi-stage and sequential attacks, offering insights into how cascading vulnerabilities can lead to broader disruptions. In a maritime context, this might involve a scenario where GPS spoofing causes navigation errors, which in turn disrupt propulsion systems and compromise operational safety. Markov models highlight the importance of addressing interconnected vulnerabilities to prevent such cascading effects. (Martina Pivarníková, November 2020)

Lastly, **Intrusion Detection Systems (IDS)** serve as real-time monitoring tools to detect and respond to anomalies in shipboard networks. Tools-like Snort can identify unauthorised access attempts or abnormal data traffic, providing immediate alerts to crews and supporting proactive threat mitigation.

Together, these models provide a comprehensive framework for understanding and managing cybersecurity challenges in maritime environments. By integrating general principles like the CIA Triad with maritime-specific tools like MaCRA and leveraging predictive methods such as

Bayesian Networks and Markov Models, the industry can enhance resilience against ship-specific cyber threats. These structured approaches form the foundation for assessing vulnerabilities, designing robust defences, and ensuring the safe and secure operation of modern vessels.

2.3.1 Overview of Cybersecurity Models and Frameworks

CIA TRIAD CYBER SECURITY MODEL (CONFIDENTIALITY, INTEGRITY & AVAILABILITY)

The maritime industry's growing reliance on computerised and interconnected systems makes it an attractive target for cybercriminals. These attackers take advantage of the fact that the industry generates significant revenue, which increases the stakes of a potential attack. The consequences of a successful cyberattack can be devastating for a company.

To protect these systems, companies rely on a cybersecurity model called the CIA triad, which consists of Confidentiality, Integrity, and Availability.

Confidentiality ensures that sensitive information is only accessible to authorised personnel, keeping it private and secure. **Integrity** protects the accuracy of the data, ensuring it is not tampered with, whether intentionally by hackers or accidentally by internal staff. Lastly, **Availability** guarantees that authorised individuals can access important information when needed, especially during critical operations or emergencies.

If any one of these three elements is compromised, the company's security system can be seriously damaged, potentially disrupting operations and exposing vital systems to risk. This can result in financial losses, reputational damage, and operational chaos. (Silgado, 2018)

For example, the ship has a power management system that controls things like power sharing and synchronizing between generators and switchboards. This system helps distribute electricity on the ship. On top of this system is a SCADA (SUPERVISORY CONTROL AND DATA ACQUISITION) system, which monitors and controls the power distribution and gives the crew control over it. Power management is vital for safety and efficiency, as it manages power from the engines, impacting fuel usage. A cyberattack on this system could disrupt operations and safety, so protection measures are essential. (Silgado, 2018)

Result of CIA system for SCADA system

SCADA system	Confidentiality	Integrity	Availability	Overall impact
Sensor data	Low	High	High	High
Statistical data	Low	Low	Low	Low

The SCADA system collects real-time sensor data for (power management) and data about power consumption (used for administrative purposes). The CIA model is used to assess the impact if this data is compromised.

Loss of confidentiality (keeping data secret) of sensor data is low impact, as the crew sees it anyway. Confidentiality means keeping data private or secret. When it comes to sensor data on the ship, like real-time information about power or fuel use, the crew already sees this data on the ship's control systems. Since this information is visible to the crew and not hidden, losing its confidentiality or having it exposed to others is not a big issue. This is why the loss of confidentiality has a low impact because even if someone else sees the data, it doesn't cause major harm or risks.

Loss of integrity (accuracy) and **Availability** (access to the data) of sensor data is a high impact because wrong or unavailable data affects safety. Integrity means the data needs to be accurate. If the sensor data on a ship becomes incorrect or gets changed (loss of integrity), the crew could make wrong decisions about power, which might cause safety problems. Availability means the

data should always be accessible. If the sensor data isn't available (loss of availability), the crew might not know the current power status, which could also lead to safety risks. Both are highly impacted because incorrect or missing data could affect the ship's safety.

For statistical data (power consumption), the loss of confidentiality, integrity, or availability has a low impact because it's mainly used for internal purposes. Statistical data is information about how much power the ship is using. This data is mainly used by the company for internal reports and not for immediate safety decisions. So, if someone else sees it (confidentiality), if it's incorrect (integrity), or if it's temporarily unavailable (availability), it doesn't cause any major problems. That's why the impact is considered low, it's useful but not critical for the ship's day-to-day safety and operations.

2.3.2 MARITIME CYBER SECURITY RISK ASSESSMENT MODEL (MaCRA)

MaCRA is one of the tools which can be used for the risk assessment of Maritime Cyber security. **MaCRA** (Maritime Cyber Risk Assessment) is a tool that helps assess cybersecurity risks specific to ships and maritime operations. It takes a large amount of data and makes it easier to understand by creating different views tailored for various users, such as ship captains, crew members, and insurers, each of whom might care about different aspects of cybersecurity.

For example, while everyone may be looking at the same risk data, MaCRA allows each person to see the information that matters most to them. A captain might focus on risks related to navigation systems, while an insurer might care more about the financial impact of a cyberattack. By providing these customized views, MaCRA makes it easier for different people to grasp the risks in a way that is most relevant to their role.

To make the data easier to work with, MaCRA simplifies complex models of cyber risk. It highlights key factors, such as specific ships, the type of attackers, or the potential consequences of an attack. This allows for a more detailed analysis of risks by considering not just the physical ship but also its environment and operations. In doing so, MaCRA helps increase the overall understanding of cyber risks in the maritime industry and supports better strategies to reduce these threats.

To assess risks, MaCRA uses three main criteria:

Vulnerability: How exposed or weak a system is to cyber threats.

Ease of Exploitation: How easily a hacker can take advantage of this vulnerability.

Reward: What a hacker might gain from attacking the system.

These criteria allow MaCRA to evaluate different threats in a structured way, helping to determine which risks are the most severe and which systems need the most protection.

Vulnerability: How exposed or weak a system is to cyber threats.

In simpler terms, Vulnerability Characteristics refers to the weak points in a ship's technological systems that hackers could exploit, which could lead to serious consequences. For example, one vulnerability might be GPS spoofing, where attackers manipulate the ship's navigation system, potentially sending it off course. This concept is important because some systems that may not seem critical for daily operations could still be weak points that attackers can target.

The MaCRA framework labels this as **a vulnerability** because a ship can have multiple weak points in its technology. While it's impossible to list every potential vulnerability for all ships globally, MaCRA collects enough real-world data to showcase how these vulnerabilities work in practice. Although most vulnerabilities focus on onboard technology (like navigation and communication systems), it's also important to consider external factors like the ship's location, weather, and even the crew members. For instance, crew members might be tricked by phishing emails, or certain geographic locations could make ships more vulnerable to piracy or crime.

As ships become more reliant on advanced technology, assessing cyber risks is crucial for both economic and physical safety. Ships now have Integrated Bridge Systems (IBS), which centralize many control functions, such as navigation and communication. While this makes operations easier, it also creates a prime target for cyberattacks because it concentrates so much valuable data and control in one place. Additionally, IBS systems often connect to the internet, opening the door to external threats like hackers.

This section of MaCRA highlights the need to carefully evaluate technological vulnerabilities and consider external factors (like politics, economics, or the crew's vulnerability to manipulation), to protect ships from potential cyberattacks. (Jones, January 7,2019)

Ease of Exploitation – Hackers can take undue advantage

The main factors such as the crew's experience, the ship's location and the technical set-up of the ship play a major role in determining how easy it is to launch a cyber-attack on the ship. This is termed Ease of Exploitation. For example, if the crew and passengers know potential cyber threats and how to respond, they could stop or reduce the chances of an attack. On the other hand, if they are unaware of how to deal with the situation, they could make it easy for the hackers to succeed in their plan.

Apart from this a ship configuration also plays a major role in cyber security measures such as the use of firewalls indicates how likely a ship could be attacked. The physical location of the ship also plays a major role in being susceptible to cyber-attacks, especially in the piracy area it might be a more attractive target for attackers. Lastly, if a hacker's goal is to steal data, certain ports or networks with weak security like outdated antivirus software could make it easier for them to succeed in their attack (Jones, January 7,2019).

It is important to note that the ease of cyber-attacks depends not just on the technology but also on where the ship is located, how prepared the crew is, and how secure the ship's systems are.

Reward: What a hacker might gain from attacking the system.

The MaCRA framework is designed to understand what motivates hackers to attack, focusing on how valuable they think the result of the attack will be. This helps distinguish between accidental events and intentional cybercrime. To clarify this, the framework categorises different types of hackers and their reasons for attacking.

Here's a simple breakdown of the hacker types:

1. **Activists (Hacktivists):** These hackers pursue ideological goals, seeking social, political, or environmental change. Their actions, such as leaking information or disrupting operations, may inadvertently benefit other attackers or cause damage.

2**. Competitors**: Typically, businesses or governments aim to gain an advantage over rivals, stealing sensitive information or disrupting operations to harm reputation or finances.

3. **Criminals**: Focused on profit, these hackers engage in theft, fraud, blackmail, and selling hacking tools. Their crimes range from aiding piracy to complex operations by organized crime.

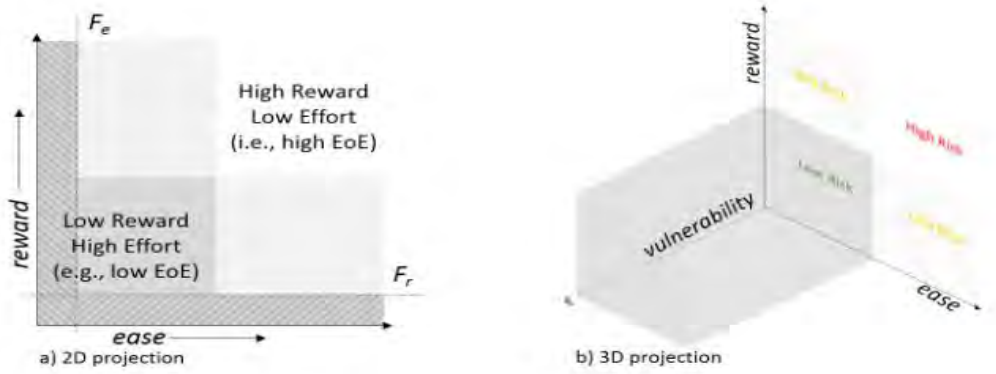
4. **Terrorists**: Aiming for death and destruction, they leverage cyber-attacks to create fear, recruit, steal resources, or turn ships into weapons for attacks.

5**. Elitists**: Primarily interested in showcasing skills, they typically avoid causing harm. They're excluded from MaCRA as their actions rarely result in negative outcomes, though sophisticated hacks could accidentally cause damage.

In summary, MaCRA evaluates hacker motivations to understand and predict potential threats.

Framework Overview

The MaCRA (Maritime Cyber Risk Assessment) framework, as depicted in the image, helps evaluate cyber risks in maritime systems by analyzing three important factors: **reward**, **ease of attack (Effort of Exploit - EoE),** and **vulnerability**. The framework allows these factors to be visualized in both 2D and 3D projections to assess risk levels.



Projection of MaCRA risk quadrants to assess the risk of maritime systems. (Jones, January 7,2019)

In the 2D projection of the left image, MaCRA evaluates two dimensions: the attacker's reward and the ease of attack. Higher rewards make a system a more attractive target, while the effort required (EoE) indicates how easily the system can be compromised. Attacks with high rewards and low effort are the most dangerous and are classified as high-risk. Conversely, systems with low rewards and high difficulty are low risk. In the 3D projection of the right image, a third dimension—vulnerability—is introduced. This indicates the system's exposure to attacks. A system with high vulnerability, high rewards, and low effort poses the greatest risk (high-risk area in red). Systems that are less vulnerable or have stronger defenses present lower rewards or require more effort and thus are lower risk.

By integrating these three factors reward, ease of attack, and vulnerability MaCRA assists maritime organisations in pinpointing major risks and prioritising cybersecurity efforts. High-risk systems, where attackers can achieve significant rewards with minimal effort due to vulnerabilities, require urgent securing. In contrast, well-protected systems that are harder to attack or less rewarding are lower risk and may not need immediate focus.

2.3.3 Bayesian Networks: Detecting Early Cyber Attacks

Bayesian networks are probabilistic models that use statistical relationships to predict the likelihood of events based on observed data. In cybersecurity, they are especially useful for detecting early signs of attacks by analysing patterns and predicting how threats may evolve. These networks consist of nodes, which represent variables such as system vulnerabilities or observed activities, and connections that define the relationships between these variables. In a maritime context, Bayesian networks can model how different components of a ship's digital systems are interconnected, enabling operators to identify potential attack paths based on initial observations. For example, if an unusual email with a suspicious attachment is received at (node A), it might be linked to the likelihood of a phishing attempt (node B), which could then lead to unauthorised access (node C). (Martina Pivarníková, November 2020)

One of the key strengths of Bayesian networks is their ability to detect hidden patterns. Even when an attack hasn't been fully developed, these models can flag unusual behaviour by

analysing small, seemingly unrelated anomalies. For instance, an increase in data traffic coupled with failed login attempts might signal the early stages of a cyberattack. By calculating the probability of various outcomes, Bayesian networks can predict the likelihood of specific threats, providing an early warning system. This capability helps prioritise responses by directing resources to high-risk scenarios. For example, if the network predicts a high probability of a ransomware attack based on observed data traffic and unauthorised user activity, immediate action can be taken to prevent escalation. (Martina Pivarníková, November 2020)

In a maritime context, Bayesian networks adapt and improve over time by learning from previous incidents. This enables them to become increasingly accurate in identifying early warning signs, such as abnormal data traffic, suspicious logins, or phishing attempts. For instance, if a crew member receives a phishing email and there's a sudden spike in outgoing data traffic, the network can connect these events and alert the crew to investigate before significant damage occurs. By leveraging these predictive capabilities, Bayesian networks provide a proactive approach to cybersecurity, allowing maritime operators to detect and mitigate threats before they escalate into severe disruptions. (Martina Pivarníková, November 2020)

Markov Models

Markov models are statistical tools used in cybersecurity to detect early signs of attacks by analyzing patterns in system behaviour. They work by creating a baseline of what is considered normal activity in a system, such as typical user actions, data flows, or network communications. Once this baseline is established, the model compares ongoing activities to detect anomalies or unusual patterns. For example, if there is a sudden surge in outgoing data traffic or repeated failed login attempts, the Markov model can identify these events as suspicious because they deviate from the expected pattern. (Ye, 2004)

What makes Markov models particularly useful is their ability to link sequences of events, allowing them to detect multi-step attacks. For instance, a phishing email might lead to an unauthorized login attempt, followed by abnormal data access. By connecting these steps, the model can predict the likelihood of an attack in progress and even anticipate what might happen next. Additionally, Markov models adapt over time, learning from new data to improve their

accuracy and reduce false alarms. This dynamic nature ensures they remain effective even as threats evolve. (Ye, 2004)

These models have been successfully applied in studies to detect intrusions and multi-stage attacks. For example, researchers have used Markov models to monitor transitions in network activities, flagging sequences that deviate significantly from the norm as potential cyberattacks (Ye, 2004). Their ability to focus on patterns rather than isolated events makes them an essential tool for identifying and responding to threats early, helping protect critical systems from severe disruptions.

Intrusion detect system

Intrusion Detection Systems (IDS) are vital tools for maintaining cybersecurity in maritime operations by monitoring networks in real-time to detect and respond to potential threats. These systems work by continuously analyzing data traffic and network behaviour to identify anomalies, such as unauthorized access attempts or unusual data flows. For example, tools like **Snort**, a popular IDS, can flag suspicious activity and immediately alert the crew, enabling a quick response to minimize potential damage (Ibokette, 2024).

Modern IDS solutions are becoming increasingly sophisticated, leveraging technologies like **machine learning** and **artificial intelligence (AI)** to enhance threat detection. These advancements allow IDS to identify evolving cyber threats more effectively while reducing false alarms, which is especially important in dynamic maritime environments where timely responses are critical (Liu, 2023). Additionally, IDS can be integrated with user-friendly interfaces that provide actionable guidance to ship crews, ensuring that even non-cybersecurity experts can take appropriate measures during an attack.

In summary, IDS plays a crucial role in real-time threat detection by analyzing network activity, providing early warnings, and enabling proactive threat mitigation. Its integration with advanced technologies and practical interfaces ensures that maritime operations remain secure against cyber threats while minimizing disruptions to critical systems. Let me know if you'd like further details or refinements.

Section 2.4 -Mechanisms of security

The maritime industry's increasing reliance on digital systems has revolutionised operations but simultaneously exposed vessels to significant cybersecurity risks. Effective mechanisms for maritime cybersecurity, such as **Vulnerability scanning**, **Network segmentation**, and **Encryption**, serve as critical defences against these threats. However, the effectiveness of these mechanisms often hinges on the capabilities of the crew to recognise and respond to cyber threats in real time. Integrating robust training programs with technical mechanisms is essential for building comprehensive cybersecurity resilience in maritime operations (BIMCO, 2024).

Vulnerability Scanning and Network Segmentation

Vulnerability scanning is a proactive and systematic process used to identify weaknesses within a vessel's digital systems. By continuously assessing vulnerabilities, operators can prioritise risks and implement corrective actions before attackers exploit them. For instance, vulnerability scanning might detect outdated software, misconfigured firewalls, or weak encryption protocols. Addressing these vulnerabilities ensures that critical systems remain secure against known cyber threats (BIMCO, 2024).

Network segmentation complements this approach by isolating critical systems, such as navigation or cargo management, from less secure components like crew internet access. This isolation minimises the risk of lateral movement during an attack, where an intruder could move from a compromised system to a more sensitive one. For example, segregating the ship's navigation system from its communication network can significantly reduce the impact of a GPS spoofing attack, ensuring that critical navigation data remains accurate and uncompromised (BIMCO, 2024).

Despite the technical sophistication of these mechanisms, their success depends on the crew's ability to interpret and act on the data generated. Vulnerability scans might raise critical issues, if crew members lack the training to recognise the severity or understand how to address them, these alerts may go unheeded. Similarly, network segmentation requires proper maintenance to ensure boundaries between systems remain intact. Untrained personnel might inadvertently introduce vulnerabilities by improperly configuring network access controls or failing to recognise anomalies.

Real-world examples demonstrate the critical importance of integrating these mechanisms with effective crew training. For instance, in a documented incident of a shipping company's breach, the failure to act on a vulnerability scan allowed the ransomware to compromise multiple systems, leading to operational delays and financial losses. Studies further emphasise that training programs that simulate cyber incidents, such as phishing attempts or network breaches, enhance situational awareness and improve decision-making under pressure (M. Canepa, 2021).

However, implementing these mechanisms faces challenges. Older vessels, for instance, may lack the necessary digital infrastructure to support comprehensive vulnerability scanning or segmentation, making retrofitting both costly and technically demanding. Additionally, varying levels of digital literacy among crew members further complicates the effective deployment of these tools. Addressing these gaps requires not only technological upgrades but also tailored training programs that empower crews to act as the first line of defence against cyber threats.

In summary, while vulnerability scanning and network segmentation form essential layers of defence in maritime cybersecurity, their effectiveness hinges on the capabilities of the crew. Training programs that integrate real-world scenarios and continuous skill development are vital to ensure these mechanisms achieve their full potential in safeguarding maritime operations.

Simulation drills are indispensable tools for preparing crews to handle real-world cyberattacks. These drills replicate ransomware attacks, system outages, phishing attempts, and navigation disruptions, providing crew members with a risk-free environment to practice their responses. For instance, the Cyber-MAR project developed hyper-realistic simulations that recreate complex maritime cyberattack scenarios. Participants in these drills gain hands-on experience in managing cyber threats, improving both their technical proficiency and decision-making under pressure. These simulations not only teach participants how to respond but also expose vulnerabilities in existing procedures, enabling organizations to refine their cybersecurity strategies (M. Canepa, 1 March 2021).

Real-time monitoring complements simulation drills by providing crews with the tools to detect and respond to threats in real-time. Advanced monitoring systems, equipped with predictive analytics and machine learning algorithms, can identify anomalies in system behaviour, such as unexpected data transmissions or unauthorised access attempts. For example, a monitoring system may detect irregular activity in a vessel's communication network, triggering an alert that allows

the crew to isolate the affected system before the threat spreads. Predictive analytics further enhance these systems by anticipating potential risks based on historical data and emerging threat patterns (Nikolov, 2024).

However, for these systems to function effectively, crew members must possess the skills to interpret alerts and take appropriate action. Poorly trained crews may misinterpret critical warnings or fail to act swiftly, leaving systems exposed to exploitation. For instance, in one documented case, a ship's crew ignored repeated alerts from its monitoring system, resulting in a ransomware attack that disrupted operations for several days. Training programs that integrate real-time monitoring with simulation drills can address this issue by teaching crews how to respond to various alert scenarios effectively (Georgios Potamos, 2021).

Phishing attacks remain one of the most prevalent and effective cyber threats, exploiting human vulnerabilities to bypass even the most advanced technical defences. These attacks often succeed due to human error, such as failure to recognise suspicious emails or URLs. Studies highlight that up to 95% of successful cyberattacks stem from human factors, including susceptibility to phishing and poor situational awareness (Bernardo Breve, 2024). In the maritime sector, where cyber vulnerabilities can lead to disruptions in global supply chains, well-trained crews play a critical role in preventing phishing attempts from escalating into system-wide compromises. Research emphasises that training programs tailored to simulate phishing scenarios and teach recognition of fraudulent emails or URLs significantly enhance crew members' ability to identify and report such attempts (Trisolvena, 2024). For instance, targeted awareness programs that employ real-world phishing examples improve decision-making and reduce the likelihood of successful breaches, ultimately fortifying the first line of defence in cybersecurity. However, a critical gap persists in the maritime industry regarding standardised training programs for recognising and responding to phishing attacks, underscoring the need for continuous, scenario-based training to address this evolving threat.

Challenges in Implementation

Despite advancements in maritime cybersecurity, integrating effective training programs with technical mechanisms presents several challenges that require strategic solutions. One major obstacle is the **cost and resource constraints** faced by many maritime operators, particularly smaller companies. Developing and deploying simulation-based training programs, such as cyber drills and virtual environments, often requires significant financial investment, specialised software, and skilled personnel to design and deliver the training. These resource-intensive requirements can be prohibitive for smaller operators, leaving gaps in crew readiness and cybersecurity resilience.

Another pressing challenge is the **technology gap in older vessels**, which often lack the digital infrastructure necessary for implementing advanced cybersecurity mechanisms. Many older ships operate on legacy systems that are incompatible with modern cybersecurity solutions like real-time monitoring or automated alerts. Retrofitting these vessels with updated systems is not only technically demanding but also incurs substantial costs and operational downtime. This creates a disparity where older ships become increasingly vulnerable to cyberattacks, as they cannot support the sophisticated tools needed to counter modern threats (Nikolov, 2024).

Additionally, **varied levels of expertise among crews** complicate the design and delivery of standardised training programs. Crew members often come from diverse technical backgrounds, with some having minimal experience with digital systems. This disparity makes it difficult to create training materials that are both accessible to less-experienced crew members and challenging enough for those with advanced knowledge. Without targeted, skill-based training solutions, many crews may struggle to grasp the complex nature of cyber threats or the proper use of defensive mechanisms. Research underscores the importance of tailoring training programs to specific crew needs, focusing on practical, hands-on scenarios to build confidence and competence (Androjna, 2020).

Addressing these challenges requires a balanced approach. Investments in cost-effective solutions, such as virtual training environments that simulate cyber incidents without physical infrastructure, can provide scalable and affordable options for operators. Additionally, fostering partnerships between industry stakeholders, governments, and educational institutions can help reduce costs by pooling resources and standardising training frameworks. For older vessels, phased retrofitting

combined with portable cybersecurity tools, like standalone threat detection devices, can offer a practical way to enhance their defences without full system overhauls. Tailored training programs, supported by continuous learning opportunities, can ensure that all crew members regardless of their expertise are equipped to handle the evolving landscape of maritime cyber threats (Bernardo Breve, 2024).

Future Directions

Emerging technologies, such as artificial intelligence (AI) and machine learning (ML), present transformative opportunities for enhancing maritime cybersecurity. AI-driven predictive analytics can analyse vast datasets to identify patterns and anomalies, enabling crews to anticipate threats and take preventive action before they escalate. For instance, predictive systems can detect unusual data traffic or unauthorised access attempts in real time, reducing response times and minimising potential damage. Additionally, virtual training environments powered by AI can dynamically adapt scenarios based on crew performance. These environments offer personalised feedback and allow crews to practice responding to various cyber incidents, improving both their technical skills and decision-making abilities (Louise Praestin Jepsen, 2024).

Beyond technology, the integration of cybersecurity into existing maritime education frameworks offers significant potential for standardising training across the industry. The IMO's Standards of Training, Certification, and Watchkeeping (STCW) provide an established framework that could incorporate mandatory cybersecurity modules. By embedding cybersecurity into certification processes, all crew members regardless of their vessel type or employer could acquire a baseline level of competence. This standardisation would address current disparities in crew expertise and ensure a consistent approach to managing cyber threats (C.H. Chang, 2019) .

In summary, the future of maritime cybersecurity lies in a blend of cutting-edge technologies and standardised training frameworks. By leveraging AI, integrating cybersecurity into education, and addressing implementation challenges, the maritime industry can build a resilient defence against evolving cyber threats while ensuring crew readiness across all levels.

Section 2.4.1 - Adoption of Industry Standards and Frameworks

The maritime sector is essential for global trade. It increasingly depends on cutting-edge digital systems for vital functions like navigation, communication, cargo management, and engine control. Although these advancements enhance efficiency, they also heighten the cybersecurity threats, thus positioning the maritime industry as a prime target for cybercriminals. These attackers take advantage of weaknesses in digital systems to disrupt operations by stealing sensitive information or compromising safety. The repercussions of such attacks can spread throughout the entire supply chain, leading to economic and operational harm worldwide. To address these issues, the maritime sector has adopted several established cybersecurity frameworks, including the **NIST Cybersecurity Framework (CSF)**, the **International Maritime Organization (IMO) Guidelines**, and the **International Association of Classification Societies (IACS) Unified Requirements (UR)**. These frameworks provide structured and actionable guidance to enhance cybersecurity resilience, making them essential tools for addressing evolving threats (Garcia, 2020).

The **NIST Cybersecurity Framework (CSF)** is one of the most comprehensive guides for managing cybersecurity risks across industries. It organises actions into five critical steps: **Identify**, **Protect**, **Detect**, **Respond**, and **Recover**, creating a systematic approach to mitigating cyber threats. In the **Identify** step, maritime organisations map and catalogue critical assets such as navigation and communication systems, ensuring that even legacy systems on older ships are accounted for. This process helps identify vulnerabilities that require protection. The **Protect** step includes implementing defences like firewalls, encryption, and access controls to safeguard these systems from unauthorised access or attacks. The **Detect** step focuses on early warning systems that monitor for unusual activity, such as unauthorised logins or abnormal data traffic. This is particularly important for early detection, as it allows operators to address threats before they escalate. The **Respond** step provides protocols to contain and manage incidents, ensuring crew members can act quickly to limit damage. Finally, the **Recover** step focuses on restoring operations efficiently, minimising downtime, and maintaining operational continuity. By following this five-step approach, maritime organisations can proactively address threats while maintaining a strong recovery plan to handle potential disruptions (Rantos, 2024).

The **IMO Guidelines**, established by the International Maritime Organization, further emphasize the need to integrate cybersecurity into everyday maritime operations. Recognizing that cybersecurity is as critical as physical safety, the IMO requires ships to incorporate cyber risk management into their **Safety Management System (SMS)** through **Resolution MSC.428(98)**. This mandate, which is effective since January 2021, ensures that cybersecurity practices such as system backups, crew training, and risk assessments are treated as part of routine safety protocols. For example, the IMO encourages ship operators to conduct regular training sessions for crew members, enabling them to recognize phishing attempts, handle suspicious activity, and respond effectively during a cyber incident. By embedding cybersecurity into the SMS, the IMO ensures that ships are better equipped to handle cyber threats while fostering a culture of awareness and preparedness across the industry (IMO's MSC-FAL.1/Circ.3, n.d.).

The **IACS Unified Requirements (UR)** complement the IMO Guidelines by addressing the technical dimensions of cybersecurity. **UR E26** provides a structured framework for protecting both **Operational Technology (OT)** and **Information Technology (IT)** systems that are critical to ship operations. For example, it mandates the use of **Intrusion Detection Systems (IDS)** to monitor critical systems in real time and flag suspicious activity. This ensures early detection of potential cyberattacks, enabling crews to act promptly. Additionally, **UR E27** focuses on safeguarding externally connected systems such as navigation and communication tools, which are particularly vulnerable to cyber threats. Measures like encryption, firewalls, and multi-factor authentication are required to protect these systems from unauthorised access. For instance, navigation systems like ECDIS (Electronic Chart Display and Information System) are protected to prevent hackers from altering critical ship data, which could endanger the vessel's safety. These requirements ensure that cybersecurity is embedded into both the design and operation of ships, making them resilient against future threats (Iacs, 2023).

Together, these frameworks establish a **layered cybersecurity approach**. The **NIST CSF** offers a roadmap for systematically addressing threats, ensuring ships are proactive in identifying vulnerabilities and recovering quickly from incidents. The **IMO Guidelines** integrate cybersecurity into broader safety management, emphasizing the importance of crew training and routine risk assessments. The **IACS Unified Requirements** provide technical standards to ensure that OT and IT systems are secure, monitored, and resilient. By combining strategic, operational,

and technical measures, these frameworks help the maritime industry maintain a robust defence posture. For my research, these frameworks are especially significant. The **NIST CSF's Detect and Respond functions** align directly with my focus on **early threat detection**. Similarly, the IMO's emphasis on crew training supports my objective of preparing onboard personnel to recognise and mitigate cyber risks effectively. The IACS guidelines provide a foundation for understanding how to integrate technical solutions, such as IDS and secure network designs, into the broader framework of cybersecurity protocols.

By adopting these frameworks, the maritime industry not only achieves regulatory compliance but also builds a resilient cybersecurity environment capable of handling increasingly sophisticated cyber threats. These measures create a robust foundation for developing test protocols, training modules, and early detection systems which are the key components of my thesis. This integration of global standards and proactive measures ensures that ships remain safe, operational, and secure in the face of evolving challenges.

Section 2.4.2 - Combating Cyber Vulnerability in Shipping

The growing use of digital systems in the maritime industry for navigation, communication, and cargo operations has introduced various cybersecurity risks. These risks, which are embedded in a ship's Information Technology (IT) and Operational Technology (OT) systems, threaten the safety of operations, financial security, and the efficiency of global trade networks. These challenges mainly arise from vulnerabilities embedded within shipboard Information Technology (IT) and Operational Technology (OT) systems, which are critical to operational safety, financial stability, and global trade. Unlike conventional security risks, cyber vulnerabilities often remain concealed within a vessel's digital framework, making them harder to detect and manage effectively. This necessitates a proactive approach that goes beyond traditional methods, focusing on identifying weak points, predicting potential attack patterns, and enhancing response capabilities (Kessler, 2019; ENISA, 2019).

This section explores essential strategies for addressing cyber vulnerabilities in shipping. These include conducting simulation exercises and vulnerability assessments to expose and mitigate weaknesses, leveraging data analysis to anticipate predictable threat patterns, and learning from real-world case studies that demonstrate successful vulnerability management (NIST, 2020; Lloyd's Register, 2021). By integrating these practices, the maritime industry can establish a

cybersecurity framework that not only ensures compliance but also strengthens resilience against future threats.

A critical area of improvement lies in addressing the gaps in current cybersecurity practices. Existing frameworks, such as those provided by the International Maritime Organization (IMO) and the International Association of Classification Societies (IACS), establish foundational security standards but often fail to evaluate the real-world resilience of individual vessels (IMO, 2021; IACS, 2023). For instance, these frameworks typically emphasize compliance but may overlook how specific factors such as a ship's operational environment, its crew's preparedness, and the unique configurations of its technology affect its ability to withstand cyberattacks. To bridge this gap, the maritime sector needs structured test protocols that assess vessel-specific vulnerabilities, moving beyond generic compliance requirements to focus on practical, real-world scenarios (BIMCO, 2024; Deloitte Insights, 2020).

In summary, combating cyber vulnerabilities requires the maritime industry to adopt a multi-layered approach. By combining proactive measures such as simulation exercises, tailored vulnerability assessments, and predictive analytics, the sector can shift from reactive compliance to building a robust cybersecurity framework (ENISA, 2019; NIST, 2020). This framework will enhance operational security and ensure the industry is well-equipped to tackle both existing and emerging cyber threats.

Section 2.4.3 - Enhancing Cyber Resilience through Vulnerability Scanning and Testing

Vulnerability scanning is a critical cybersecurity practice that systematically examines computer systems, networks, and applications to identify weaknesses that could be exploited by unauthorised users. Using automated tools, it detects known issues such as outdated software, configuration errors, missing patches, or weak passwords, providing organisations with the opportunity to address these gaps proactively before malicious actors can exploit them (NIST, 2020). The primary goal is to strengthen defences by identifying potential risks early, ensuring systems remain secure and operational. In the maritime industry, where both Information Technology (IT) and Operational Technology (OT) systems play a central role, vulnerability scanning is crucial. These complex networks are responsible for essential functions like navigation, communication, and cargo management, meaning any cyber vulnerability could disrupt operations, compromise safety, or result in significant financial losses. Given these high stakes, the maritime sector has

increasingly recognised cybersecurity as an urgent priority, with vulnerabilities posing risks that extend beyond individual ships to the entire supply chain (Kessler, 2019).

Regular vulnerability assessments not only support compliance with regulatory standards but also provide valuable insights into the effectiveness of existing cybersecurity measures. For example, such assessments can help shipping companies allocate resources effectively, update security policies, and prepare for evolving threats (ENISA, 2019). However, while scanning for known vulnerabilities is essential, it alone may not be sufficient. To comprehensively address cyber resilience, field research and vessel-specific testing are equally important. These tailored tests account for each vessel's unique configuration, operating environment, and crew readiness, offering a deeper understanding of specific risks. Simulated attack scenarios, for instance, can reveal overlooked vulnerabilities, enabling targeted improvements in both technical defences and crew response protocols.

By combining regular vulnerability scanning with vessel-specific resilience testing, the maritime industry can go beyond theoretical assessments to build proactive defence strategies. These practices ensure that ships are better equipped to handle emerging threats, reinforcing their cybersecurity posture while maintaining operational safety and reliability (BIMCO, 2024). This layered approach not only enhances cyber resilience but also supports the development of a robust, adaptive cybersecurity framework tailored to the evolving challenges of maritime operations.

Section 2.4.4 - Scope and Compliance Requirements: Strengthening Cybersecurity Practices with Training Integration

In the maritime industry, vulnerability scanning must address both Information Technology (IT) and Operational Technology (OT) systems, which sets it apart from standard office environments. IT systems include traditional infrastructure such as networks, workstations, and software used for business operations. OT systems, on the other hand, are responsible for physical control functions onboard ships, such as navigation, communication, and safety operations. These OT systems are critical to vessel operations, meaning any cybersecurity issue could lead to severe consequences, such as navigation errors, system malfunctions, or even full operational shutdowns, highlighting the vital need for comprehensive scanning of both systems (IMO.org, 2021).

As cyber threats grow increasingly sophisticated, regulatory bodies and insurers have made vulnerability scanning a core component of compliance and risk management protocols. Guidelines like the International Maritime Organisation's (IMO) cybersecurity standards now mandate regular vulnerability assessments as part of a ship's Safety Management System (SMS). These assessments ensure that vessels identify and mitigate security risks promptly. For maritime operators, compliance with these standards is more than a regulatory necessity, it is essential for maintaining operational integrity, meeting audit requirements, and securing insurance coverage. Documenting these cybersecurity measures not only enhances ship resilience but also assures stakeholders that vulnerabilities are being managed proactively (Bimco, 2024).

Moreover, compliance requirements offer an opportunity to integrate real-world crew training into vulnerability assessment practices. Regular vulnerability scans can act as triggers for simulated attack responses, providing a hands-on way for crews to learn how to identify and respond to cyber threats. For instance, if a scan uncovers a potential weak point in the navigation system, this insight can be used to create a training exercise that simulates an attack exploiting that vulnerability. These exercises not only help the crew become more adept at handling cybersecurity incidents but also ensure they can apply theoretical knowledge in practical, high-stakes scenarios (ENISA.europa.eu, 2019).

By combining regular vulnerability scanning with structured crew training, maritime operators can address one of the most pressing gaps in current practices, the lack of vessel-specific resilience assessments. Each ship operates with unique systems, configurations, and crew dynamics, which means a one-size-fits-all approach to cybersecurity is insufficient. Tailoring scanning and training to individual vessels ensures that defences are not just compliant but also practical and effective against real-world threats. This proactive approach strengthens both technical defences and human readiness, creating a comprehensive cybersecurity framework that meets evolving challenges while protecting critical maritime operations (Lloyd's, 2021).

Section2.4.5 - Challenges and Limitations of Vulnerability Scanning and Penetration Testing in Maritime Cybersecurity

While vulnerability scanning and penetration testing are essential for enhancing cybersecurity in maritime operations, they present notable challenges and limitations that need to be addressed to ensure maximum effectiveness. A primary concern is the expertise gap, especially regarding the specialised nature of Operational Technology (OT) systems aboard ships. Unlike conventional IT environments, OT systems are closely linked with the ship's physical functions, such as navigation and engine controls, and often utilise outdated legacy technologies that were not designed with cybersecurity in mind. This intricacy complicates the effective analysis of these systems. Moreover, there is a lack of cybersecurity professionals equipped with the skills to manage these unique systems, particularly in remote maritime settings. This shortage increases costs and restricts the regularity and thoroughness of vulnerability assessments on ships (Lloyd's, 2021).

Another limitation is the reliance on external expertise for detailed assessments. While open-source tools can provide basic insights, in-depth testing often requires external consultants who possess the expertise and resources to analyse complex shipboard systems. However, coordinating such external evaluations is logistically challenging, as ships frequently operate in remote areas or follow tight schedules. Furthermore, conducting vulnerability scans can sometimes disrupt onboard systems, as scanning processes may temporarily cause system downtime or reset configurations. This risk requires careful planning to ensure scanning does not interrupt critical operations (Lloyd's, 2021). An additional concern is the **security of the scanning process itself**, as malicious actors could exploit similar techniques to identify weaknesses in ship systems. To mitigate this risk, scanning results must be securely documented and shared only with authorised personnel. This ensures that sensitive information does not fall into the wrong hands and that vulnerabilities are addressed rather than exposed (ENISA.europa.eu, 2019).

Penetration testing (pen testing), which simulates cyberattacks to evaluate system defenses, faces similar challenges. For example, the three main types of Pen testing Black Box, Gray Box, and White Box each reveal different vulnerabilities but require varying levels of system knowledge and access. **Black Box testing**, where the tester has no prior knowledge of the system, mimics an external hacker's approach and is useful for evaluating perimeter defences. **Gray Box testing**, where the tester has partial access, highlights insider threats or risks from crew members with

limited permissions. **White Box testing**, which provides the tester with full system knowledge, uncovers vulnerabilities in internal configurations and permissions. However, pen testing on OT systems poses risks, as simulated attacks might inadvertently disrupt sensitive shipboard operations, such as navigation or propulsion controls (Bimco, 2024).

Despite these limitations, both vulnerability scanning and pen testing are essential components of maritime cybersecurity. However, these tools often fall short in evaluating a vessel's **real-world resilience under threat scenarios**. Structured field research and vessel-specific resilience testing are necessary to bridge this gap. For example, by simulating cyberattacks in controlled environments, operators can assess how well crew members and technological defences respond under realistic conditions. Such testing not only identifies technical vulnerabilities but also highlights human and procedural weaknesses, offering insights into areas for improvement (ENISA.europa.eu, 2019).To address these challenges, the maritime sector needs tailored approaches that balance the logistical complexities of vulnerability scanning and pen testing with their critical importance for cybersecurity. Integrating these assessments into proactive resilience strategies, such as **training crews through real-world simulations** ensures that both technical defences and human response capabilities are continuously improved. These steps are vital for creating a comprehensive cybersecurity framework that protects maritime operations against evolving threats.

Proactive Cyber Threat Management Through Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) systems are a critical element of modern cybersecurity, offering robust tools to monitor, detect, investigate, and respond to cyber threats on endpoint devices such as computers, servers, and other connected systems. Unlike traditional antivirus software, which primarily blocks known threats, EDR leverages behavioural analysis, machine learning, and pattern recognition to identify advanced and unknown threats in real-time. This capability makes EDR particularly relevant for the maritime industry, where isolated ships rely on interconnected systems to manage navigation, communication, and operational controls. (Bimco, 2024) EDR ensures that any unusual activities or anomalies are detected early, allowing for swift containment and response to minimise potential disruptions. For example, the **IMO** has recognised EDR as a proactive solution to support its guidelines on maritime cybersecurity by enabling real-time detection and response to potential incidents (IMO.org, 2021).The core functions of EDR

include continuous monitoring, threat detection, incident investigation, and automated containment of threats. Continuous monitoring allows for tracking endpoint activity in real time, identifying potential threats such as unauthorized access or malware attempting to compromise operational systems. Incident investigation tools in EDR help identify the root cause of an attack, mapping its progression and providing actionable insights for preventing recurrence (ENISA.europa.eu, 2019). Automated response features ensure immediate action to isolate compromised devices, block malicious files, or disconnect affected endpoints from the network, which is particularly valuable in maritime environments where crews may lack immediate access to cybersecurity expertise (Kessler, 2019).

Despite its advantages, implementing EDR in maritime settings faces challenges, such as the complexity of securing operational technology (OT) systems alongside traditional IT systems. OT systems, including navigation and propulsion controls, are sensitive to disruptions and require careful calibration of EDR responses to avoid unintended impacts. Additionally, limited connectivity at sea can hinder real-time data transmission to shore-based security teams, making autonomous response mechanisms critical (Iacs, 2023). These challenges underscore the need for tailored EDR solutions that align with the unique conditions and requirements of maritime operations. By incorporating EDR into the literature review, you can establish it as a foundational tool that complements early detection, a focus of your thesis. Its relevance to maritime cybersecurity, especially in identifying threats and enabling swift responses, makes it a valuable addition to your study (BIMCO, 2024).

Section 2.5 – Conclusion

The maritime industry relies heavily on advanced digital systems for navigation, communication, and operational efficiency. While these technologies enhance productivity, they also expose vessels to significant cybersecurity threats, including GPS spoofing, ransomware attacks, and unauthorized access to critical systems. These threats extend beyond individual ships, potentially disrupting global supply chains and trade. Incidents like the Maersk ransomware attack underscore the vulnerabilities within the industry, with financial losses exceeding $300 million and long-term operational impacts (Greenberg, 2018). Despite international regulations such as IMO's Resolution MSC.428(98) and structured frameworks like the NIST Cybersecurity Framework, significant gaps remain in cybersecurity preparedness. While compliance with these standards

ensures a baseline level of protection, it does not guarantee resilience against evolving and sophisticated cyberattacks (IMO.org, 2021).

A critical issue identified is the lack of structured, vessel-specific crew training programs. Legacy systems on older vessels exacerbate these vulnerabilities, as they are often incompatible with modern cybersecurity measures and rely heavily on manual oversight (Kessler, 2021). Furthermore, while technical frameworks provide valuable tools for assessing and mitigating risks, their effectiveness depends on the human element, trained crew members who can recognise and respond to threats in real time. For instance, frameworks like MaCRA (Maritime Cyber Risk Assessment) offer a systematic approach to evaluating risks based on vulnerabilities and exploitation potential, but these insights must be complemented by hands-on crew readiness (Jones, January 7,2019).

Emerging tools, such as Bayesian Networks and Markov Models, provide predictive capabilities for early threat detection and failure management. However, these technologies alone cannot ensure resilience without integration into comprehensive training programs. Effective crew training, coupled with practical measures such as regular penetration testing, simulation drills, and vulnerability scanning, is critical to building a robust defence. These activities ensure that both technical systems and human operators can respond effectively under real-world conditions (Martina Pivarníková, November 2020).

This literature review highlights the urgent need for an integrated approach that combines technical measures with structured training programs tailored to vessel-specific needs. By addressing gaps in current practices, this research proposes a structured protocol that incorporates predictive analytics, comprehensive audits, and regular training exercises. This framework aims to strengthen maritime cybersecurity by ensuring that technical defences are complemented by a well-prepared and capable crew, ultimately enhancing the industry's resilience against evolving threats.

Chapter 3 – Research Methodology

Section 3.1 – Choosing the Suitable Model

This chapter outlines the research design, data collection methods, and analytical approaches used to address the:

Main Research Question:

How can effective test protocols be designed to evaluate and enhance crew readiness for addressing cybersecurity threats in the maritime industry?

To answer this question, the research focuses on identifying key cybersecurity challenges, evaluating current practices, and designing actionable solutions based on expert insights. The study employs the **Design Cycle Framework**, combining a risk-based approach with layered defence strategies to systematically explore and address the research objectives. This methodology leverages semi-structured interviews with cybersecurity experts and thematic analysis to extract insights for developing training protocols and test designs tailored to maritime operations.

3.2 Choosing the Suitable Model

To design test protocols for enhancing crew readiness and cybersecurity resilience in the maritime industry, it is critical to adopt a model that aligns with the research objectives and the operational complexities of ships. This research utilises a **risk-based approach** and a **layered defence strategy**, which provide a clear and practical framework for addressing the following sub-research questions:

1. **What are the current challenges faced by maritime crews in identifying and responding to cybersecurity threats?**
2. **What training methods and drills are currently used to enhance cybersecurity awareness and preparedness among maritime crews?**
3. **How can threat simulations and vulnerability tests be adapted to improve crew readiness for addressing cybersecurity threats?**

3.2.1 Risk-Based Approach

The risk-based approach focuses on identifying, assessing, and prioritising cybersecurity threats based on their likelihood and impact. This is particularly relevant in maritime operations, where threats like ransomware attacks, GPS jamming, malware and phishing schemes pose significant risks to navigation, communication, and cargo systems. By understanding these threats, the first sub-research question, **what are the current challenges faced by maritime crews?** is addressed. This approach is aligned with international standards like the IMO's Guidelines on Maritime Cyber Risk Management (MSC-FAL.1/Circ.3, 2017), which emphasize risk assessment as a foundational step for effective cybersecurity management.

For instance:

- **Identifying Threats**: Interviews with experts aim to reveal the most common and critical threats encountered by crews.
- **Assessing Risks**: Experts provide insights into how these threats affect ship operations, guiding the prioritisation of training needs.

3.2.2 Layered Defence Strategy

The layered defence strategy, also known as defence in depth, builds on risk assessments by implementing multiple protective layers. These include:

1. **Technical Measures**: Firewalls, intrusion detection systems (IDS), and regular vulnerability scans.
2. **Human Factors**: Crew training, role-specific preparedness, and awareness campaigns.
3. **Contingency Planning**: Simulated drills and backup protocols for handling cyber incidents.

This strategy aligns with the second sub-research question, **what training methods and drills are currently used?** by examining how current practices incorporate both technical and human elements. For example, the inclusion of penetration tests and simulated attacks

ensures that crews are not only aware of threats but also capable of responding to them effectively.

3.2.3 Proactive Tools: Vulnerability Tests and Threat Simulations

Proactive tools such as vulnerability tests and threat simulations are integral to assessing and improving crew readiness. These tools directly address the third sub-research question, **How can threat simulations and vulnerability tests improve crew readiness?**

Vulnerability Testing: Regular penetration tests mimic real-world attacks to identify weaknesses in onboard systems (e.g., ECDIS, PLCs). These tests provide actionable insights for training crews to address specific vulnerabilities.

Threat Simulations: Simulated drills prepare crews for real-life scenarios, such as ransomware attacks, enhancing their ability to identify threats and respond effectively. These simulations directly address the research objective of designing crew-centric training protocols to mitigate cyber risks.

3.2.4 Summary

The chosen model, a combination of the risk-based approach and layered defence strategy, provides a structured framework for addressing the main research question and its sub-questions. It ensures that:

- **Threats are systematically identified and assessed.**
- **Current practices are evaluated and improved.**
- **Proactive measures are implemented through vulnerability tests and simulations.**

This model forms the foundation for designing effective test protocols and training modules that enhance crew readiness and resilience against cybersecurity threats.

3.3 Data Collection: Interview Questions

To answer the main research question, how can effective test protocols be designed to assess and improve crew preparedness concerning cybersecurity threats in the maritime environment industry? To this end, Semi-structured interviews took place with cybersecurity experts. The goal was to gain a clear understanding of the current challenges and practices. We also explored innovative methods to improve cybersecurity readiness for maritime crew members. The interview questions are structured into thematic categories, each designed to align with specific sub-research questions and the overarching research objectives.

3.3.1 Interview Questions and Thematic Grouping

Understanding the Cyber threat Landscape

This section identifies the nature and scope of cybersecurity threats in the maritime industry, establishing a foundation for targeted crew training.

1. **What does the maritime industry currently face as the most common and critical cyber threats?**

   This question helps to establish the context for crew training by defining the specific threats.

2. **How do cyber threats typically manifest on ships, and what early warning signs should crew members be trained to recognise?**

   This question addresses the need for training designs that enable early detection.

3. **Are there any specific vulnerabilities unique to onboard systems (e.g., ECDIS, PLCs, or bridge systems)?**

   This question links cybersecurity training to ship-specific vulnerabilities.

Designing Effective Training Programs

This category explores the elements of a comprehensive training program tailored to maritime operations.

4. **What should a comprehensive cybersecurity training program for maritime crew members include to enable early detection of threats?**
   This question addresses the core objective of designing an effective training program.

5. **How can vulnerability testing and cyber threat simulations be effectively integrated into crew training programs?**

   Provides actionable insights for training design and protocols.

6. **Do you think different crew roles, such as deck officers and engineers, require specialised cybersecurity training? Why or why not?**

   Highlights the importance of tailoring training protocols to specific roles onboard ships.

Tools, Techniques, and Methodologies

This section focuses on practical approaches to training delivery.

7. **What tools or methodologies would you recommend for training crew members in recognising and mitigating cyber threats?**

This question helps identify practical solutions for training delivery.

Practical Implementation Challenges

This category addresses barriers and solutions for implementing cybersecurity training in real-time situations.

8. **What are the biggest challenges in implementing cybersecurity training programs onboard ships?**

   It helps to anticipate and address barriers to adoption.

9. **How can training programs address the varying technical expertise of crew members, especially those with limited IT knowledge ?**

   Explores how to make training feasible for crew members with different levels of technical proficiency.

Contribution to Training Design

The final question is forward-looking and seeks expert input for module development.

10. **If you were to design a training module for early detection of cyber threats, what key elements would you include?**

Provides expert recommendations for the design and content of training protocols.

3.3.2 Justification for Interview Questions

The interview questions have been carefully designed to align with the research objectives and provide valuable insights for addressing the sub-research questions. They are structured to explore the core elements of the **Risk-Based Approach**, **Layered Defence Strategy**, and the use of **Proactive Tools** discussed in Section 3.2. These questions seek expert insights and practical advice to create effective training modules. The goal is to boost crew readiness against cybersecurity threats. The focus is mainly on Technical aspects, including system vulnerabilities and tools and on human elements , such as crew awareness and preparedness.

This approach ensures a thorough understanding of the challenges and potential solutions. It emphasizes not only identifying issues but also developing actionable strategies to enhance cybersecurity resilience in the maritime industry.

3.3.2 Summary

Organising and presenting the interview questions aligns the data collection process with the research objectives. The questions focus on key cybersecurity challenges, crew vulnerabilities, and training needs in the maritime industry. This structure ensures the responses provide relevant insights that support the study's goals. The analysis will use thematic analysis to identify patterns and key insights. These findings will help design practical test protocols and targeted training programs. Addressing identified gaps and challenges will improve the cybersecurity readiness of maritime crews, equipping them to respond to evolving threats. This approach ensures the research outcomes are actionable and meet real-world needs.

3.4 Data Analysis Approach

The interviews will undergo thematic analysis. This method identifies patterns and themes in the responses, clarifying the information from participants. The analysis will group similar ideas or recurring topics relevant to the research objectives. For instance, if several experts emphasize crew training as crucial for tackling cybersecurity threats, this will emerge as a significant theme.

This process organises insights and aligns them with the main research question and sub-questions. Thematic analysis effectively extracts meaningful findings, aiding in the design of training protocols and testing solutions tailored to the maritime industry's challenges.

3.5 Design Cycle Framework

The framework of the design cycle offers a structured method for developing and enhancing solutions through continuous testing and feedback. This framework is crucial for this research, ensuring that training protocols and test designs are practical and tailored to the maritime industry's specific needs.

The Design Cycle includes four main stages:

Analysis: Start by understanding the problem. Collect information through expert interviews to gain insights into common cyber threats, vulnerabilities, and challenges faced by maritime crews.

Design: Use the findings from the analysis to create initial test protocols and training programs. These should address the identified challenges and focus on preparing crew members to handle cybersecurity threats.

Implementation: Put the designed solutions into action, either in a simulated environment or through practical application. For instance, conduct simulated cyberattacks to assess how well the training prepares crew members for real-world scenarios.

Evaluation: Review the outcomes of the implementation to determine what worked and what needs improvement. Gather feedback from participants and make observations during testing to refine the solutions, enhancing their effectiveness and reliability. The iterative nature of the Design Cycle allows training protocols to evolve alongside emerging threats, adapting to technological advancements and changing operational needs in the maritime industry. Each cycle strengthens the solutions, ensuring they remain effective against real-world challenges.

3.6 Limitations of the Methodology

This research methodology aims to systematically meet the research objectives, but it has some limitations. The use of semi-structured interviews with a small group of experts poses a challenge. While these participants offer valuable insights, their views may not capture the full range of challenges and practices in the maritime industry. The tight research timeline may limit opportunities for broader data collection or follow-up interviews. The reliance on thematic analysis introduces subjectivity, as it depends on the researcher's interpretation of the data. The findings reflect the specific contexts of the interviewed experts, which may not apply to other ships or situations. Despite these limitations, the methodology lays a solid foundation for addressing the research questions and providing actionable insights to enhance crew readiness and cybersecurity resilience.

Chapter 4

Developing Test Protocols to Enhance Maritime Crew Cybersecurity Readiness

4.1 – Introduction

The maritime industry increasingly relies on advanced digital navigation, communication, and cargo management systems. While these technologies enhance efficiency and safety, they also attract cyber criminals. The risks include Ransomware attacks, Phishing schemes, GPS spoofing Malware infections. These threats can disrupt operations, lead to financial losses, and jeopardize crew and vessel safety (ENISA.europa.eu, 2019). A significant gap exists in practical training for maritime crews to address these threats effectively. This chapter aims to bridge that gap by developing test protocols for training maritime professionals in the early detection of cyber threats. Early detection is vital. It enables crews to take preventive measures before minor issues escalate into major crises. The protocols focus on real-world scenarios, ensuring crew members understand cyber risks and are ready to respond. Training will emphasise hands-on learning, including Recognising unusual system behaviours, identifying phishing attempts, and responding to spoofing attacks. This approach equips the crew to manage threats with confidence (Divine C. Chupkemi, 2024).

This chapter focuses on creating practical training programs for ships. These programs will be easy to implement and adaptable to the changing cyber threat landscape. The key elements include insights from industry experts, real-world examples of cyber incidents, and lessons learned from previous experiences. These components will help crews stay ahead of cybercriminals, reducing risks and ensuring operational safety (Martina Pivarníková, November 2020). The chapter emphasises the need for continuous learning in cybersecurity training. As technology evolves, training programs must remain flexible and relevant. The aim is to equip maritime crews with actionable skills, not just theoretical knowledge, for their daily tasks.

By focusing on awareness, preparedness, and proactive measures, this chapter contributes to building a stronger, more resilient maritime industry that can withstand the growing challenges of the digital age (Working, 2020).

4.2 Understanding the Current Cybersecurity Landscape

4.2.1 Overview of Maritime Cyber Threats

The maritime industry's reliance on interconnected digital systems for navigation, communication, and cargo management exposes it to a range of cyber threats. These threats have evolved alongside technological advancements, making ships and maritime operations increasingly vulnerable. Among the critical threats are phishing, spoofing, jamming, malware attacks, and hacking. This section examines these threats, their implications for maritime operations, and how they inform the development of effective crew training protocols.

Phishing: A Growing Concern

Phishing is one of the most prevalent and evolving cyber threats in the maritime industry. Cybercriminals impersonate trusted entities to deceive crew members into revealing sensitive information, such as passwords or system credentials. This technique exploits human error, often through fake emails or messages, enabling attackers to infiltrate shipboard systems or access critical data. The rapid digitalisation of the maritime sector has amplified this threat, as crews increasingly rely on electronic communications (Arachchilage, 2014).

The consequences of phishing can be severe, often serving as gateways for more advanced attacks like malware infections or ransomware. For example, successful phishing attempts can compromise navigation systems or financial transactions, causing operational delays and reputational damage. Addressing phishing requires both technological solutions, such as AI-based detection tools and email filters, and human-centered strategies such as targeted training. Regular phishing simulations have proven effective in enhancing crew awareness and promoting proactive responses (Trisolvena, 2024).

Spoofing and Jamming: Threats to Navigation and Communication

Spoofing and jamming pose unique challenges in maritime cybersecurity, particularly affecting navigation and communication systems. GPS spoofing misleads vessels about their actual location, while jamming disrupts critical satellite signals. These attacks can steer ships off course or impede

their ability to coordinate with port authorities, leading to safety risks and operational disruptions. For instance, GPS spoofing incidents in the Black Sea caused over 20 vessels to report incorrect positions, highlighting the gravity of such threats (Martina Pivarníková, November 2020).

Jamming, which involves deliberate interference with satellite signals, is often reported in high-risk regions like the Persian Gulf. Ships have inadvertently entered unauthorised waters due to disrupted GPS signals, creating potential security hazards. Advanced detection techniques, such as the Interacting Multiple Model Unscented Kalman Filter (IMM-UKF) integrated with IMU sensors, offer real-time insights into signal reliability and have proven effective in mitigating jamming attacks. Tools like Orolia's Threat Blocker provide additional protection by countering GPS jamming (Taheri, 2023).

Malware Attacks on Maritime Vessels

Malware remains a persistent threat to maritime operations, infiltrating systems through phishing emails, infected USB drives, or unsecured networks. Malware can disrupt navigation and propulsion systems, leading to delays and safety risks. Notably, vulnerabilities in Integrated Navigation Systems (INS) have made them a target for malware, highlighting the critical need for robust cybersecurity measures (Lund, 2018).

Mitigating malware risks involves implementing automated threat detection programs and intrusion detection systems tailored for maritime networks. These technologies can identify suspicious activities, isolate threats, and minimise damage. Additionally, adopting secure protocols for data transfer and providing crew training on safe digital practices are essential to reducing vulnerabilities (Jones, 2012) (https://www.nhlstenden.com, 2024).

Implications for Crew Training Across Cyber Threats

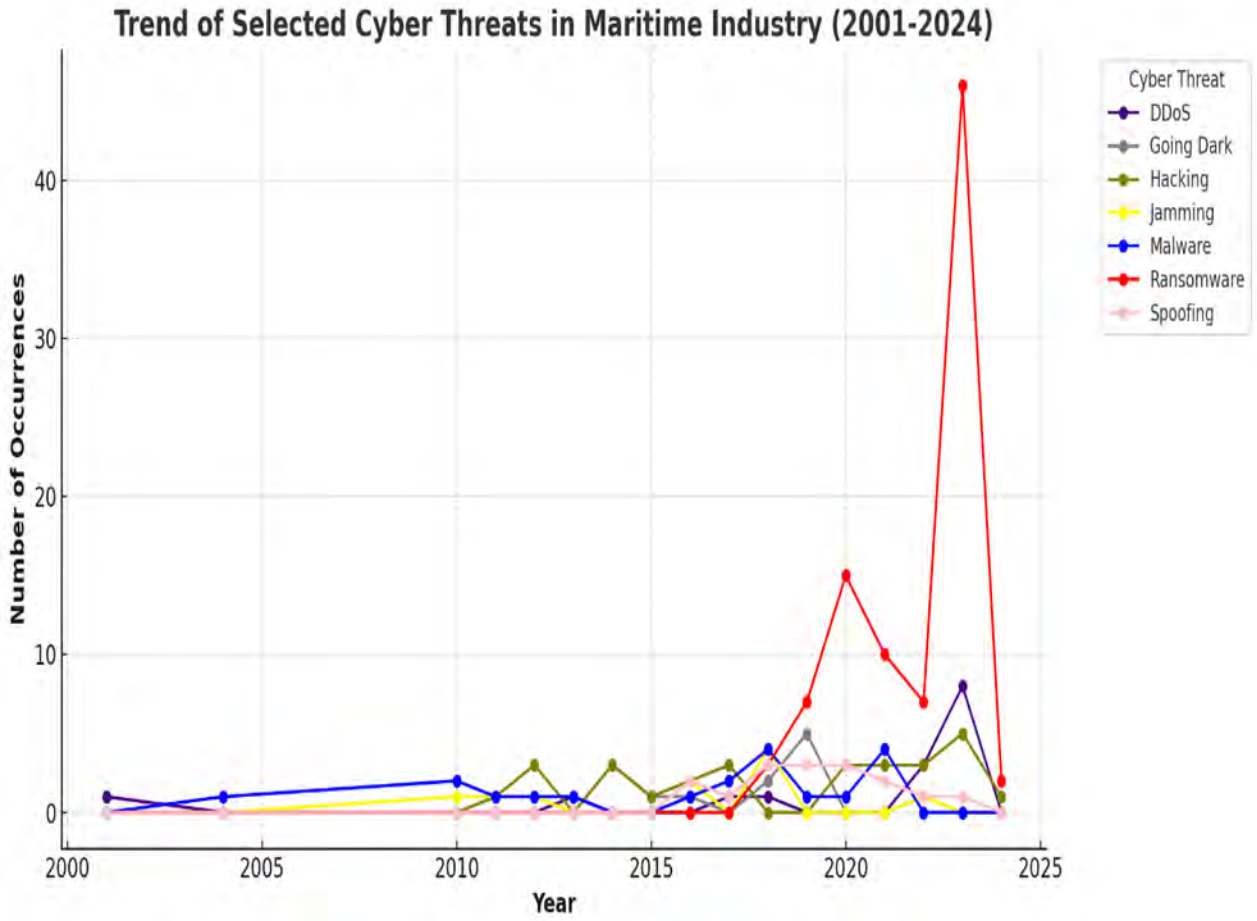
The variety and complexity of cyber threats, including phishing, spoofing, jamming, and malware, underscores the necessity of comprehensive crew training programs. Training must address foundational knowledge, such as understanding the characteristics of each threat, and practical skills, such as recognising phishing emails, detecting abnormal system behaviours, and responding to spoofing or jamming attempts.

Scenario-based simulations have proven particularly effective in preparing crews for real-world challenges. For example, phishing simulations can train crews to identify and report suspicious communications, while exercises mimicking spoofing or jamming attacks can develop their ability to implement alternative navigation strategies. Virtual reality and gamified training methods further enhance engagement and skill retention, providing immersive, hands-on experiences that replicate the complexities of modern cyber threats (Sabillon, 2021) (https://www.nhlstenden.com, 2024).Tailoring training to specific roles ensures targeted skill development. For instance, navigation officers can focus on GPS-related threats, while engineers address malware risks. By fostering a proactive and informed crew, these training programs not only reduce vulnerabilities but also ensure the safety and efficiency of maritime operations in an increasingly digitised world (Martina Pivarníková, November 2020).

4.2.2 MCAD Data Analysis: Trends and Critical Threats

The data collected from NHL Stenden University's Maritime Cybersecurity Awareness Database (MCAD) offers a detailed look at cyber threats in the maritime industry over the past 23 years, from 2001 to 2024. It tracks various types of attacks, including ransomware (when cybercriminals lock systems and demand payment), hacking (unauthorised access to systems), spoofing (faking identities or signals), and jamming (disrupting communication signals).

The graph below shows how often these types of attacks have happened and how much damage they've caused over time. We can see how these threats have grown, changed, or even become more sophisticated by looking at these trends. This information is crucial for designing effective training programs for maritime crews, as it highlights the kinds of cyber risks, they are most likely to face and how these risks could disrupt ship operations or safety (https://www.nhlstenden.com, 2024).



The graph highlights how different types of cyber threats have impacted the maritime industry from 2001 to 2024, showing trends in ransomware, hacking, malware, spoofing, and jamming. One of the most alarming patterns is the sharp increase in ransomware attacks after 2019, peaking in 2023. This reflects how attackers exploit the growing reliance on interconnected shipboard systems, targeting them for financial gain. Hacking, on the other hand, shows consistent activity over the years, emphasising its persistent risk to both ships and onshore operations, such as compromising navigation systems like GPS or ECDIS. Malware, though less frequent, poses a critical threat by infiltrating systems and disabling essential functions, often through phishing or infected devices (https://www.nhlstenden.com, 2024).

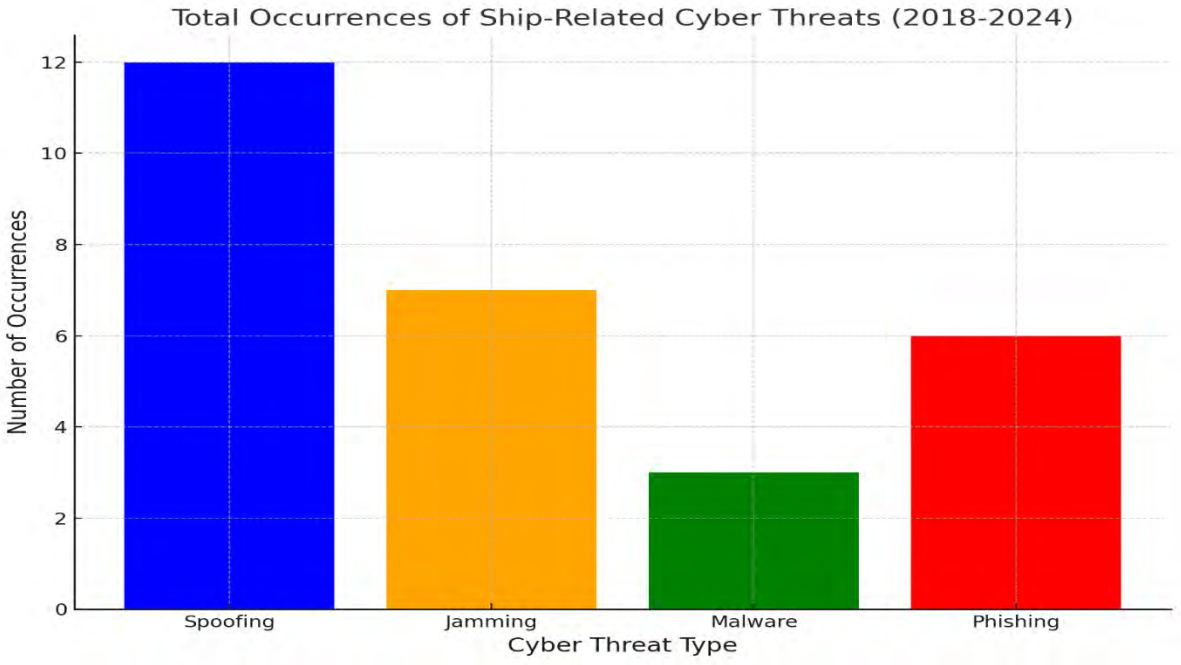
Other threats, such as spoofing and jamming, occur less often but have significant impacts. Spoofing can mislead ships about their location, redirecting them into dangerous waters or causing operational confusion. Similarly, jamming disrupts satellite communication and navigation

systems, which can severely compromise safety, especially in congested maritime regions. The data shows that while some threats are sporadic, their impact on operations is substantial (https://www.nhlstenden.com, 2024).

These trends emphasise the need for specialised training programs to prepare crew members for early detection of cyber threats. Training must focus on recognising signs of ransomware, hacking, and malware attacks, while also equipping crews to respond to more subtle threats like spoofing and jamming. By understanding these evolving risks, the maritime industry can implement effective test protocols and resilience-building exercises to safeguard its operations and systems. This analysis supports the importance of integrating threat simulations and real-world scenarios into crew training, a key focus of this thesis (https://www.nhlstenden.com, 2024).

Maritime Cyber Threats Targeting Ship Operations

The bar chart illustrates the total occurrences of four key ship-related cyber threats: spoofing, jamming, malware, and phishing. This visual representation highlights the prominence of each threat, with spoofing and jamming being the most frequent. These insights emphasize the critical need for targeted crew training programs to address these evolving threats, ensuring the safety and resilience of ship operations.



The bar chart provides an overview of the **total occurrences of ship-related cyber threats**, including **Spoofing, Jamming, Malware, and Phishing**, during the period 2018 to 2024. These threats represent critical vulnerabilities in maritime operations, each posing unique risks to the safety and efficiency of ships. Among these, **spoofing** emerges as the most frequent threat, where attackers manipulate GPS signals, causing ships to misinterpret their actual location. This can lead to dangerous situations such as route deviations, collisions, or even entering unauthorised waters. The high frequency of spoofing highlights the urgent need for crew training to detect abnormal navigation data and validate GPS signals using redundant systems or alternative technologies. (https://www.nhlstenden.com, 2024)

Jamming is another significant concern, disrupting satellite communications critical for navigation, communication, and operational control. Such incidents often occur in congested shipping lanes or regions with high geopolitical tension, where reliance on GPS systems is highest. Training crew members to recognise and respond to communication disruptions caused by jamming is essential to maintaining safe operations. Meanwhile, **Phishing**, is though not as frequent in ship-related contexts, exploits human error by deceiving crew members into revealing sensitive information or installing malicious software. This underscores the importance of crew awareness and education in identifying suspicious emails or communication attempts. (https://www.nhlstenden.com, 2024)Finally, **Malware** represents a persistent threat, infiltrating onboard IT systems through infected devices, unsecured networks, or phishing schemes. Malware attacks can corrupt files, disrupt operations, and compromise essential shipboard systems. Training programs must emphasise strict cybersecurity hygiene, such as avoiding unauthorised USB devices and recognising signs of malware infection. (https://www.nhlstenden.com, 2024)

These trends underscore the need for targeted crew training programs to address these threats effectively. By incorporating **scenario-based exercises**, crews can practice responding to spoofing and jamming incidents in real-time, enhancing their preparedness. Similarly, promoting IT security awareness and implementing regular cybersecurity drills can help to mitigate phishing and malware risks. The chart reinforces the importance of your thesis focus on designing effective test protocols and crew training for the early detection and mitigation of cyber threats onboard ships, ultimately ensuring safer and more resilient maritime operations. (https://www.nhlstenden.com, 2024)

4.2.3 Implications for Maritime Cybersecurity Training

The evolving landscape of maritime cyber threats, including spoofing, jamming, phishing, and malware attacks, underscores the critical need for effective and targeted crew training programs. These threats not only disrupt ship operations but also pose significant safety risks, making it essential for crew members to be adequately prepared to detect and mitigate these challenges. Training programs tailored to these threats are vital for safeguarding the maritime industry's digital and operational ecosystems (Martina Pivarníková, November 2020).

A key implication of the analyzed trends is the need to focus on foundational knowledge and practical skills. Crew members must understand the characteristics of each cyber threat. For instance, training on spoofing should include recognising suspicious navigation data and validating GPS signals using redundant or alternative systems like eLoran (Taheri, 2023). Jamming-focused training should teach crews to detect and respond to communication disruptions, particularly in high-risk or geopolitically sensitive areas. Similarly, phishing training should emphasise identifying suspicious emails or communication attempts that aim to extract sensitive information or introduce malware (Arachchilage, 2014).

Hands-on and scenario-based training is critical for effective preparation. Simulating real-world cyber incidents, such as spoofing that redirects vessels or jamming that disrupts navigation, allows crews to practice their responses in controlled environments. This approach enhances decision-making skills and builds confidence in handling unexpected situations. For phishing and malware, simulations can train crews to recognize attack patterns, respond appropriately, and maintain IT hygiene to prevent breaches (Sabillon, 2021).

Additionally, advanced technologies such as virtual reality (VR) and artificial intelligence (AI) can elevate training programs. VR can create immersive experiences that replicate complex scenarios, such as GPS spoofing or ransomware-induced system failures. AI-powered tools can analyze crew performance during training, identifying gaps and customizing learning modules to address specific weaknesses. These tools also simulate evolving threats, keeping training aligned with the latest cyber risk landscape (Ibokette, 2024).

Finally, continuous learning and regular updates to training programs are essential. Cyber threats are constantly changing, and static training programs are inadequate. Incorporating real-world data, such as the insights from the Maritime Cybersecurity Awareness Database (MCAD), into regular training updates ensures that crews stay informed about the latest threats and mitigation strategies (Mersinas, 2022).

By integrating these elements, maritime cybersecurity training programs can proactively address the industry's unique challenges, empowering crews to act as the first line of defense against cyber threats. This not only reduces operational vulnerabilities but also strengthens the overall resilience of maritime operations in an increasingly digital world.

4.3 Designing Test Protocols and Training Modules

Introduction

The maritime industry's growing reliance on interconnected systems for navigation, communication, and operations has significantly increased its exposure to cyber threats. As highlighted in Section 4.2, these threats include phishing, malware, GPS spoofing, and ransomware attacks, each posing unique risks to ship operations and safety (Trisolvena, 2024). While understanding these risks is critical, the next step involves translating this knowledge into actionable strategies. Subsection 4.3 focuses on the design of test protocols and training modules that equip maritime crews with the skills and awareness necessary to detect and respond to cyber threats effectively.

Building on Earlier Insights

The vulnerabilities discussed earlier such as legacy systems like ECDIS running outdated software and the increasing sophistication of phishing attacks that underscore the urgent need for comprehensive training protocols. These protocols must address not only the technical aspects of cybersecurity but also human factors, such as unintentional errors made by crew members. For instance, **Interviewee 1** emphasised, the real threat often comes from untrained crew who unintentionally connect infected devices to restricted networks, introducing risks like ransomware

or malware. Similarly, **Interviewee 2** highlighted that outdated OT systems are rarely patched, making them prime targets for remote attacks or physical breaches.

These insights highlight the dual focus needed in test protocols: securing the technological landscape and fostering a cybersecurity-conscious culture among crew members.

4.3.1 Framework for Test Protocols

To address the growing cybersecurity challenges in the maritime industry, it is essential to design effective test protocols that focus on identifying system vulnerabilities and improving the crew's ability to detect and respond to threats early. Expert insights highlight several key elements that are crucial for creating a strong framework to safeguard ship operations.

Understanding Vulnerabilities in Onboard Systems

Ships rely heavily on interconnected systems, such as the Electronic Chart Display and Information System (ECDIS) and Programmable Logic Controllers (PLCs), which often run on outdated software like Windows XP or Windows 7. These outdated systems no longer receive security updates, making them easy targets for cybercriminals. For instance, malware can exploit these vulnerabilities to disrupt navigation or control systems, leading to operational delays or even dangerous situations. **Interviewee 1** noted that Outdated OT systems and legacy software are particularly vulnerable to ransomware or malware attacks. **Interviewee 2** added that regular updates and system audits are crucial to protect these systems and reduce risks. Addressing these vulnerabilities is a foundational step in designing test protocols that strengthen a ship’s defences.

Defining Key Indicators of Cyber Threats

Cyberattacks on ships often start in subtle ways, making it challenging for crew members to notice them early. These attacks may begin with small, unexpected changes in the systems, such as unauthorised updates appearing without anyone triggering them, software behaving in a abrupt manner, or devices shutting down unexpectedly. While these issues might seem minor at first, they can signal the start of a serious cyber threat. Interviewee 1 explained that many crew members overlook such anomalies because they are not trained to recognise them as potential warning signs.

For example, an unplanned software update could be a hacker trying to install malicious programs. Similarly, irregular network activity or unusual error messages might indicate that an attacker is already inside the system.

Interviewee 2 emphasised that training crew members to identify these subtle signs is critical to stopping threats before they escalate. Teaching crews to notice and respond to unusual system behaviour is one of the most effective ways to prevent bigger problems, they explained. Test protocols should include exercises that help crew members practice identifying these early indicators, such as simulated network issues, fake unauthorised updates, or software behaving unpredictably. By making this training hands-on and straightforward, even crew members with little technical expertise can learn to recognise the signs of a cyberattack and act quickly. This proactive approach can prevent small issues from building up into major crises, ensuring the safety and operational continuity of the vessel.

4.3.2: Integration of Threat Simulations

The maritime industry faces increasingly complex cyber threats, including phishing attempts, GPS spoofing, and malware attacks. These evolving threats expose vulnerabilities in shipboard systems and demand proactive training approaches to mitigate risks. One such approach is the integration of threat simulations into crew training programs, which has proven to be an invaluable strategy for enhancing readiness and resilience. Simulations replicate real-world cyber incidents in controlled environments, allowing crew members to practice responses, improve critical thinking, and enhance situational awareness. These hands-on exercises bridge the gap between theoretical knowledge and practical application, making training both engaging and impactful (Kessler, 2020).

Threat detection simulations take various forms, such as virtual reality (VR)-based environments, gamified modules, and scenario-specific drills. These methods not only prepare crews for potential incidents but also bring confidence in their ability to detect and mitigate cyber threats early. The growing adoption of simulations within the maritime sector underscores their relevance in addressing unique vulnerabilities, including navigation and communication systems (Garcia, 2020). Interviewee 1 emphasised the importance of these methods, stating, “Simulated phishing

or GPS spoofing exercises help the crews to build the confidence to handle real-world scenarios effectively." Similarly, **Interviewee 2** highlighted, Hands-on drills bridge the gap between theoretical knowledge and operational skills, making cybersecurity training more practical and relevant.

Case Study: Virtual Training Environment for Maritime Cybersecurity

The Nikola Vaptsarov Naval Academy (NVNA) in Bulgaria has introduced a Virtual Training Environment (VTE) to improve the cybersecurity skills of maritime crews. This initiative responds to the growing reliance on interconnected digital systems in ships and ports, which increases vulnerability to cyber threats. The VTE offers hands-on cybersecurity training while addressing the cost and logistical challenges of traditional methods (Nikolov, 2024).

The VTE uses open-source software, making it affordable yet highly effective. Unlike expensive commercial tools, it replicates real-world cyberattacks, such as phishing, ransomware, and unauthorised data access. For instance, trainees can practice responding to a simulated phishing email or containing malware that infiltrates a ship's navigation system. Interviewee 1 pointed out that "affordable and accessible tools like open-source platforms are key to ensuring widespread adoption of advanced training methods."

One of the VTE's standout features is its role-based training, tailored to the responsibilities of different crew members. IT administrators focus on securing critical onboard systems, while general crew members learn to identify suspicious emails or unusual system behavior. **Interviewee 2** stressed the importance of this approach, stating, "Role-specific training ensures that every crew member is equipped to address the threats most relevant to their responsibilities, whether it's securing navigation systems or detecting malware in PLCs.

The system operates on a secure platform isolated from the academy's main IT network, allowing trainees to engage in simulations without risking real-world operations. Remote accessibility further enhances its flexibility and reach, making it suitable for diverse maritime personnel (Nikolov, 2024). A pilot course focused on Maritime Cyber Hygiene demonstrated the VTE's impact. Trainees learned to detect vulnerabilities, respond to cyberattacks, and strengthen overall readiness. By engaging in these hands-on exercises, crew members not only improved their

technical skills but also gained confidence in their ability to handle real-world challenges. Additionally, the VTE aligns with international cybersecurity regulations, including the International Ship and Port Facility Security (ISPS) Code and the International Safety Management (ISM) Code. These frameworks emphasise the importance of proactive risk management, operational resilience, and secure communication protocols. Through its simulations, the VTE ensures compliance with these global standards, further validating its role as a comprehensive training solution for maritime cybersecurity (Nikolov, 2024).

In summary, the NVNA's Virtual Training Environment is a game-changing tool that provides realistic, cost-effective, and highly relevant cybersecurity training for the maritime industry. It serves as a model for other institutions and shipping companies aiming to enhance their cybersecurity defenses while preparing their crews to handle the complex challenges of modern cyber threats.

Practical Implications for Test Protocols and Training

The Virtual Training Environment (VTE) developed by the Nikola Vaptsarov Naval Academy (NVNA) showcases how realistic threat simulations can significantly improve maritime cybersecurity readiness. By replicating real-world scenarios like phishing attacks or GPS spoofing in a safe and controlled setting, the VTE allows crews to practice responding to cyber incidents without putting actual operations at risk. Interviewee 1 emphasised the value of this approach, noting that *"hands-on simulations enable crews to test protocols effectively and build confidence in managing cyber threats."* Interviewee 2 added, *"These exercises bridge the gap between theoretical training and real-world application, preparing crews to handle complex incidents proactively."*

A standout feature of the VTE is its tailored training for different crew roles. For example, IT administrators focus on protecting navigation and communication systems, while general crew members learn to identify and report suspicious activities, such as unusual emails or unexpected system behavior. This role-specific training ensures that everyone on board is equipped to address threats relevant to their responsibilities. As Interviewee 1 explained, *"Customising training for different roles like engineers focusing on PLC vulnerabilities and deck officers learning to secure*

navigational systems makes the training practical and impactful." Interviewee 2 agreed, adding that "role-specific exercises ensure every crew member knows their part in protecting the ship, regardless of their technical expertise."

The VTE is particularly innovative because it uses open-source software, making it far more affordable than commercial training tools. Despite its lower cost, the system delivers high-quality training that is accessible to maritime institutions worldwide. **Interviewee 1** pointed out that "affordable tools like these are critical for ensuring that even smaller shipping companies can adopt advanced cybersecurity practices." This accessibility sets an important example of how cost-effective solutions can improve cybersecurity preparedness across the industry.

Another key aspect of the VTE is its emphasis on teamwork and communication during simulated crises. Trainees practice responding to challenging scenarios, such as ransomware attacks or GPS jamming, while coordinating with their team members. This collaboration strengthens their technical skills and enhances their ability to communicate effectively under pressure, a critical skill during real emergencies. **Interviewee 2** highlighted that team-based exercises teach crews to rely on one another and act quickly, which is essential in high-pressure situations. The training aligns perfectly with the Design Cycle Framework discussed in Chapter 3. This approach involves continually testing and refining protocols based on feedback from simulations. For instance, if a simulated ransomware attack reveals weaknesses in crew responses, the training can be adjusted to address those gaps. Over time, this iterative process ensures that both the crew and the protocols they follow remain effective against emerging threats. **Interviewee 1** emphasised that "regularly updating training based on new challenges ensures crews stay prepared as cyber threats evolve."

By focusing on realistic scenarios, teamwork, and continuous improvement, the VTE equips maritime personnel to stay ahead of evolving cyber risks. Both interviewees agreed that this approach not only helps crews react effectively to incidents but also builds a proactive mindset for safeguarding ship systems against threats like phishing, malware, and GPS spoofing. Ultimately, the VTE provides a powerful blueprint for integrating threat simulations into cybersecurity training, strengthening the industry's ability to adapt to an increasingly digital and interconnected world.

4.4. Simulated Drills for Crew Readiness

The maritime industry faces a growing spectrum of cyber threats, ranging from phishing and malware to GPS spoofing and system intrusions. As these risks become more sophisticated, traditional training methods often fall short in equipping crews to respond effectively in real-world scenarios. Simulated drills have emerged as a groundbreaking approach to bridge this gap, providing hands-on, immersive training that mirrors the complexities of modern cyber incidents. These drills create controlled environments where crew members can practice detecting, mitigating, and recovering from cyberattacks without endangering actual operations (Nikolov, 2024). **Interviewee 1** emphasised Simulations give crews the opportunity to experience high-pressure situations, helping them to develop both technical skills and confidence in their ability to respond effectively. Similarly, **Interviewee 2** noted, Drills tailored to realistic scenarios, like phishing or GPS spoofing, ensure that crews are not just trained theoretically but prepared to handle incidents practically. By integrating simulations into regular training routines, maritime organisations not only enhance technical proficiency but also foster teamwork, critical thinking, and situational awareness key attributes for navigating the digital challenges of today's maritime landscape. In this section, we explore a detailed case study showcasing the transformative impact of multidimensional simulations on maritime cybersecurity training, illustrating their potential to revolutionise crew preparedness (M. Baldauf, 2016).

The maritime industry faces ever-evolving cyber threats, such as phishing, GPS spoofing, and malware attacks, which demand robust preparedness from ship crews. To tackle these challenges effectively, simulated drills have emerged as a cornerstone of cybersecurity training. These exercises replicate real-world cyber incidents in controlled environments, allowing crew members to practice responses, enhance situational awareness, and build confidence in mitigating threats. By integrating realistic scenarios into regular training routines, maritime organisations can bridge the gap between theoretical knowledge and practical application, ultimately fostering operational resilience (M. Baldauf, 2016).

Benefits of Simulation-Based Training

Simulated drills offer several key advantages in enhancing crew readiness:

Realistic threat scenarios are designed to mimic the types of cyberattacks that crews might encounter in real-world situations, such as phishing attempts, GPS manipulation, or malware intrusions. For example, a phishing simulation might involve a fake email sent to the crew, tempting them to click on a malicious link or share sensitive information. Similarly, GPS manipulation scenarios could involve creating false navigation data, tricking the crew into believing the ship is in a different location, which could lead to dangerous route deviations (Nikolov, 2024). Malware simulations might show how a virus could disrupt vital systems like engine controls or navigation charts. These exercises allow crew members to experience the potential consequences of cyber threats in a controlled and safe environment. Interviewee 1 highlighted, *"Realistic simulations enable crews to understand how threats manifest in actual operations, making it easier for them to recognise and respond effectively when faced with similar challenges in real life."* They help participants to understand the complexities of these attacks, recognise the warning signs early, and practice effective responses, all without risking the actual safety of the ship or its operations. This hands-on exposure makes training more impactful and prepares crews to handle similar threats confidently in real situations (M. Baldauf, 2016).

Simulations are designed to help crew members to build essential skills for managing cyber threats. On the technical side, they teach participants how to identify unusual or suspicious behaviour in ship systems, such as unexpected changes in navigation data, sudden system slowdowns, or alerts indicating potential malware activity. These skills are crucial for spotting early warning signs of cyberattacks before they escalate into bigger problems. **Interviewee 2** explained that recognising unusual activities, such as unexpected software updates or unauthorised changes in a ship's systems, is critical because these are often the first signs that something is wrong. For example, a cyber attacker might push a fake software update to install malware or gain control of a system. Similarly, unauthorised changes like someone altering navigation settings without approval can indicate that a system has been compromised. If crew members are trained to notice and act on these small but significant anomalies early, they can stop the attack before it causes serious damage. This can prevent larger issues like the loss of critical systems, disruptions

to operations, or even safety risks to the vessel and crew. Essentially, spotting these warning signs early gives the crew a chance to take control and fix the issue before it turns into a major crisis. At the same time, simulations also focus on improving non-technical skills like critical thinking and decision-making. Crews are put in high-pressure scenarios that mirror the real-world challenges, such as responding to a phishing attack or recovering from a system breach. These exercises encourage participants to think quickly, assess the situation accurately, and make sound decisions even when under stress. Interviewee 1 pointed out that simulations play a big role in teaching crews how to stay calm and make quick, clear decisions during challenging situations. For example, in the middle of a cyberattack, such as malware affecting navigation systems, it can feel overwhelming with multiple problems happening at once. Simulations give the crew a chance to practice identifying what needs to be addressed first, like securing critical systems or isolating the issue and then acting in a step-by-step manner. This training helps them to develop the confidence to prioritise tasks effectively and avoid panic, even when under intense pressure. By practicing these scenarios, crews learn how to stay focused, think clearly, and work together to handle crises efficiently. By combining technical training with problem-solving and teamwork, simulations prepare crews to handle complex cyber incidents effectively and confidently in real-life maritime operations (Nikolov, 2024).Simulations also focus on building strong teamwork and collaboration skills among crew members. In a crisis scenario, such as a cyberattack disrupting navigation or communication systems, it's critical for everyone on the team to work together efficiently. These exercises emphasise the need for clear and open communication so that everyone understands what's happening and what their responsibilities are.

For example, during a simulated cyberattack, the navigation officer might focus on checking GPS data for accuracy, while the IT specialist investigates the source of the problem. Meanwhile, the captain oversees the situation, coordinating efforts and making key decisions. By practicing these role-specific tasks in a controlled environment, crew members learn how to rely on one another and respond quickly and effectively in emergencies. This teamwork ensures that everyone knows their role and can contribute to resolving the crisis, making the entire operation safer and more efficient.

Case Study: Multidimensional Simulation for Maritime Training

This case study demonstrates how simulation-based training can significantly improve maritime cybersecurity readiness. The training program was designed to prepare crews for a variety of cyber incidents and broader operational challenges through realistic, hands-on simulations. The program had two main goals.

First, it focused on Emergency Response Training, where participants were exposed to scenarios such as phishing attacks, unauthorised access to sensitive data, and malware infections. These exercises ensured that crew members were ready to identify and manage system intrusions effectively (M. Baldauf, 2016).

Secondly, it emphasises **Crisis Management**, simulating large-scale disruptions like compromised navigation systems or ransomware attacks that could cripple a ship's operations. These scenarios helped participants to develop critical skills such as teamwork, clear communication, and quick decision-making under pressure. By recreating real-world cyber challenges in a controlled environment, this training framework provided crews with the practical experience they needed to handle modern cybersecurity threats with confidence (M. Baldauf, 2016).

Key Features of the Training

The simulation exercises created **realistic scenarios** that closely mimicked the kinds of cyber threats modern ships face. For example, one scenario involved spoofed GPS signals, where attackers send false location data to a ship’s navigation system, causing it to believe it is in a completely different position. This could lead to dangerous situations, like the ship steering off the course into hazardous waters. Another scenario involved manipulated engine controls, where attackers gain unauthorised access to a ship's systems, altering its speed or direction without the crew’s knowledge. Additionally, the simulations included phishing emails, which are deceptive messages designed to trick crew members into revealing sensitive information or installing harmful software. These exercises gave participants firsthand experience in detecting and responding to these threats, helping them better understand the risks and develop practical strategies to safeguard ship operations (M. Baldauf, 2016).

The simulation exercises placed a strong emphasis on **teamwork and collaboration** among different departments onboard the ship. In real-life crises, effective coordination between crew members is critical to managing and resolving threats efficiently. For example, the bridge officers responsible for navigation needed to communicate seamlessly with the engineers managing the ship's propulsion systems. Similarly, IT personnel had to work closely with other departments to quickly identify and mitigate cyber threats. These exercises highlighted how every role contributes to overall security and how clear communication and coordinated efforts are essential during emergencies. By practicing these scenarios, crew members learned to trust and rely on each other's expertise, ensuring that they could respond as a cohesive team when faced with complex challenges (M. Baldauf, 2016).

Each simulation in the training program was designed with clear and practical **learning goals** to ensure that participants gained valuable skills relevant to real-world challenges. For example, one objective was to help crew members to identify vulnerabilities in shipboard systems, such as weaknesses in navigation software or communication networks, that could be exploited by cyber attackers. Another key goal was teaching them how to respond effectively to active cyber incidents, like stopping a phishing attempt or isolating malware to prevent it from spreading. Additionally, the simulations focused on recovery techniques, showing participants how to restore systems and operations after an attack to minimise downtime and damage. These targeted learning objectives ensured that the crew not only understood the risks but also felt confident in applying solutions, making them better prepared for potential cybersecurity threats at sea (M. Baldauf, 2016).

Results and lessons learned

The training had a noticeable positive impact on the participants. They expressed they were feeling much more confident in their ability to spot and deal with cyber threats, even in stressful and time-sensitive situations. For example, they learned how to recognise suspicious activities, like unusual emails or unexpected system behaviour, and respond quickly to stop potential attacks. **Interviewee 1 highlighted,** Practical, hands-on training is incredibly effective because it allows crew members to practice in situations that closely resemble real-life challenges they might face at sea. For example, they get to experience how to handle a simulated phishing attack or respond to unexpected system failures in a safe, controlled environment. This type of training shows them the

direct consequences of their actions, both good and bad so they can see what works and what doesn't. By practicing in realistic scenarios, they build the skills and confidence to respond quickly and effectively when something unexpected happens in real life. This preparation helps them feel more in control, reducing panic and hesitation when they face actual cyber threats at sea. The hands-on experience from the training gave them the skills and the assurance they needed to handle real-life challenges. This boost in confidence is especially important for maritime crews who often work in high-pressure environments where quick and accurate decisions can make a big difference in protecting their ship and its operations. The training sessions placed a strong emphasis on teamwork, helping crew members understand how crucial it is to work together during a cyber incident. Participants learned how to coordinate their actions, share information quickly, and rely on each other's strengths to tackle problems effectively. **Interviewee 2** explained that the best training programs focus on teamwork because handling a cyber incident isn't something that one person can do alone, it requires the entire crew to work together. Each crew member needs to clearly understand their specific responsibilities during a crisis, like who will check the navigation system, who will investigate the issue, and who will communicate updates to the rest of the team. When everyone knows their role, they can act quickly and avoid confusion. Training that emphasises teamwork teaches crew members how to coordinate their efforts, share information effectively, and rely on one another's strengths, especially in high-pressure situations. This kind of collaboration ensures that the team can respond to challenges efficiently and avoid making mistakes, even in stressful emergencies. For example, one team member might focus on identifying the source of a cyber threat, while another works on containing the issue, and a third communicates updates to the rest of the crew. This collaborative approach ensured that everyone understood their role in an emergency and could act confidently and efficiently. The exercises showed that strong teamwork is not just helpful but essential in handling complex cyber challenges in maritime operations (M. Baldauf, 2016).

Through the training, crew members developed a better understanding of how the various systems on a ship, such as navigation, communication, and engine controls, are all connected and rely on each other to function smoothly. They learned that a problem in one system, like GPS manipulation or a malware attack, could quickly impact other systems, leading to bigger issues. **Interviewee 1** observed, one of the most important takeaways for crews is understanding how interconnected

systems are. A problem in one part of the ship, like navigation, can affect everything else, from communication to propulsion. Recognising these links is crucial for preventing bigger problems. This heightened awareness helped them to realise how vulnerable these interconnected systems can be to cyber threats. By recognising these connections, crew members were better prepared to identify potential risks early and take steps to protect not just individual systems but the entire ship's operations.

Practical Implications

The findings from this case study align closely with the objectives of my thesis, demonstrating how multidimensional simulations can prepare maritime crews for real-world challenges.

Incorporating simulation frameworks into my proposed test protocols can bridge the gap between theory and practice for maritime crews. While theoretical concepts help crew members to understand the basics of cybersecurity threats, hands on simulations bring these ideas to life. **Interviewee 1** highlighted that practical exercises are crucial because they help to make complex ideas much easier to understand. When crew members are dealing with technical challenges like phishing attacks or GPS spoofing, simply reading about these threats isn't enough. By practicing how to recognise and respond to these issues, crew members can see how these concepts work in real life. For example, instead of just learning about phishing, they might simulate spotting a fake email and deciding how to respond safely. Similarly, with GPS spoofing, they might practice identifying unusual navigation data and switching to backup systems. These hands-on exercises turn abstract ideas into skills they can confidently use when a real threat occurs. By practicing in realistic scenarios, such as dealing with a simulated phishing attack or managing a spoofed GPS signal, crew members gain a deeper understanding of how cyber threats unfold in real-world settings. These simulations allow them to apply what they've learned in a safe, controlled environment, helping them to build confidence and practical skills. This hands-on approach ensures that the training isn't just about learning concepts but also about being fully prepared to respond effectively to real-life challenges (M. Baldauf, 2016).

Standardising crew preparedness across the maritime industry is critical to ensuring that all ships and personnel adhere to the same level of cybersecurity awareness and skills. This approach helps to ensure that the crew is well-prepared to handle threats, no matter where they operate. By aligning training programs with international standards like the **International Safety Management (ISM) Code** and the **International Ship and Port Facility Security (ISPS) Code**, the maritime industry can maintain a consistent framework for cybersecurity measures. These standards emphasise the importance of safeguarding shipboard systems and operations through proactive risk management, secure communication, and effective response protocols.

For example, the ISM Code focuses on safety and environmental management, requiring procedures to handle potential hazards, including cyber risks. Similarly, the ISPS Code sets guidelines for protecting maritime facilities and ships from security threats, extending to digital systems in today's interconnected landscape. **Interviewee 1** pointed out that training programs should follow important international standards, like the ISM (International Safety Management) Code and the ISPS (International Ship and Port Facility Security) Code. These standards act as guidelines to ensure that all ships and crews, no matter where they operate, maintain a consistent and strong level of cybersecurity readiness. By aligning training with these codes, it ensures that crews are learning the same best practices for detecting and responding to cyber threats, whether they're working on a cargo ship in Asia or a passenger vessel in Europe. This consistency helps build a unified defense across the maritime industry, making sure no ship or port becomes a weak point for cyberattacks. Training crews to meet these standards ensures they understand how to detect and mitigate cyber threats like phishing, GPS spoofing, or malware attacks, fostering a unified defence strategy across the global maritime network. This not only enhances operational safety but also builds confidence among stakeholders, including port authorities and shipping companies, about the industry's resilience against evolving cyber threats (M. Baldauf, 2016).

Simulations can act as a hands-on and practical way to test and improve cybersecurity training programs. This framework involves a continuous process of designing, testing, evaluating, and refining solutions to ensure they are effective. By using simulations, maritime crews can practice handling real-world cyber threats in a controlled setting.

Each time a simulation is conducted, the outcomes, such as how well the crew responded to a phishing attack or mitigated a GPS jamming incident provide valuable feedback. This feedback can be used to adjust the training, identify gaps in knowledge, and introduce new scenarios to address emerging threats. Over time, this process ensures that the training becomes more targeted, effective, and aligned with the specific needs of the maritime industry. It also helps the crew on board ship to build confidence and develop quick decision-making skills, which are critical in managing real-life cyber incidents. By continuous testing and refining training through simulations, maritime organisations can stay one step ahead of cyber threats and maintain high standards of cybersecurity readiness (M. Baldauf, 2016).

4.4.2 Evaluation and Feedback Mechanisms

Introduction

Evaluation and feedback are vital for ensuring the success of any training program, especially in cybersecurity training for maritime crews. Without proper evaluation, it is difficult to determine whether the training objectives have been achieved and if the participants are adequately prepared to handle cyber threats. Feedback mechanisms enable trainers to identify gaps in learning and refine the training approach to meet real-world needs effectively. This process of continual improvement aligns seamlessly with the Design Cycle Framework discussed in Chapter 3, where iterative refinement plays a critical role in enhancing the relevance and effectiveness of training modules (Nikolov, 2024). By consistently evaluating and improving the training protocols, maritime operations can maintain a proactive stance against evolving cybersecurity threats.

Methods of Evaluation

Evaluating the effectiveness of cybersecurity training programs requires a multifaceted approach to capture both quantitative and qualitative outcomes. Pre and post-training assessments are one of the most effective methods to measure the improvement in knowledge and skills among trainees. For example, participants can complete quizzes or practical tests before and after the training to gauge how well they have absorbed the material (Louise Praestin Jepsen, 2024).

Performance metrics during simulations offer another layer of insight. These metrics could include the response time to detect and mitigate threats, the accuracy of actions taken during simulated

incidents, and the efficiency of teamwork. Observations made by instructors or supervisors during these drills also provide valuable information about how crew members perform under pressure and where they may need additional support or practice. These methods together ensure a well-rounded evaluation of both individual and team performance (Mersinas, 2022).

Feedback collection mechanisms

Collecting feedback from both trainees and trainers is essential to understanding the strengths and weaknesses of the training program. Post-training surveys are an efficient way to capture participants' experiences and identify areas where they faced challenges. These surveys can ask specific questions about the clarity of the training material, the relevance of the scenarios, and their confidence in applying the learned skills (C.H. Chang, 2019).

Debriefing sessions are equally important, providing a platform for trainees to reflect on their performance and discuss the challenges they encountered during the simulations. This collaborative feedback process often leads to valuable insights that might not surface through surveys alone (Louise Praestin Jepsen, 2024). Additionally, simulation tools, such as virtual environments or software logs, can provide objective data about participant actions, response times, and overall performance. This information helps trainers identify trends and pinpoint areas that need improvement (Divine C. Chupkemi, 2024).

Key metrics of assessment

The success of a training program can be measured using several key metrics. Crew readiness and confidence levels are among the most important indicators. Participants who feel better equipped to handle cyber incidents are more likely to respond effectively in real-life scenarios. Reduction in response times during simulated threats is another critical metric, as faster detection and mitigation of threats are essential to minimizing potential damage (C.H. Chang, 2019).

The ability of crew members to detect abnormal system behaviors during exercises serves as another significant measure of success. This skill indicates that participants are not only absorbing theoretical knowledge but also applying it effectively in practical situations. Tracking these metrics over time ensures that the training program continues to meet its objectives and evolves alongside emerging threats (Louise Praestin Jepsen, 2024).

Practical Implications

Evaluation and feedback mechanisms have far-reaching implications for the design and implementation of training protocols. Insights gathered from these processes directly inform the refinement of test protocols and training modules, ensuring they remain relevant and effective. By incorporating feedback into iterative improvements, trainers can address gaps in learning, update scenarios to reflect current threats, and adapt the material to the specific needs of different crew roles (Divine C. Chupkemi, 2024).

Continuous improvement through evaluation and feedback also ensures compliance with international standards like the ISM and ISPS codes, which emphasize the importance of preparedness and resilience in maritime operations (Nikolov, 2024). By fostering a culture of learning and adaptability, these mechanisms help maritime organisations stay ahead of cybersecurity challenges, ultimately safeguarding their operations, crew, and assets.

4.4.3 Customisation for Role-Specific Training

In the maritime industry, cybersecurity threats affect various shipboard systems differently, creating the need for tailored training programs. Generic, one-size-fits-all approaches fail to adequately address the unique challenges faced by specific crew roles such as navigation officers, engineers, and IT personnel. Customization of training modules ensures that the skills and knowledge imparted are relevant to the participants' responsibilities and the cyber threats they are most likely to encounter.

The Need for Customisation in Maritime Cybersecurity Training

The maritime industry operates with a wide range of complex systems that are essential for navigation, communication, and operational efficiency. However, these systems are increasingly vulnerable to cyberattacks, necessitating role-specific cybersecurity training to effectively prepare crew members for their unique challenges and responsibilities.

For example, **navigation officers** frequently interact with critical systems like the Electronic Chart Display and Information System (ECDIS) and the Global Navigation Satellite System (GNSS).

These systems, while vital for safe navigation, are susceptible to attacks such as GPS spoofing and jamming, which can mislead a vessel about its position. Research highlights that these systems were designed before cybersecurity became a primary concern, making them vulnerable due to a lack of encryption or robust authentication mechanisms (C.H. Chang, 2019).

Similarly, **engineers** are responsible for managing machinery systems that rely on Programmable Logic Controllers (PLCs). These systems are critical for ship propulsion and operational safety but are prime targets for malware and ransomware attacks. Malware can infiltrate through unsecured networks or compromised USB devices, causing significant disruptions to operations.

Meanwhile, **IT personnel** handle the ship's communication networks, which bridge onboard and onshore systems. They face threats like phishing attempts and unauthorised access, which could compromise sensitive data or disrupt the entire ship's operation. The interconnected nature of modern maritime systems demands heightened vigilance and specialised knowledge to secure these networks against cyber threats (Lund, 2018).

Role-Specific Training Objectives

Training for Navigation Officers in Cybersecurity

Navigation officers play a critical role in ensuring the safe operation of a ship, but the systems they rely on, such as GPS and the Electronic Chart Display and Information System (ECDIS), are highly vulnerable to cyberattacks like spoofing and jamming. **Spoofing** occurs when attackers manipulate GPS signals to provide false location data, potentially steering a vessel off course or into dangerous waters. **Jamming**, on the other hand, disrupts satellite signals entirely, leaving navigation systems unable to function properly. These types of attacks can have severe consequences, from collisions to grounding incidents, making it essential for navigation officers to be well-prepared to identify and respond to these threats (Androjna, 2020).

Training programs for navigation officers must focus on equipping them with the skills to detect and validate GPS signals using redundant systems like eLoran, a terrestrial navigation system that provides a reliable backup when GPS signals are compromised. Officers need to practice cross-

verifying location data with other tools, such as radar and visual navigation aids, to ensure the accuracy of the ship's position (Thompson, 2014).

In addition, real-world simulations that mimic GPS signal manipulation or jamming incidents are critical for enhancing situational awareness. These simulations allow officers to experience the pressure and complexity of managing such scenarios in a controlled environment. For instance, they can practice identifying warning signs, such as sudden discrepancies in speed or position data, and implement corrective measures like switching to manual navigation or activating backup systems. This hands-on approach not only improves their technical skills but also builds confidence in their ability to make quick and informed decisions during emergencies (Louise Praestin Jepsen, 2024).

Ultimately, by focusing on these practical and scenario-based training methods, navigation officers can develop a deeper understanding of the vulnerabilities in their systems and the proactive steps needed to maintain operational safety in the face of evolving cyber threats (Lund, 2018).

Engineers: Training for Malware Detection and Prevention

Engineer's onboard ships are responsible for maintaining critical systems that rely heavily on Programmable Logic Controllers (PLCs). These systems, essential for propulsion, navigation, and cargo operations, are increasingly vulnerable to malware attacks due to their reliance on outdated or unpatched firmware and the absence of antivirus support in many PLCs (Prashant Hari Narayan Rajput, 2021). Training programs for engineers must prioritise secure handling of software updates, the implementation of antivirus measures, and robust malware detection techniques.

One innovative approach is the use of external malware detection mechanisms, such as Amaya, which employs machine learning and signature detection to identify malware threats without compromising the real-time performance of PLCs (Prashant Hari Narayan Rajput, 2021). Engineers should be trained to utilize such tools to secure PLCs against advanced threats like ransomware or malicious firmware updates.

In addition, it is essential for engineers to understand the specific vulnerabilities associated with PLC firmware. For instance, firmware updates distributed over insecure internet connections have

been exploited in cyberattacks targeting industrial control systems. By adopting methods such as digitally signed firmware and encryption, engineers can safeguard critical shipboard systems from unauthorised modifications (Chris W. Johnson, 25 August 2017).

Training programs should also emphasise the segregation of networks to minimise the risk of malware spreading across connected systems. For example, separating PLC networks from external internet connections reduces exposure to potential cyber threats, thus safeguarding essential shipboard operations (Zachry Basnight, 2013). Engineers must also learn how to interpret and act on anomaly detection logs generated by monitoring tools to address emerging threats effectively.

Furthermore, real-world training scenarios should simulate malware infections targeting PLCs. These simulations can help engineers practice the identification of unusual patterns, such as falsified sensor readings or unauthorized command executions, which are indicative of malware activity (Ryan Pickren, 2024). Incorporating these practical exercises into training modules enhances engineers' confidence and their ability to mitigate potential risks onboard.

In conclusion, comprehensive training programs tailored for engineers must integrate practical tools, advanced detection technologies, and real-world simulations to address the growing cybersecurity challenges associated with PLCs. This multifaceted approach not only equips engineers with the skills needed to protect critical shipboard systems but also aligns with international cybersecurity standards and best practices.

IT Personnel: Securing Shipboard Networks and Enhancing Cyber Resilience

Shipboard IT personnel this could be the Electro Technical Officer on board who can play a critical role in maintaining cybersecurity across the vessel's interconnected systems. Their training must be tailored to include strategies for identifying phishing attacks, monitoring unusual network activity, and implementing robust multi-layered defences to protect shipboard systems like the Electronic Chart Display and Information System (ECDIS) and the Global Navigation Satellite System (GNSS). Research has consistently emphasised the growing complexity of maritime cybersecurity due to the reliance on these systems and their vulnerabilities to external threats.The importance of computational vulnerability scanning in identifying weaknesses in systems like

ECDIS. IT personnel must be proficient in deploying such tools to detect vulnerabilities arising from third-party components or outdated software. The study revealed that even type-approved ECDIS setups, with properly maintained software, could remain vulnerable without robust scanning protocols and regular updates (Lund, 2018).Network segregation is one of the most critical defenses against malware and unauthorised access attempts targeting **ECDIS** and **GNSS** systems. Network segregation ensures that essential systems operate independently of non-critical networks, minimising the impact of a potential breach. IT personnel should be adept at implementing this strategy and using updated antivirus and scanning software to enhance security (Thompson, 2014).

Moreover, real-time network monitoring is crucial for detecting and responding to cyber threats effectively. Proposed methods for detecting sophisticated network threats, such as DNS (Domain Name System) rebinding attacks, which can bypass traditional firewalls and compromise local systems. IT personnel trained in these advanced detection techniques can protect shipboard IoT networks and data flow, ensuring operational continuity (Xudong He, 2023).

In conclusion, IT personnel must develop expertise in advanced threat detection, vulnerability scanning, and secure network design to protect critical shipboard systems. Through tailored training programs that address the unique vulnerabilities of maritime systems, IT personnel can significantly enhance the cybersecurity posture of modern vessels.

Chapter 5: Discussion, Implications, and Recommendations

5.1 Introduction

This chapter serves as a crucial bridge between the research findings presented in Chapter 4 and the broader implications for the maritime industry. Its primary purpose is to synthesise the insights gained from the study, analyse their significance, and propose actionable recommendations to address cybersecurity challenges. By reflecting on the findings and incorporating perspectives from industry experts, this chapter aims to connect theoretical knowledge with real-world applications, ensuring that the proposed solutions align with the practical needs of maritime operations.

A key focus of this chapter is the importance of learning and adaptability in cybersecurity, particularly in the dynamic context of the maritime industry. As cyber threats continue to evolve, training protocols, test designs, and operational strategies must remain flexible. This iterative approach aligns with the Design Cycle Framework discussed earlier, emphasising continuous refinement based on evaluation and feedback (Nikolov, 2024).

The integration of expert interview insights enriches the discussion by grounding the findings in practical, real-world experiences. These insights highlight the challenges and opportunities faced by maritime professionals in implementing cybersecurity measures, offering valuable perspectives that complement the case studies and research findings presented earlier. Specific attention will be given to critical cyber threats, vulnerabilities in onboard systems, and the role of training programs in improving crew readiness. By doing so, this chapter evaluates the relevance and effectiveness of the proposed training protocols and explores how they contribute to enhancing crew resilience against cyber threats (M. Baldauf, 2016).

5.2 Findings with Interview Data

5.2.1 Current and Critical Cyber Threats

The maritime industry faces a complex array of cyber threats that can severely disrupt operations and compromise safety. Insights from both interviewees shed light on the most pressing risks and emphasise the urgent need for both technical upgrades and crew training to tackle these challenges.

One of the most widespread threats is phishing, where attackers trick crew members into sharing sensitive information or downloading harmful software through deceptive emails. **Interviewee 1** explained that these attacks exploit a lack of cybersecurity awareness among crew members. For instance, phishing emails may appear as legitimate communication from a trusted source, leading crew members to unknowingly compromise ship systems. **Interviewee 2** added that phishing attacks are becoming more sophisticated, often targeting specific crew members involved in financial or navigational tasks. This targeted approach increases the risk of successful breaches.

Ransomware and malware attacks are also major concerns. These threats can infiltrate ship systems through infected devices, unsecured networks, or phishing schemes. **Interviewee 1** highlighted the role of outdated ship systems like ECDIS (Electronic Chart Display and Information System) and PLCs (Programmable Logic Controllers) in making vessels vulnerable. These systems often run on older operating systems that no longer receive regular security updates, creating easy entry points for attackers. **Interviewee 2** stressed that malware can operate undetected for extended periods, gradually compromising critical ship operations like navigation, propulsion, and communication. This silent nature of malware makes early detection and strong preventative measures vital.

External threats like GPS spoofing and GNSS jamming further complicate the cybersecurity landscape. **Interviewee 1** pointed out that GPS spoofing involves attackers sending false signals to mislead a ship's navigation system, potentially steering it off course or into hazardous waters. These incidents can have severe safety implications, especially in congested or geopolitically sensitive areas. **Interviewee 2** added that GNSS jamming disrupts satellite communications, which are critical for navigation and communication. Such disruptions can leave vessels vulnerable, particularly in regions with high shipping activity or political tensions.

Another significant yet often overlooked risk comes from insider threats. **Interviewee 1** emphasised that crew members, often unintentionally, can introduce malware or ransomware to a ship's systems by connecting infected personal devices to restricted networks. For example, a crew member may unknowingly use a USB drive that contains malware, compromising the entire ship's network. **Interviewee 2** noted that these insider risks highlight the importance of fostering a cybersecurity-conscious culture. Crew members must be made aware of how their actions, such as using unsecured devices or failing to report anomalies, can pose risks to the vessel's safety and operations.

While both interviewees agreed on the severity of these threats, their recommendations diverged slightly. **Interviewee 1** emphasised addressing the technical weaknesses of outdated systems through regular updates, maintenance, and implementing stronger network security measures. **Interviewee 2** , however, focuses on the human element, advocating for comprehensive training programs to build crew awareness and equip them with the knowledge to recognise and respond to cyber threats effectively.

In conclusion, the maritime industry's cybersecurity challenges arise from outdated technology and human factors. Phishing, malware, ransomware, GPS spoofing, GNSS jamming, and insider risks are all significant threats. The interviewee's insights underline the need for a dual approach that combines upgrading legacy systems with robust training programs to enhance crew readiness and resilience. This balanced strategy is essential for safeguarding maritime operations in the face of evolving cyber risks.

5.2.2 Manifestation of Cyber Threats and Early Warning Signs

Cyber threats on ships often begin subtly, making them difficult to detect in the early stages. Both interviewees highlighted that these threats typically manifest as small anomalies that can easily be overlooked but have the potential to escalate into major issues if not addressed promptly.

Manifestation of Cyber Threats

Interviewee 1 explained that cyberattacks often start with hackers trying to stay undetected. They gradually infiltrate systems, learning about vulnerabilities before initiating disruptive actions. For

example, malware might silently infect a system and trigger unauthorised updates or introduce errors that seem like routine technical glitches. Similarly, phishing attacks might deceive crew members into sharing sensitive information, which attackers could then use to gain access to critical systems like navigation or engine controls.

Interviewee 2 added that hackers often exploit outdated or unpatched software, which is common on many vessels. Systems like ECDIS or PLCs, frequently running older operating systems, are prime targets. Threats can also manifest as unexpected system reboots, unusual error messages, or operational delays. Hackers aim to make their actions appear as normal technical issues, making early detection by untrained crew members even more challenging.

Early Warning Signs

Both interviewees emphasised the importance of recognising specific early warning signs that could indicate a cyber threat:

- **Unauthorised System Updates**: Interviewee 1 pointed out that unplanned updates, especially those not manually triggered, could signal a potential cyberattack. These updates may mask malicious activities, such as data breaches or system manipulations.
- **Abnormal System Behaviour**: Interviewee 2 stressed that unexpected changes in system operations, like slower performance, unusual error codes, or unfamiliar pop-ups, are key red flags. These anomalies might indicate that hackers are compromising a system.
- **Unexpected Shutdowns**: Both interviewees noted that sudden or frequent shutdowns, without clear technical reasons, often precede significant attacks. These shutdowns might be used to mask data theft or to prepare for more severe disruptions like ransomware attacks.

Importance of Crew Training

The ability to detect and respond to these warning signs is critical for preventing small issues from turning into catastrophic events**. Interviewee 1** emphasised that training programs must teach crew members how to identify and report these signs immediately, even if they lack technical expertise. For instance, teaching crew members how to recognise a fake software update or abnormal network activity can significantly reduce response times and mitigate risks.

Interviewee 2 suggested using hands-on simulations to enhance learning, such as exercises where crew members practice identifying unusual system behaviors or reacting to phishing attempts. This practical approach ensures that even non-technical personnel are equipped to play an active role in cybersecurity.

Cyber threats manifest subtly but can escalate quickly if not detected early. Training programs that focus on identifying unauthorised updates, abnormal system behaviours, and unexpected shutdowns are essential to enhance maritime cybersecurity. By equipping crew members with the skills to spot these early indicators, maritime operations can proactively defend against evolving cyber threats.

5.2.3 Vulnerabilities of Onboard Systems

Onboard systems like ECDIS (Electronic Chart Display and Information System), PLCs (Programmable Logic Controllers), and bridge systems are essential for a ship's operations, but they also come with significant cybersecurity challenges. These systems, which are crucial for navigation, machinery control, and overall ship management, often have vulnerabilities that make them attractive targets for cyberattacks.

One of the key issues highlighted by both interviewees is the use of **outdated operating systems** on these systems. For example, ECDIS often runs on older versions of Windows, such as XP or 7, which no longer receive security updates. This lack of updates creates easy entry points for malware and other cyber threats. **Interviewee 1** noted that this is especially problematic because the maritime industry is slow to upgrade due to the operational downtime required for system overhauls, which shipping companies aim to avoid to save costs.

Another challenge is **unpatched firmware** on PLCs and other machinery controllers. These devices are often left with their default configurations, which attackers can exploit to gain unauthorised access. **Interviewee 2** pointed out that many PLCs lack advanced cybersecurity features, such as built-in defences against unauthorised access or intrusion, making them particularly vulnerable.

Additionally, the **lack of encryption** on communication systems, especially for ECDIS and bridge systems, leaves sensitive data exposed. For instance, unencrypted navigation data can be intercepted or manipulated, enabling GPS spoofing attacks that mislead the crew about the ship's location. **Interviewee 2** stressed that encryption is a simple but often overlooked solution that can significantly reduce the risk of data tampering.

Both interviewees agreed that addressing these vulnerabilities requires proactive measures. **Interviewee 1** emphasised the importance of **regular updates** for operating systems and firmware to patch known vulnerabilities. This process needs to be prioritised despite the challenges of downtime, as outdated systems pose too great a risk to ignore.

Interviewee 2 suggested the implementation of **standardised cybersecurity protocols** across the maritime industry. These protocols would include mandatory software updates, encryption of communication systems, and periodic security audits. Standardisation would help to ensure that all vessels, regardless of size or type, adhere to a consistent level of cybersecurity preparedness.

In summary, onboard systems are critical for a ship’s operations but remain highly vulnerable due to outdated software, unpatched firmware, and the absence of encryption. Addressing these issues through regular updates and standardized cybersecurity protocols can go a long way in mitigating these risks and ensuring safer maritime operations.

5.2.4 Cybersecurity Training for Crew Members

Training maritime crew members in cybersecurity is vital for safeguarding ships from a wide range of cyber threats. A well-structured training program provides both foundational knowledge and practical skills, ensuring that crew members are prepared to identify and respond to threats effectively. One of the most critical components of such training is teaching crew members how to recognise phishing attempts, which are often disguised as legitimate communications. Phishing emails may trick individuals into sharing sensitive information or clicking harmful links, leading to system breaches. Training should include examples of common phishing tactics and equip crew members with strategies to verify the authenticity of messages and identify suspicious patterns (M. Baldauf, 2016).

Another essential focus is fostering strong cyber hygiene practices, which involve adopting safe behaviours when using onboard systems. This includes avoiding unauthorised USB devices, creating strong and unique passwords, and being cautious when connecting personal devices to the ship's network. Good cyber hygiene reduces the risks of introducing malware or other threats to critical shipboard systems. Emphasising the importance of regular maintenance, such as updating software and patching vulnerabilities, further reinforces the need for proactive measures to keep systems secure (Nikolov, 2024).

Understanding the vulnerabilities of shipboard systems is another key component of effective training. Many systems, such as ECDIS and PLCs, often operate on outdated or unpatched software, making them attractive targets for attackers. Training programs should educate crew members about these risks and the importance of maintaining system updates to minimise vulnerabilities. Practical drills are important for bridging the gap between theoretical knowledge and real-world application. For instance, phishing simulations expose crew members to fake phishing scenarios, allowing them to practice identifying and reporting suspicious emails. Similarly, simulated cyberattacks, such as GPS spoofing or malware infiltration, provide a controlled environment for crews to develop problem-solving skills and build confidence in handling crises (M. Baldauf, 2016).

Case studies of real-world incidents can further enhance training by illustrating the consequences of cyber threats and the importance of taking precautions. For example, examining ransomware attacks that have targeted shipping companies underscores the relevance of preparedness and the need for vigilant practices. Such examples not only educate crew members about potential risks but also motivate them to apply their training diligently (Nikolov, 2024).

By combining theoretical lessons with hands-on exercises, cybersecurity training programs can bring in confidence in crew members. When they understand how their actions can prevent or mitigate cyber incidents, they become more proactive and capable during emergencies. This training approach also fosters teamwork and coordination, as crew members learn to collaborate effectively under pressure. Ultimately, well-rounded training programs that address phishing, cyber hygiene, system vulnerabilities, and practical drills ensure that maritime crews are equipped to safeguard ship operations against evolving cyber threats (M. Baldauf, 2016) (Nikolov, 2024).

5.2.5 Integrating Vulnerability Testing and Simulations

Simulation-based training plays a pivotal role in equipping maritime crews to respond effectively to cybersecurity threats. By incorporating realistic and role-specific scenarios, simulations provide crew members with hands-on experience in tackling incidents such as phishing, GPS spoofing, and malware attacks. These exercises mirror real-world challenges, offering a safe environment for practice while ensuring operational safety is not compromised (Nikolov, 2024).

For engineers, simulations may focus on identifying vulnerabilities in PLCs or responding to unauthorised system changes. Deck officers could practice recognising GPS manipulation and assessing its impact on navigation. IT personnel might engage in exercises that address network breaches or malware containment. These tailored approaches ensure that every crew member understands their specific responsibilities in mitigating cyber threats (M. Canepa, 2021).

Interviewee 1 highlighted that simulations provide an invaluable opportunity to test and refine existing protocols, revealing vulnerabilities in shipboard systems that may not be evident during routine operations. They emphasised the importance of introducing scenarios that simulate GPS spoofing, phishing attempts, and unauthorised system changes, as these represent the most pressing cyber threats faced by maritime crews. Similarly, **Interviewee 2** stressed the need for role-specific exercises, noting, Engineers and deck officers face vastly different challenges, tailored training ensures that both groups are equally prepared. For example, engineers could focus on identifying vulnerabilities in PLCs or responding to unplanned system behavior, while deck officers might practice detecting and mitigating navigational tampering, such as GPS manipulation or AIS spoofing.

The iterative nature of simulation-based training aligns with the Design Cycle Framework discussed earlier. Metrics such as crew response times, communication efficiency, and accuracy in detecting abnormalities are used to refine protocols continuously. This approach ensures training remains adaptive to emerging threats (M. Baldauf, 2016).

The integration of simulations into training not only enhances technical preparedness but also fosters teamwork and collaboration. **Interviewee 2** observed that such exercises encourage open communication and mutual reliance, crucial for effective crisis management. By simulating high-

pressure scenarios, crews can practice their roles and refine their responses, building confidence and competence to handle real-world challenges.

In summary, simulation-based training, coupled with vulnerability testing, is crucial for modern maritime cybersecurity preparedness. By tailoring exercises to crew roles, addressing operational challenges, and incorporating continuous feedback, these programs ensure crews are equipped to mitigate risks and safeguard shipboard operations effectively (Louise Praestin Jepsen, 2024).

5.2.6 Role-Specific Training Requirements

In the maritime industry, different crew roles interact with specific systems and face unique cybersecurity challenges. This makes it essential to tailor training programs to the responsibilities and vulnerabilities of each role. A one-size-fits-all training approach may leave crew members ill-equipped to handle the threats they are most likely to encounter.

Engineers are responsible for maintaining critical systems like Programmable Logic Controllers (PLCs) and other machinery, which are frequently targeted by malware and ransomware. These systems often lack advanced cybersecurity defenses and are prone to vulnerabilities due to outdated firmware or limited patching. Engineers need training that focuses on identifying and addressing these technical risks, such as recognizing signs of malware activity, securing firmware updates, and ensuring network segregation to limit the spread of cyber threats (Prashant Hari Narayan Rajput, 2021).**Deck officers**, on the other hand, work closely with navigation systems like the Electronic Chart Display and Information System (ECDIS) and the Global Navigation Satellite System (GNSS). These systems are vulnerable to GPS spoofing, jamming, and tampering. Training for deck officers should emphasise detecting suspicious changes in navigation data, validating GPS coordinates using alternative methods, and responding effectively to potential spoofing attacks. For example, a deck officer might be trained to cross-check GPS data with radar or visual observations to ensure the ship remains on course (Chris W. Johnson, 25 August 2017).

Both interviewees agreed on the importance of tailoring cybersecurity training to these specific roles. **Interviewee 1** pointed out that engineers need to focus on technical vulnerabilities, like securing PLCs against malware, while deck officers should prioritise safeguarding navigation systems. **Interviewee 2** added that role-specific training ensures that crew members are better

equipped to handle the unique risks tied to their responsibilities, creating a more comprehensive defense against cyber threats. Role-specific training programs not only enhance individual expertise but also improve overall ship security. When each crew member understands their role in preventing and mitigating cyber threats, the entire team can work together more effectively during a crisis. By focusing on the specific needs of engineers, deck officers, and other specialized roles, maritime organizations can build a stronger, more resilient cybersecurity culture onboard their vessels.

5.2.7 Tools and Methodologies for Training

Effective training programs for maritime crews must go beyond theoretical knowledge to provide hands-on, interactive learning experiences that prepare participants to tackle real-world cyber threats. One of the most effective approaches is the use of virtual labs, which replicate shipboard systems like ECDIS or PLCs. These labs allow crew members to practice identifying unauthorised access, detecting abnormal system behaviour, or isolating malware in a safe, controlled digital environment. For instance, a virtual lab might simulate a GPS spoofing attack, enabling navigation officers to practice verifying location data using alternative tools (Nikolov, 2024).

Another powerful method is gamified training modules, which make learning engaging and enjoyable. These modules use points, leaderboards, and real-time feedback to motivate participants while reinforcing critical cybersecurity skills. For example, crew members can earn points for spotting phishing attempts in a simulated email inbox or responding correctly to a jamming event. Such scenarios make training memorable and encourage active participation (M. Baldauf, 2016).Mock phishing campaigns are also a highly effective tool. These exercises involve sending realistic but fake phishing emails to crew members to test their ability to recognise and avoid social engineering attacks. After the exercise, feedback sessions help participants to understand what they missed and how to improve, significantly reducing the likelihood of falling victim to actual phishing attempts in the future (Arachchilage, 2014).

Interactive workshops and role-specific drills further enhance training by tailoring exercises to the unique responsibilities of different crew members. For example, deck officers may focus on detecting GPS or AIS manipulation and responding to compromised navigation systems, while

engineers could practice isolating malware or managing anomalies in PLCs. IT personnel might work on identifying unusual network activity or unauthorised access attempts. These targeted exercises ensure that each crew member is well-prepared to handle challenges specific to their role (Garcia, 2020).

Innovative technologies like augmented reality (AR) and virtual reality (VR) are also proving to be valuable in training. By immersing participants in lifelike scenarios, these tools allow crews to practice handling high-pressure situations, such as malware-induced navigation failures or spoofed GPS signals, in a safe and controlled environment. This immersive approach not only enhances technical skills but also builds confidence in dealing with complex incidents (Sabillon, 2021).

Finally, effective training programs include continuous feedback and assessment tools to evaluate crew performance during exercises. Metrics like response time, accuracy in detecting threats, and decision-making under stress provide actionable insights for trainers. These insights can be used to refine future training sessions, ensuring that crews are always improving and staying prepared for evolving cyber threats (Nikolov, 2024).By integrating these tools and methodologies, maritime organisations can create engaging and practical training programs that build crew confidence, improve technical proficiency, and foster a strong cybersecurity culture across the industry.

5.2.8 Challenges in Implementing Training Programs

Implementing effective cybersecurity training programs in the maritime industry is not without its challenges. One of the most pressing issues highlighted by **Interviewee 1** is the varying levels of IT knowledge among crew members. Maritime crews come from diverse backgrounds, and while some may have a basic understanding of digital systems, others may struggle with even fundamental cybersecurity concepts. This disparity makes it difficult to design inclusive training programs that cater to all levels of expertise. Additionally, limited time availability is a significant hurdle. Ships operate on tight schedules, and downtime for training can disrupt operations and add costs for shipping companies (Nikolov, 2024). As suggested by **Interviewee 1**, flexible and modular training programs are a practical solution, allowing crews to learn in short sessions during off-duty hours without impacting their work schedules.

Interviewee 2 pointed out another critical challenge: the lack of a cybersecurity culture in the maritime industry. Traditionally, crew members have focused on physical safety and operational tasks, often viewing cybersecurity as secondary or unrelated to their daily responsibilities. This mindset can lead to negligence in following cyber hygiene practices or underestimating the importance of protecting digital systems. To address this, training programs must emphasise the direct connection between cybersecurity and operational safety. How a successful GPS spoofing attack could lead to navigation errors or how malware could disrupt critical ship functions can help crew members to understand the real-world implications of cyber threats. As **Interviewee 2** noted, fostering a culture where cybersecurity is seen as integral to safety and efficiency is key to driving engagement and participation.

Another challenge is the **time constraints of maritime operations**, as crew members often work long hours and have limited opportunities to attend training. Addressing this requires innovative and accessible approaches, such as multilingual materials, role-specific training, and interactive online modules. These methods ensure that crew members, regardless of their technical background or language proficiency, can benefit from training without feeling overwhelmed.

Another effective strategy is incorporating **role-based training**, which tailors the content to the specific responsibilities of each crew member. Engineers can focus on securing onboard systems like PLCs, while navigation officers learn to counter GPS spoofing. This targeted approach not only makes training more relevant but also ensures that every crew member contributes effectively to the ship's overall cybersecurity defense (Nikolov, 2024).

Finally, management support and clear communication are essential to fostering a cybersecurity culture. Leaders in the maritime industry must emphasise the importance of cybersecurity, allocate resources for training, and set expectations that all crew members actively participate in these programs. By promoting a top-down commitment to cybersecurity, organisations can gradually built a culture where crew members recognise the value of protecting both digital and physical assets (Trisolvena, 2024).

Overcoming these challenges requires innovative training methods, a commitment to flexibility, and a cultural shift towards prioritizing cybersecurity as a core aspect of maritime operations.

These efforts will ensure that crews are better prepared to identify, respond to, and mitigate cyber threats, safeguarding both their vessels and the broader maritime industry.

5.2.9 Designing Early Threat Detection Modules

Developing effective training modules for early threat detection is essential to equip maritime crews with the skills needed to recognise and respond to potential cyberattacks before they escalate. **Interviewee 1** emphasised that a strong training program should begin with fundamental knowledge of common threats, including **phishing, malware, and ransomware**. Practical exercises should form the backbone of the module, enabling crew members to identify suspicious activities, such as unauthorised updates, abnormal error messages, or phishing attempts disguised as legitimate communications. These practical exercises can help bridge the gap between theoretical knowledge and real-world application, ensuring that crew members understand not just what to look for but how to act.

Role-playing scenarios is another key suggestion from **Interviewee 1**, are invaluable in enhancing the learning experience. These scenarios should mimic real-world incidents, such as identifying an email that appears to be from a shipping company but includes malicious links or noticing irregular activity on a system dashboard. These immersive exercises provide hands-on experience in recognising threats and applying the appropriate response protocols.

Interviewee 2 highlighted the importance of focusing on the recognition of abnormal system behaviors, such as unexpected system delays, unauthorised updates, or erratic operational patterns. These signs are often early indicators of a cyberattack, such as malware infiltration or system manipulation by an external attacker. To address this, training modules should incorporate **interactive simulations** that replicate such anomalies. For example, trainees could practice identifying discrepancies in GPS coordinates caused by spoofing attacks or recognising sudden changes in network activity indicative of an intrusion.

Both interviewees agreed that **real-world case studies** should be an integral part of the training. These case studies would provide participants with practical examples of past incidents, illustrating how cyber threats were identified and mitigated. Case studies not only enhance understanding but

also make the training relatable by showing how theoretical concepts are applied in real maritime operations.

Another crucial component, as suggested by **Interviewee 2**, is teaching the protocols for reporting and responding to detected threats. Modules should include step-by-step instructions on what crew members should do when they notice suspicious activity, including whom to inform, how to document the issue, and the immediate actions required to contain the threat. This ensures that the entire crew is aligned and ready to act swiftly, reducing response times and preventing further damage. These training modules should also be role-specific, addressing the distinct responsibilities of various crew members. For example, engineers might focus on securing systems like PLCs and addressing technical vulnerabilities, while navigation officers would concentrate on detecting anomalies in systems like ECDIS or AIS. Tailoring the training to specific roles ensures that every crew member is adequately prepared for the threats they are most likely to encounter.

By combining practical exercises, role-playing scenarios, interactive simulations, and real-world case studies, the proposed training modules can build both the technical expertise and situational awareness needed to handle cyber threats effectively. Incorporating the insights of the interviewees, this approach ensures that maritime crews are equipped not only to detect threats early but also to respond with confidence and precision, safeguarding shipboard systems and operations.

5.3 Case Studies in Maritime Cybersecurity

5.3.1 Virtual Training Environment (VTE): Building Real-World Readiness

The Virtual Training Environment (VTE) is a pioneering program designed to enhance maritime cybersecurity by providing hands-on, realistic training for ship crews. This program replicates real-world cyber threats, such as phishing attempts, ransomware attacks, and GPS spoofing, in a safe and controlled virtual environment. Through these simulations, crew members can practice identifying and responding to complex cyber threats without risking actual operations. For instance, a phishing scenario might involve a simulated email attempting to trick crew members into sharing sensitive information, while GPS spoofing exercises could simulate navigational disruptions, training crews to identify and mitigate these issues effectively (Nikolov, 2024).

One of the key benefits of the VTE program is its focus on role-specific training, which ensures that all crew members, from navigation officers to IT personnel, are equipped to handle threats relevant to their specific responsibilities. By tailoring exercises to different roles, the training not only improves technical skills but also fosters better collaboration and teamwork during high-pressure situations. This approach is particularly valuable in enhancing crew confidence, as participants gain the practical knowledge needed to act decisively when faced with real-world challenges (Nikolov, 2024).The lessons learned from the VTE program highlight the importance of continuous training to keep pace with evolving cyber threats. Crew members have shown significant improvement in their ability to detect early warning signs, such as unauthorised system changes or suspicious emails, and respond promptly to contain threats. Additionally, the program underscores the necessity of aligning cybersecurity training with international standards like the ISM and ISPS codes, ensuring that maritime operations remain secure and compliant (M. Baldauf, 2016).

Overall, the VTE program demonstrates how simulation-based training can bridge the gap between theoretical knowledge and practical application, ultimately strengthening maritime cybersecurity readiness and resilience. This innovative approach serves as a model for integrating cybersecurity into regular crew training, ensuring safer and more secure maritime operations globally

5.3.2 Case Study: Multidimensional Simulation Frameworks

Multidimensional simulation frameworks are an innovative approach to training maritime crews for a variety of cyber incidents, such as phishing, malware intrusions, and GPS spoofing. These simulations create immersive, real-world scenarios where crew members can practice identifying, managing, and mitigating cyber threats in a controlled environment. For example, one scenario might simulate a cyberattack on navigation systems, requiring the crew to detect false GPS signals and implement alternative strategies to maintain course. Another scenario might focus on a simulated malware breach, teaching participants to isolate affected systems and prevent the attack from spreading (Arachchilage, 2014).

A key strength of multidimensional simulations is their emphasis on collaboration and teamwork. Effective cybersecurity in maritime operations often relies on seamless communication and

coordination between different departments, such as deck officers, engineers, and IT personnel. These frameworks encourage crew members to work together, share information, and rely on one another's expertise during high-pressure situations. For instance, during a simulated attack, engineers might focus on stabilising mechanical systems, while IT specialists troubleshoot the network, and deck officers ensure safe navigation. This collaborative approach prepares crews to function cohesively during real-life incidents, reducing response times and minimising operational disruptions (Androjna, 2020).

Role-specific exercises are another critical component of these simulations. Training is tailored to the unique responsibilities of each crew member. For example, navigation officers might learn to detect spoofed GPS signals, while engineers are trained to secure machinery systems like PLCs from cyber intrusions. This targeted training ensures that every individual understands the threats they are most likely to encounter and how to respond effectively. In addition to technical skills, multidimensional simulations also develop non-technical skills such as decision-making, critical thinking, and communication under stress. High-pressure scenarios help crew members build confidence, enabling them to remain calm and make sound decisions in real-life emergencies. This dual focus on technical and non-technical skills ensures that crews are well-rounded and capable of addressing the multifaceted challenges posed by cyber threats (M. Baldauf, 2016).

Overall, multidimensional simulation frameworks offer a comprehensive and practical way to enhance maritime cybersecurity readiness. By combining role-specific training, collaboration, and skill development, these simulations equip crews with the knowledge and confidence needed to safeguard ship operations in an increasingly digital and interconnected maritime landscape.

5.4. Alignment Between Interview Insights and Case Studies

The insights gathered from interviewees align closely with the findings from the case studies, reinforcing the practical applicability of the proposed training protocols. Both the interviews and case studies emphasised the critical role of hands on, simulation-based training in addressing the unique cybersecurity challenges faced by maritime crews. For instance, **Interviewee 1** highlighted the importance of practical exercises, such as mock phishing scenarios and system manipulation drills, to build confidence and readiness among crew members. This perspective is mirrored in the

Virtual Training Environment (VTE) case study, which demonstrated how simulated ransomware and GPS spoofing scenarios can effectively prepare crews for real-world threats (Nikolov, 2024).

Furthermore, **Interviewee 2** stressed the significance of role-specific training, pointing out that engineers and navigation officers face different types of cyber risks and require tailored exercises. This insight resonates with the multidimensional simulation framework discussed in case studies, where customized modules were designed for specific roles to enhance both technical and non-technical skills (M. Baldauf, 2016). Such alignment underlines the importance of tailoring training to the diverse responsibilities aboard ships.

Additionally, both interviewees underscored the need for iterative training approaches, which is strongly supported by the Design Cycle Framework explored in the case studies. The process of testing, evaluating, and refining training protocols ensures that they remain relevant in the face of evolving cyber threats. For example, feedback from simulated drills, such as response times and system recovery efficiency, provides actionable insights to continuously improve crew preparedness. This alignment between expert interviews and case studies underscores the validity of integrating simulation-based training as a cornerstone of maritime cybersecurity programs. By combining expert opinions with documented outcomes from real-world applications, this research offers robust recommendations to enhance the cybersecurity posture of the maritime industry.

5.4.1 Implications for Maritime Cybersecurity Training

The findings emphasise the urgent need to standardise maritime cybersecurity training across the industry, aligning it with international standards such as the ISPS and ISM Codes. These codes stress the importance of risk management, operational safety, and preparedness in maritime operations, particularly given the rising cyber threats targeting shipboard systems and infrastructure. Training programs that adhere to these frameworks not only ensure regulatory compliance but also elevate crew readiness to address cyber incidents effectively.

One significant implication is the integration of practical, hands-on training modules that align with the ISPS and ISM Codes. As outlined by studies, compliance with these codes involves developing a robust cybersecurity framework encompassing technical and human-centric defenses (E. Othman, 2005). For example, the ISPS Code mandates that ship personnel have specific

security knowledge and participate in regular security exercises, ensuring that all crew members are familiar with procedures to prevent cyber breaches.

Additionally, aligning training modules with the iterative improvement principles of the ISM Code can enhance the effectiveness of cybersecurity protocols. Studies highlight that regular feedback from simulations and real-world experiences helps refine these protocols, making them adaptive to evolving threats (Mukherjee, 2007). For example, drills focusing on phishing attempts or malware infiltration can uncover vulnerabilities, which can then be addressed in future training cycles.

By embedding international standards into the training curriculum, maritime organisations can foster a culture of proactive cybersecurity awareness. This approach ensures that all crew members, regardless of role or technical expertise, are equipped to identify, report, and mitigate potential threats, aligning operational practices with global expectations for safety and security (X. M. Zhao, 2005). Moreover, it builds stakeholder confidence by demonstrating a commitment to maintaining high safety standards across the maritime network.

5.4.2 Addressing Key Gaps

Despite advancements in maritime cybersecurity training, significant gaps remain in current practices. Interviewees emphasised challenges such as varying levels of IT knowledge among crew members and the lack of a cybersecurity culture on ships. These issues, combined with findings from case studies, highlight the need for more inclusive and standardised training programs that can bridge these critical gaps effectively.

One key gap is the insufficient attention to role-specific training. While engineers and IT personnel require in-depth knowledge of system vulnerabilities, deck officers need skills to protect navigational systems from threats like GPS spoofing. **Interviewee 2** stressed that tailored training modules are essential, as engineers and deck officers face vastly different challenges customised training ensure all roles are equally prepared. This is supported by case studies showing that multidimensional simulations are highly effective in preparing crews for their specific responsibilities (M. Baldauf, 2016).

Another major gap is the lack of consistent updates to training protocols to match evolving cyber threats. As highlighted by both interviewees and case studies, outdated modules fail to prepare crews for modern challenges like phishing and malware infiltration. A solution lies in integrating iterative improvements into training programs, using feedback from vulnerability testing and real-world incident analysis to keep the content relevant (E. Othman, 2005).

Finally, the gap in fostering a cybersecurity-conscious culture onboard ships must be addressed. **Interviewee 1** highlighted that many crew members prioritise operational tasks over cybersecurity, often underestimating the risks associated with poor cybersecurity practices, such as neglecting to follow security protocols, using weak passwords, or failing to report suspicious activities. . Addressing this requires embedding cybersecurity into daily routines through regular drills, accessible training materials, and practical examples of potential threats, such as the consequences of failing to secure personal devices or detect phishing emails.

Bridging Gaps in Maritime Cybersecurity Training

To address the identified gaps, maritime organisations should adopt strategies that effectively prepare crews for the dynamic nature of cyber threats. Firstly, role-specific training modules are essential to provide specialised knowledge tailored to the distinct responsibilities on board. For instance, engineers need to secure operational machinery, while deck officers must focus on navigation systems vulnerable to threats like GPS spoofing. Tailored modules ensure that every crew member is trained in the specific challenges they face, enhancing their readiness and confidence to respond effectively. **Interviewee 2** emphasised that tailored training helps to ensure equal preparedness across roles, while case studies support the effectiveness of focused learning strategies (Nikolov, 2024).

Additionally, **updating training content regularly** is critical to keeping pace with the evolving cybersecurity landscape. Emerging threats like advanced phishing schemes or malware variants demand training that reflects current realities. Integrating feedback from simulations can help refine training modules, ensuring they stay relevant and effective. For example, response metrics from exercises, such as how quickly threats are identified and neutralised, can shape future training improvements (E. Othman, 2005).

Finally, fostering a **cybersecurity-conscious culture** is vital. Linking cybersecurity practices to overall ship safety and efficiency can create a sense of ownership among crew members. For example, regular briefings and practical demonstrations can make abstract cyber risks more relatable. Both interviewees highlighted the importance of making cybersecurity a priority, with Interviewee 1 suggesting modular approaches to training that accommodate the tight schedules of maritime crews. Embedding cybersecurity into the daily workflow not only reinforces its importance but also aligns with international standards like the ISM and ISPS Codes, which mandate robust security protocols (X. M. Zhao, 2005).By addressing these gaps, the industry can ensure that crews are better prepared to protect ships from cyber threats while maintaining compliance with international safety standards like the ISPS and ISM Codes .

5.5 Conclusion

This chapter has brought together insights from expert interviews and case studies to provide a comprehensive understanding of the current state of maritime cybersecurity training. Key findings include identifying critical cyber threats, such as phishing, GPS spoofing, and malware, and the challenges posed by outdated systems and inconsistent crew awareness (Garcia, 2020). The interviews highlighted the importance of role-specific training, the need to foster a cybersecurity culture, and the value of hands-on simulations in preparing crews for real-world scenarios. Case studies, like the Virtual Training Environment (VTE) and multidimensional simulation frameworks, demonstrated how practical exercises can enhance technical skills, collaboration, and decision-making under pressure (Nikolov, 2024).These findings build directly on the research objectives outlined in Chapter 4, advancing the goal of developing effective test protocols and training modules that address the unique challenges of the maritime industry. By aligning interviewee perspectives with case study evidence, this chapter underscores the importance of integrating practical, up-to-date training methods to ensure crew readiness against evolving cyber threats (M. Baldauf, 2016).

As we transition into the next chapter, the focus will shift to actionable recommendations for implementing these insights in the maritime sector. These recommendations will aim to bridge existing gaps, standardise practices across the industry, and align with international standards, ultimately contributing to a safer and more resilient maritime cybersecurity framework.

Chapter 6: Conclusion

6.1 Recap of Research Objectives and Key Findings

The primary goal of this research was to explore how maritime crews can be better prepared to handle the growing risks posed by cyber threats. With the maritime industry increasingly dependent on digital systems for navigation, communication, and operational controls, addressing vulnerabilities has become a critical priority. This study set out to identify key cybersecurity challenges and propose training programs that enhance crew readiness and resilience (Nikolov, 2024).One of the most significant findings was the evolving nature of cyber threats, which include phishing, malware, GPS spoofing, and system intrusions. These threats often exploit outdated ship systems and gaps in crew awareness, creating vulnerabilities that jeopardise safety and operational continuity. Interviewees emphasised the dual challenge of addressing technical vulnerabilities and fostering a culture of cybersecurity among crew members (C.H. Chang, 2019).

The study also highlighted the effectiveness of simulation-based training and role-specific exercises in improving crew preparedness. Realistic scenarios, such as responding to phishing attempts or mitigating GPS spoofing, were shown to enhance technical skills and situational awareness. Aligning these programs with international standards like the ISPS and ISM Codes ensures a consistent framework for cybersecurity measures across the maritime industry (Nikolov, 2024).

Finally, actionable recommendations were proposed to bridge existing gaps in training practices. These included updating training content to reflect emerging threats, designing modules tailored to specific crew roles, and emphasising the importance of cybersecurity for safety and operational efficiency. By addressing these gaps, the maritime sector can build a more robust cyber defence against evolving cyber threats (Mersinas, 2022).

This recap underscores the importance of aligning research insights with actionable strategies, bridging theoretical knowledge with practical applications to create a safer and more resilient maritime industry.

6.1.1 Answers to Research Questions

Main Research Question

Effective test protocols to evaluate and enhance crew readiness for addressing cybersecurity threats in the maritime industry can be designed by integrating insights from expert interviews, case studies, and established international frameworks. The research highlights the need for a structured, multi-layered approach combining simulation-based training, role-specific exercises, and proactive tools like threat simulations and vulnerability testing. These protocols must address both technical and human factors to ensure resilience against evolving cyber threats.

Insights from interviews with cybersecurity experts revealed that one of the primary challenges is the lack of tailored training programs addressing the diverse expertise levels among crew members. Experts emphasised that training must move beyond theoretical knowledge and incorporate hands-on experiences, such as phishing simulations and exercises responding to GPS spoofing attacks. Case studies further supported these findings by demonstrating the effectiveness of real-world scenarios in preparing crew members to detect and mitigate threats. For example, a simulated ransomware attack on a ship's navigation system highlighted gaps in crew response time, underscoring the importance of iterative training exercises to improve decision-making under pressure (Kessler, 2020).

Additionally, **Vulnerability testing** emerged as a critical tool for identifying and addressing weaknesses in onboard systems. Experts noted that these tests are especially valuable for older vessels operating with legacy systems that are more susceptible to cyberattacks. Incorporating penetration tests as part of the protocols ensures that crews are prepared to handle specific vulnerabilities unique to their ship's systems (Nikolov, 2024). Case studies demonstrated that periodic vulnerability assessments helped reduce the risk of system intrusions and increased crew confidence in responding to identified risks.

International standards like the ISPS and ISM Codes provide a valuable framework for aligning these protocols with global practices. By embedding cybersecurity into routine operations and safety management systems, the protocols ensure that training is consistent, standardised, and scalable across vessels and shipping companies. This alignment fosters a culture of cybersecurity

awareness, ensuring crew members at all levels understand their role in safeguarding operations against cyber threats (Garcia, 2020).

In conclusion, effective test protocols must integrate technical defences with tailored training, iterative drills, and proactive assessments. By leveraging the combined insights from expert interviews, case studies, and global frameworks, the maritime industry can build a robust system for enhancing crew readiness and operational resilience in the face of escalating cyber threats. These protocols not only meet regulatory requirements but also establish a strong foundation for addressing future challenges in cybersecurity.

6.2 Addressing Key Challenges in Crew Cybersecurity Preparedness

Maritime crews face several challenges in identifying and responding to cybersecurity threats, stemming from a combination of outdated systems, insufficient training, and varying levels of technical expertise among crew members. Many vessels, particularly older ones, rely on legacy systems that lack modern cybersecurity protections, making them highly vulnerable to threats such as phishing, GPS spoofing, and ransomware attacks. Experts interviewed during this research emphasised that these outdated systems not only increase the risk of breaches but also make it more difficult for crew members to recognise and respond effectively to evolving cyber threats. For instance, one expert highlighted that crew members often struggle to differentiate between legitimate and malicious emails, leading to delays in addressing phishing attempts (Nikolov, 2024).

The lack of standardised cybersecurity training programs further exacerbates these vulnerabilities. Case studies demonstrated that while some maritime companies implement basic awareness campaigns, many fail to provide role-specific training that prepares crew members for real-world scenarios. For example, a case study on a simulated GPS spoofing attack revealed that the crew lacked the situational awareness needed to identify the manipulation of navigational data, which could have led to significant operational disruptions. This underscores the critical need for training that addresses both the technical and human dimensions of cyber resilience (Kessler, 2020).

Another challenge lies in the varying levels of technical expertise among crew members. Maritime crews often come from diverse backgrounds, with some having minimal exposure to digital

systems. This difference complicates the adoption of a uniform training model. Experts noted that engineers and officers may require different types of training tailored to their roles, such as engineers focusing on system vulnerabilities while deck officers are trained to identify operational threats like spoofed GPS signals. Without this differentiation, cybersecurity measures remain inconsistent, leaving critical gaps in crew preparedness (Garcia, 2020).

In summary, maritime crews face interconnected challenges driven by outdated systems, insufficient standardised training, and varying expertise levels. Insights from expert interviews and case studies highlight the urgent need for tailored, role-specific training programs and proactive tools to help crews effectively identify and respond to modern cyber threats. These steps are crucial to mitigate vulnerabilities and enhance overall cybersecurity resilience in the maritime sector.

6.3 Evaluating Training Methods for Maritime Cybersecurity

Training methods currently used in the maritime industry include **simulation drills**, **vulnerability testing**, and **awareness campaigns**, which aim to enhance crew preparedness against cybersecurity threats. Simulation drills are particularly effective in providing hands on experience, as they mimic real-world scenarios such as phishing attacks, GPS spoofing, and ransomware incidents. Experts interviewed during this research emphasised that these drills allow crew members to practice identifying and responding to threats in a controlled environment, building both their technical skills and confidence. For instance, a case study highlighted how a phishing simulation helped crew members recognise suspicious emails, reducing the likelihood of falling victim to actual attacks (Nikolov, 2024).

Vulnerability testing, such as penetration tests, is another key tool used to identify weaknesses in onboard systems like navigation and communication platforms. These tests not only uncover technical vulnerabilities but also help crews understand how such weaknesses can be exploited, reinforcing the importance of proactive monitoring and response. However, interviews revealed that while vulnerability testing is widely recognised as essential, its implementation across the industry is inconsistent, and often limited by resources and expertise (Technology, NIST (2020)).

Awareness campaigns, which focus on educating crew members about basic cybersecurity practices, are also employed. These campaigns typically cover topics such as recognising phishing

attempts, creating strong passwords, and reporting suspicious activity. While valuable, the research found that these initiatives often lack depth and fail to address role-specific needs. For example, engineers may need advanced training in detecting system anomalies, whereas deck officers might require a focus on operational threats like GPS interference. Experts and case studies both stressed that standardised and tailored training programs are critical to addressing these gaps and ensuring consistency across the industry (Martina Pivarníková, November 2020).

In summary, while existing methods such as simulation drills, vulnerability testing, and awareness campaigns provide a foundation for cybersecurity training, their effectiveness is undermined by inconsistencies and a lack of standardisation. Tailored programs that align with the specific responsibilities of crew members, coupled with regular updates to address emerging threats, are essential to improve preparedness and resilience in the maritime sector. By implementing such structured and role-specific training protocols, the industry can ensure that crews are equipped to handle evolving cyber threats effectively.

6.4 Adapting Simulations and Tests to Improve Crew Readiness

Threat simulations and vulnerability tests are critical tools for enhancing crew readiness, as they allow for the identification of potential risks and the development of effective response strategies. Simulation drills, such as those replicating phishing attacks, ransomware incidents, or GPS spoofing, are particularly valuable for providing hands-on experience. These exercises help crew members practice recognising anomalies and responding promptly under realistic conditions. For example, a case study involving a simulated GPS spoofing attack demonstrated how targeted drills improved crew situational awareness and response coordination, mitigating operational risks before they could escalate (M. Baldauf, 2016).

However, vulnerability tests and penetration testing (pen testing) introduce additional complexities. Unlike simulations, which focus on operational readiness, these tests require technical expertise to identify, exploit, and address system vulnerabilities. Interviewees highlighted that it is unrealistic to expect crew members, especially those without advanced technical training, to perform such tests independently. For instance, pen testing often involves sophisticated tools and methodologies, such as simulating zero-day attacks or exploiting

encryption weaknesses, which are outside the scope of standard crew training. Case studies further revealed that while pen tests uncovered critical vulnerabilities in communication and navigation systems, crews struggled to interpret the findings or take corrective action without external support (Bernardo Breve, 2024).

To overcome these challenges, experts emphasised the importance of integrating these tools with simplified, role-specific training for crew members. Rather than requiring crews to execute vulnerability tests themselves, the focus should shift to helping them understand the implications of test results and implementing recommended security measures. For example, training modules can teach deck officers how to recognise alerts generated by intrusion detection systems, while engineers can learn to apply specific security patches or reconfigure systems based on pen test reports. Collaborating with external cybersecurity professionals for periodic audits and advanced testing ensures that the complexities of vulnerability assessments are managed effectively, while still contributing to overall crew readiness (M. Canepa, 2021).

In summary, threat simulations and vulnerability tests can be adapted to enhance maritime cybersecurity by combining technical expertise with practical crew training. Simulation drills offer hands on learning opportunities, while external expertise ensures that complex assessments, such as pen tests, are conducted effectively by the cyber expert team periodically. By focusing on role-specific skills and integrating expert-led insights, the maritime industry can create a balanced and practical approach to building cybersecurity resilience.

6.5 Contributions and Implications

This research makes a significant contribution to strengthen maritime cybersecurity by addressing critical gaps in crew readiness, vulnerability management, and training protocols. It offers practical insights into creating comprehensive training programs tailored to the unique needs of the maritime industry, ensuring that both technical and non-technical crew members are prepared to handle evolving cyber threats. These findings align closely with international standards, such as the **International Ship and Port Facility Security (ISPS) Code** and the **International Safety Management (ISM) Code**, both of which emphasise the importance of risk management, secure operations, and proactive measures against cyber threats. By aligning proposed practices with these standards, this study provides a framework that is not only compliant but also scalable across different vessels and shipping companies (Divine C. Chupkemi, 2024).

The study also underscores the practical value of simulation-based training and iterative learning methods, which can be integrated seamlessly into maritime operations. Training programs based on real-world scenarios, such as phishing simulations and GPS spoofing drills, enable crew members to apply theoretical knowledge in practical contexts, bridging the gap between understanding and action. This ensures that maritime organisations are not only meeting regulatory requirements but also fostering a culture of cybersecurity awareness, which is crucial in the interconnected and increasingly digitised maritime sector (Kessler, 2020).

Moreover, the recommendations provided in this research address the industry's urgent need for standardised practices and collaborative solutions. By advocating for role-specific training modules, continuous content updates, and feedback loops from simulations, the study contributes to a proactive and adaptive cybersecurity framework. This framework helps mitigate risks effectively, ensuring that vessels remain operationally safe and secure against a backdrop of escalating cyber threats. Ultimately, these contributions not only improve operational resilience but also instill greater confidence among stakeholders in the maritime industry's ability to safeguard its assets and operations against emerging challenges (Garcia, 2020).

This section highlights how the research bridges theoretical understanding with actionable solutions, making it both practical for industry adoption and aligned with global maritime standards.

6.6 Final Reflections

Maritime cybersecurity is no longer an optional concern, it has become essential to keep global shipping operations safe, efficient, and resilient. As cyber threats grow more advanced, it is crucial for cybersecurity efforts to constantly evolve and improve. This research emphasises the urgent need for maritime organisations to take proactive and standardised steps to protect their operations. Cybersecurity isn't something that can be addressed once and forgotten, it's an ongoing process that demands regular updates, tailored training for different roles, and hands-on learning through practical simulations (BIMCO, 2024).

The interconnected nature of modern maritime systems amplifies vulnerabilities, making it imperative for organisations to prioritise cybersecurity as a shared responsibility among all crew members. By integrating comprehensive training programs and aligning with international standards like the **ISPS** and **ISM Codes**, maritime companies can create a unified framework for mitigating risks and enhancing operational resilience. The research underscores that fostering a culture of cybersecurity awareness is essential for empowering crew members to detect and respond to threats effectively, ultimately preventing incidents before they escalate (E. Othman, 2005).

This study calls for immediate action by maritime organisations to invest in cybersecurity as a critical operational priority. The maritime sector must embrace continuous learning, leverage innovative training tools like simulations, and commit to regular evaluations of their cybersecurity protocols. The stakes are too high to ignore. By making cybersecurity a cornerstone of maritime operations, the industry can not only protect its assets but also build trust and confidence among stakeholders, ensuring a safer future for global shipping (Ferney Martínez 1, January 2024).

References

Androjna, A. B. T. P. I. &. G. H., 2020. Assessing Cyber Challenges of Maritime Navigation.. *Journal of Marine Science and Engineering*..

Aobo Zhou, Q. Z. J. Z., 2023. *Ship Intrusion Detection Technology Based on Bayesian Optimization Algorithm and XGBoost*. s.l., s.n.

Arachchilage, N. &. L., 2014. Security awareness of computer users: A phishing threat avoidance perspective. *S Comput. Hum. Behav,* pp. pp. 304-312..

Armstrong, M. J. K. N. A. &. N. D., 2018. *The Knowledge, Skills, and Abilities Used by Penetration Testers: Results of Interviews with Cybersecurity Professionals in Vulnerability Assessment and Management*. .

Bernardo Breve, G. D. V. D. L. D. S., 2024. *Detection And Mitigation Of Cyber attacks that exploit human vuLnerabilitiES*. s.l., Proceedings of the 2024 International Conference on Advanced Visual Interfaces.

Bimco, 2024. BIMCO GUIDELINES.

BIMCO, I. &., 2024. *Cyber Security Work book for Onboard ship Use*. 5th ed. s.l.:Bimco & International Chamber Of Shipping.

BIMCO, I. O. S. O. A., n.d. *The Guidelines on cyber security onboard ships,* s.l.: s.n.

C.H. Chang, S. W. Z. W., 2019. Evaluating cybersecurity risks in the maritime industry.

Case Studies in Maritime Cybersecurity. (2021).

Chris W. Johnson, M. E., 25 August 2017. Defending Against Firmware Cyber Attacks on Safety-Critical Systems.

Divine C. Chupkemi, K. M., 2024. Challenges in Maritime Cybersecurity Training and Compliance. *Journal of Marine Science and Engineering*.

DNV, I. U. R. f. C. S., 2024. *Unified Requirements for Cyber SecurityMandatory from 1 January 2024*.. s.l.:s.n.

Dupont, B., 2019. *The cyber-resilience of financial institutions: significance and applicability,* s.l.: s.n.

E. Othman, A. H., 2005. Towards Effective Implementation of the ISPS Code Onboard Ships.

Elstial, A. M. K. S. N. &. G. T., 2024. *Enhancing Cybersecurity through Effective penetration testing and Vulnerability Scanning. International Science and Technology*.

ENISA.europa.eu, E. (. U. A. f. C., 2019. *Cybersecurity and Resilience of Smart Ships.,* s.l.: s.n.

Ferney Martínez 1, 2. ·. L. E. S. ·. A. S.-O. ·. D. G. R. ·., January 2024. Maritime cybersecurity: protecting digital seas. *International Journal of Maritime Security*.

Ferney Martínez1, 2. ·. L. E. S. ·. A. S.-O. ·. D. G. R. ·., 2 January 2024. Maritime cybersecurity: protecting digital seas. *International Journal of Information Security (2024) 23:1429–1457*.

Garcia, D. &. R., 2020. *The Role of Artificial Intelligence in Enhancing Maritime Cybersecurity.*. s.l., s.n.

Georgios Potamos, A. P. S. S., 2021. Towards a Maritime Cyber Range training environment. *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*.

Greenberg, A., 2018. *The untold story of NotPetya, the most devastating cyberattack in history. Wired. Retrieved from [Wired](https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/)*. [Online]
[Accessed September 2024].

Greenberg, A. T. U. S. o. N. t. M. D. C. i. H. W. R. f. W., 2018. *Greenbe The Untold Story of NotPetya, the Most Devastating Cyberattack in History. ,* s.l.: Wired.com.

https://www.nhlstenden.com, n.d. *maritime-cyber-attack-database,* s.l.: s.n.

Iacs, 2023. [Online]
[Accessed 2024].

Ibokette, A. O. T. A. A. A. F. O. I. &. O. F., 2024. Mitigating Maritime Cybersecurity Risks Using AI-Based Intrusion Detection Systems and Network Automation During Extreme Environmental Conditions. *International Journal of Scientific Research and Modern Technology* .

IMO.org, I. M. G. o. M. C. R. M. I. R. M. A. f., 2021. *International Maritime Guidelines on Maritime Cyber Risk Management. IMO Resolution MSC.428(98). Available from: IMO.org*. [Online]
[Accessed October 2024].

IMO's MSC-FAL.1/Circ.3, n.d. provides detailed guidelines on maritime cyber risk management, highlighting network segmentation as a crucial component..

Imo, 2021. International Maritime Organization (IMO) Guidelines: IMO's Resolution MSC.428(98).

Insights, N. t. N. C. T. L. I. f. t. S. I. D., Deloitte. (2020).. *Navigating the New Cyber Threat Landscape: Insights for the Shipping Industry. Deloitte Insights. Available from: Deloitte.com,* s.l.: s.n.

Jones, K. T. K. &. P. M., 2012. Threats and Impacts in Maritime Cyber Security. Engineering & Technology Reference.

Jones, K. T. K., January 7,2019. MaCRA: A model-based framework for Maritime Cyber risk assessment. *WMU journal of Maritime Affairs (AM)*.

Kessler, G. C. &. S. S. (. M. C. A. G. f. L. a. M. A. H., 2021. *Maritime Cybersecurity: A Guide for Leaders and Managers*.. s.l.:s.n.

Kessler, G. C. &. S. S. (. M. C. T. R. a. I. o. C. A. o. t. M. S. J. o. M. R. 1. 2.-3., 2020. Maritime Cybersecurity: The Risks and Impact of Cyber Attacks on the Maritime sector. *Journal of Maritime Research, 18(2), 23-36.),* pp. 23-36.

Kessler, G. C., 2019. Kessler, G. C... *Cybersecurity in the Maritime Domain: A Growing Threat in Need of Mitigation." Journal of Information Warfare, 18(3), 22-34*.

Kessler, G. C., 2019. Maritime Cybersecurity: A Growing Threat Goes Unanswered." In The Maritime Executive. Retrieved from The Maritime Executive.

Kessler, G. C. i. m. T. b. a. c. o. i. n. t. i. t. s. i. M. T. a. R. 2. 1.-2., 2019. *Cybersecurity in maritime: The benefits and challenges of implementing new technology in the shipping industry Maritime Technology and Research, 2(3), 15-22*.. s.l.:s.n.

Kshetri, N., 2017. Can Blockchain Strengthen the Internet of Things. pp. 68-72.

Liu, W. X. X. W. L. Q. L. J. A. D. W. &. K. M., 2023. Intrusion Detection for Maritime Transportation Systems With Batch Federated Aggregation. *IEEE Transactions on Intelligent Transportation Systems,* pp. 24, pp. 2503-2514..

Lloyd's, 2021. *Cybersecurity guidance for shipowners and operators. Lloyd's register. Available from: LloydsRegister.com.* [Online]
[Accessed November 2024].

Louise Praestin Jepsen, P. H. M. N. K., 2024. Increasing maritime cybersecurity awareness through game-based learning. *Journal of Physics: Conference Series*.

Lund, M. H. O. &. J., 2018. An Attack on an Integrated Navigation System.

M. Baldauf, J. S.-H. A. K. K. B. G. T., 2016. Multidimensional simulation in team training for safety and security in maritime transportation. *Journal of Transportation Safety & Security*.

M. Canepa, F. B. D. D., 2021. ASSESSING THE EFFECTIVENESS OF CYBERSECURITY TRAINING AND RAISING AWARENESS WITHIN THE MARITIME DOMAIN.

M. Canepa, F. B. D. D. S. V., 1 March 2021. *Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain*. s.l., s.n.

Marco Balduzzi, A. P., 2014. *A security evaluation of AIS automated identification system*. s.l., s.n.

Martina Pivarníková, P. S. B., November 2020. Early-Stage Detection of Cyber Attacks.

McCauley, J. (., 2020. GPS Jamming Incidents Rise in Shipping Hotspots. Maritime Executive.. *Maritime Executive.*.

Mersinas, K. &. D. C., 2022. Reducing the Cyber-Attack Surface in the Maritime Sector via Individual Behaviour Change.

MSC-FAL.1/Circ.3., n. M. O. (. (. G. o. M. C. R. M., 2017. *nternational Maritime Organization (IMO). (2017). Guidelines on Maritime Cyber Risk Management. MSC-FAL.1/Circ.3.*. [Online]
[Accessed 2024].

Mukherjee, P., 2007. The ISM Code and the ISPS Code: A critical legal analysis of two SOLAS regimes. *WMU Journal of Maritime Affairs*.

Nikolov, B., 2024. *Approach to Developing a Maritime Cybersecurity Virtual Training Environment*. s.l., Proceedings of the 15 th International Scientific and Practical Conference. Volume II, 220-225.

Prashant Hari Narayan Rajput, M. M., 2021. Towards Non-intrusive Malware Detection for Industrial Control Systems. *Design, Automation & Test in Europe Conference & Exhibition*.

Rantos, A. D. *. a. K., 2024. Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2.0. *Marine Science and Engineering*.

Ryan Pickren, T. S. S. Z., 2024. Compromising Industrial Processes using Web-Based Programmable Logic Controller Malware.

Sabillon, R., 2021. *Audits in Cybersecurity,* s.l.: s.n.

SEA, H. T. D. A. J. A. S. A., 2019.

Senarak1, C., November 2023. *Port cyberattacks from 2011 to 2023: a literature review,* s.l.: s.n.

Silgado, D. M., 11/4/2018. *Cyber-attacks: a digital threat reality affecting the maritime Research Paper,* s.l.: s.n.

Silgado, D. M., 11-4-2018. *Cyber-attacks: a digital threat reality affecting the maritime.* [Online].

Silgado, D. M., 2018. Cyber-attacks: a digital threat reality affecting the maritime. Issue World Maritime University.

Silva, A. &. S. P. C. C. I. f. t. M. I., 2020. Collaborative Cybersecurity Intelligence for the Maritime Industry. *In Journal of Maritime Research, 16(2),* pp. 203-216..

Specialty, A. G. C. &., 2021. • *Safety and Shipping Review 2021*. *(https://www.agcs.allianz.com/news-and-insights/reports/shipping-safety.html)*. [Online] [Accessed September 2024].

Taheri, M. N. M. &. K. K., 2023. Detection and Identification of GNSS Spoofing Cyber-Attacks for Naval Marine Vessels.. *IEEE International Symposium on Inertial Sensors and Systems (INERTIAL),* pp. pp. 1-4..

Technology, G. t. V. S. .. N. I. o. S. a. T., NIST (2020). *Guide to Vulnerability Scanning (Special Publication 800-115). National Institute of Standards and Technology.,* s.l.: s.n.

Thompson, B. M., 2014. GPS Spoofing and Jamming.

Trisolvena, M. &. S. N., 2024. Phishing Cyber Security Threats. *Jurnal Improsci.*.

Working, C. C. R. M., 2020. *Cyber Security Implementation Guidelines: Essential Security Practices for the Shipping Industry. International Chamber of Shipping.,* s.l.: s.n.

X. M. Zhao, Y. C. W. R., 2005. Examining and Promoting ISPS Code Training for Chinese Seafarers.

Xudong He, J. W. J. L., 2023. DNS Rebinding Threat Modeling and Security Analysis for Local Area Network of Maritime Transportation Systems. *IEEE Transactions on Intelligent Transportation*.

Y. Yoo, H.-s. P., 24 May 2021. Qualitative Risk Assessment of Cybersecurity and Development of Vulnerability Enhancement Plans in Consideration of Digitalised Ship. *Journal of Marine Science and Engineering*.

Ye, N. Z. Y. &. B. C., 2004. Robustness of the Markov-chain model for cyber-attack detection.. *IEEE Transactions on Reliability,* pp. 53, pp. 116-123.

Zachry Basnight, J. B. J. L., 2013. Firmware modification attacks on programmable logic controllers.