

**ROYAL MILITARY ACADEMY**

175<sup>th</sup> Promotion POL  
Colonel Joseph WARNAUTS

**Academic year 2024 – 2025**

2<sup>nd</sup> Master

# **Design and Implementation of a Naval Cyber Range for Cybersecurity Awareness and Research**

Second Lieutenant Officer Cadet

Louis-Henri LAQUAY



Master Thesis of the department CISS  
presented to obtain the academic degree  
of Master in Engineering Science  
under the supervision of Lieutenant Colonel Thibault DEBATTY, Dr. ir  
Brussels, 2025



# **Design and Implementation of a Naval Cyber Range for Cybersecurity Awareness and Research**

Louis-Henri LAQUAY





# Abstract

The digitalization of naval platforms, with the growing interconnection of their IT (Information Technology) and OT (Operational technology) systems, have made warships increasingly vulnerable to cyber threats. Despite this critical exposure, the maritime sector, and especially the naval domain, still suffers from a lack of controlled, realistic environments to train crews, test defences, and simulate cyberattacks. The need for tailored and operationally relevant maritime cyber ranges has never been more urgent.

This thesis addresses that gap by developing a naval cyber range designed to emulate the onboard network architecture and cyber-physical interactions of Belgian next-generation Mine Countermeasure (MCM) warships. Unlike generic models, this work delivers a runnable prototype based on a carefully simplified version of the complex MCM warship network, balancing realism and resource efficiency.

The naval cyber range is built to simulate the digital environment of a modern warship, combining virtual machines and lightweight container modules to realistically reproduce onboard systems. It features simulated communications across standard maritime protocols, including navigation, automation, and radar data flows. A central ship simulator continuously generates dynamic vessel data, such as position, heading, and speed, which is shared across the simulated systems to ensure consistency. The platform includes realistic interfaces for crew interaction, such as bridge navigation displays, radar screens, and control panels. It also supports core network services like email, internal name resolution, and scenario-specific attack tools. Together, these components create a rich and interactive environment for training, testing, and threat simulation.

To validate its training potential, a complete cyber awareness scenario was implemented and tested with volunteer participants during a live session at the Royal Military Academy. The scenario involved a phishing attack, malware deployment, lateral movement to a server, GPS spoofing, and radar denial-of-service. Trainees were tasked with detecting, analysing, and remediating the intrusion in real-time while navigating the simulated ship to accomplish their mission. The session was a success, providing high engagement, meaningful learning outcomes, and extensive feedback.

The thesis delivers several concrete contributions: a functional naval cyber range prototype with a modular and scalable architecture, a fully developed cyber awareness scenario, and an AI-ready platform capable of generating realistic maritime traffic datasets. Performance was validated under resource-constrained conditions, confirming feasibility even without commercial infrastructure.

Looking forward, the cyber range opens new pathways for research, including automated threat detection, AI integration, and the creation of high-fidelity maritime datasets. With further collaboration and system expansion, the prototype could evolve into a production-grade naval cyber range for training, research, and defence development.

This work lays the foundation for a unique operationally relevant naval cyber training environment available to Belgian Defence, where realism, flexibility, and innovation converge to support maritime cybersecurity excellence.



## Preface

This master thesis constitutes the final step in the pursuit of the academic degree of *Master in Engineering Science*. It represents the culmination of my work and research conducted during the final year of my studies, and reflects both an academic journey and a personal commitment to advancing knowledge in the field of cybersecurity.

I would first like to express my sincere gratitude to my promoter, Lieutenant Colonel Thibault Debatty, Dr. ir, for his dedicated supervision throughout the entire research process and the redaction of this thesis. His thoughtful guidance and insightful suggestions consistently pushed the project forward and added significant value to its development.

My deepest appreciation also goes to my second reader, Mr. Yemen Rhouma, ir, whose unwavering support proved essential for the successful execution of this project. His clear and practical advice, as well as his considerable efforts in ensuring I had access to the necessary infrastructure and resources, were invaluable. His active involvement and continuous feedback played a key role in keeping the project on track and aligned with its objectives.

I would also like to warmly thank the three volunteer participants who engaged in the cyber awareness training session conducted as part of this thesis. Their involvement and constructive feedback provided important insights into the practical relevance and usability of the developed solution.

In addition, I wish to acknowledge the support of my fellow students of the 175<sup>th</sup> promotion POL. The mutual encouragement and camaraderie we shared during both the thesis period and our broader university journey have been truly meaningful. I extend heartfelt thanks to my family for their ongoing interest in my work and for the foundational education and values they have instilled in me.

A special mention goes to the Polytechnic student association and its members, whose countless enjoyable moments and shared experiences offered me much-needed balance and relief throughout my studies.

Finally, I am thankful for the strength and clarity I found through faith during the course of this work.

*Laquay L.*  
Brussels, 2025



# Contents

<b>Abstract</b>	<b>i</b>
<b>Preface</b>	<b>iii</b>
<b>List of Figures</b>	<b>ix</b>
<b>List of Tables</b>	<b>xi</b>
<b>List of Abbreviations</b>	<b>xiii</b>
<b>1. Introduction</b>	<b>1</b>
1.1. Background and Motivation . . . . .	1
1.2. Problem Statement . . . . .	2
1.3. Objectives and Contributions . . . . .	3
1.4. Scope and Limitations . . . . .	3
1.5. Structure of the Thesis . . . . .	4
<b>2. Literature Review and State of the Art</b>	<b>5</b>
2.1. Maritime Cybersecurity: A Growing Concern . . . . .	5
2.2. Existing Maritime Cyber Ranges and Training Tools . . . . .	5
2.2.1. Plymouth University Cyber-SHIP Lab . . . . .	6
2.2.2. European Union Cyber-MAR Project . . . . .	6
2.2.3. U.S. Navy USS Secure Cyber Testbed . . . . .	8
2.2.4. Maritime and Port Authority of Singapore (MPA) Maritime Testbed of Ship-board Operational Technology (MariOT) . . . . .	8
2.2.5. Genoa University Maritime cybersecurity Testbed (MaCySTe) . . . . .	8
2.3. Cybersecurity Training Methodologies Using Cyber Ranges . . . . .	10
2.3.1. U.S. Army Persistent Cyber Training Environment (PCTE) . . . . .	10
2.3.2. Cyber Simulation TRaining for Impacts to Kinetic Environment (CyberSTRIKE) . . . . .	10
2.3.3. European Union Cyber-MAR project . . . . .	11
2.4. Gaps and Opportunities Identified in Current Research . . . . .	12
2.4.1. Non-existence of Naval Cyber Range Usable by the Belgian Defence . . . . .	12
2.4.2. Cost of High Quality Maritime Cyber Ranges . . . . .	13
2.4.3. Cyber Ranges Incorporating Hardware Devices . . . . .	13
2.4.4. Converging Architecture in Existing Maritime Cyber Ranges . . . . .	13
2.4.5. Training Methodologies . . . . .	14
2.4.6. Open-source MaCySTe Project . . . . .	14
<b>3. Mine Countermeasure Warship Network Architecture Analysis</b>	<b>15</b>
3.1. Overview of Warship Information Systems . . . . .	15
3.1.1. Ship Networks Listing . . . . .	16
3.1.2. Ship Systems Overview . . . . .	16
3.2. Network Architecture on MCM Warships . . . . .	18
3.2.1. Conceptual Organisation of the Networks . . . . .	18
3.2.2. Mission Management System INFRAstructure (MMS Infra) Network . . . . .	19
3.2.3. Integrated Platform Management System (IPMS) Network . . . . .	21

3.2.4.	Integrated Bridge Management System (IBMS) Network . . . . .	23
3.2.5.	Integrated Communication Sub-System (ICS) Network . . . . .	24
3.3.	Simplification Choices for Simulation Purposes . . . . .	25
3.4.	Relevant Devices and Corresponding Communication Protocols . . . . .	26
3.5.	Requirements for a Realistic Yet Feasible Simulation . . . . .	27
<b>4.</b>	<b>Design and Framework Selection</b>	<b>29</b>
4.1.	Design Goals and Constraints . . . . .	29
4.1.1.	Available Resources . . . . .	29
4.1.2.	Possibility of a Cloud Solution . . . . .	29
4.1.3.	Framework Required Features . . . . .	30
4.1.4.	Simulation Needs . . . . .	31
4.2.	Selected Frameworks and Technologies: Justification and Integration . . . . .	31
<b>5.</b>	<b>Implementation of the Naval Cyber Range</b>	<b>33</b>
5.1.	Network Topology Setup . . . . .	33
5.1.1.	EVE-NG Installation . . . . .	33
5.1.2.	Images Installation . . . . .	34
5.1.3.	MCM Warship Network Architecture Implementation . . . . .	34
5.2.	Traffic Simulation Methodology and Data Flows . . . . .	38
5.2.1.	Problem of Distributed Data Generation . . . . .	38
5.2.2.	Centralized Simulation Approach . . . . .	39
5.2.3.	Implementation Using Bridge Command . . . . .	39
5.2.4.	Data Distribution via NATS Message Queue (MQ) and JetStream Key-value Store . . . . .	39
5.3.	Code and Configuration Files . . . . .	39
5.3.1.	Code Distribution and Development Workflow . . . . .	39
5.3.2.	Repository Structure . . . . .	40
5.4.	Software Development and System Components . . . . .	41
5.4.1.	Components Implementation . . . . .	41
5.4.2.	Podman Networks Implementation . . . . .	43
5.4.3.	Container Management . . . . .	43
5.5.	Modularity and Extensibility of the Project Structure . . . . .	43
5.6.	Graphical Interfaces for User Interaction . . . . .	44
5.6.1.	Ship Simulator Display . . . . .	44
5.6.2.	Radar Operator . . . . .	46
5.6.3.	Engine Operator . . . . .	48
5.6.4.	WECDIS Operator . . . . .	50
5.6.5.	Cyber Range Manager . . . . .	51
5.7.	Integration of Cyber Threats/Attacks . . . . .	52
5.7.1.	Design and Implementation of the Malware . . . . .	52
5.7.2.	Cyber Attack Sequence . . . . .	53
5.7.3.	Expected Trainee Response and Forensic Investigation . . . . .	57
<b>6.</b>	<b>Testing and Evaluation</b>	<b>59</b>
6.1.	Functional Testing and Validation . . . . .	59
6.1.1.	Infrastructure and Networking . . . . .	59
6.1.2.	Graphical User Interfaces . . . . .	59
6.1.3.	Cyber Attack Scenario . . . . .	60
6.2.	Performance Evaluation and Resource Usage . . . . .	60
6.3.	Cyber Awareness Training Session and Evaluation . . . . .	61
6.3.1.	Cyber Awareness Training Setup and Deployment Environment . . . . .	61
6.3.2.	Execution of the Cyber Awareness Scenario with Volunteer Trainees . . . . .	64
6.3.3.	Session Outcome and Observations . . . . .	68

6.3.4. Feedback from the Trainees Regarding the Cyber Awareness Scenario and Usability of the Naval Cyber Range . . . . .	69
6.4. Exportability and Future Reusability of the Project . . . . .	69
<b>7. Discussion</b>	<b>71</b>
7.1. Assessment of Objectives Fulfilled . . . . .	71
7.2. Strengths and Limitations of the Current Work . . . . .	71
7.3. Practical Relevance for Cyber Awareness Training . . . . .	72
7.4. Potential for Research in Maritime Cybersecurity . . . . .	73
<b>8. Future Work and Improvements</b>	<b>75</b>
8.1. Enhancing Cyber Awareness Training . . . . .	75
8.1.1. Use of More Powerful Hardware or Cloud Solutions . . . . .	75
8.1.2. Extending the Library of Available Maritime Cyber Threats . . . . .	75
8.1.3. Advanced Scenario Management Tools . . . . .	76
8.1.4. AI Integration in Cyber Training . . . . .	76
8.2. Enabling Maritime Cybersecurity Research . . . . .	76
8.2.1. Enhanced Realism and Complexity . . . . .	77
8.2.2. Integration of Machine Learning . . . . .	77
8.2.3. Traffic dataset creation . . . . .	77
8.3. Long-Term Vision for a Full-Scale Maritime Cyber Range . . . . .	77
<b>9. Conclusion</b>	<b>79</b>
9.1. Summary of Work . . . . .	79
9.2. Final Reflections . . . . .	79
<b>A. MCM Warship Network Architecture Additional Content</b>	<b>81</b>
A.1. MCM Warship IBMS Sub-Networks and Systems Overview . . . . .	81
<b>B. Framework Selection Additional Information</b>	<b>83</b>
B.1. Comparison Between Cloud Services and Owned Hardware Cyber Range Solutions . .	83
B.2. Evaluation of Available Tools and Frameworks for Cyber Range Platform Implementation	84
<b>C. Cyber Range Implementation and Network Configuration Details</b>	<b>85</b>
C.1. Device Images List and Installation Procedure . . . . .	85
C.2. Mail Infrastructure Installation and Configuration . . . . .	85
C.2.1. Mail Server Installation and Configuration . . . . .	85
C.2.2. Mail Client Installation and Configuration . . . . .	86
<b>D. Naval Cyber Range Management Useful Information</b>	<b>89</b>
D.1. Naval Cyber Range Sub-network and Virtual Machine List . . . . .	89
D.2. Container Management Useful Commands . . . . .	89
D.3. Links to Graphical User Interfaces . . . . .	90
D.3.1. IP Addresses URLs . . . . .	90
D.3.2. Name Resolution URLs . . . . .	90
<b>E. Scenario Additional Material</b>	<b>91</b>
E.1. Example Solution for Eradicating Malware and Performing Initial Forensics Analysis .	91
E.1.1. Malware Removal . . . . .	91
E.2. Scenario Tasking Mails . . . . .	92
E.3. Setup Explanation Briefing . . . . .	94
E.4. Mission Briefing . . . . .	100
E.5. Feedback Form and Results . . . . .	104





## List of Figures

2.1. Cyber range architecture overview of Cyber-MAR . . . . .	7
2.2. MaCySTe testbed containers architecture . . . . .	9
3.1. MCM warship network architecture overview . . . . .	18
3.2. MCM warship MMS INFRA network architecture . . . . .	19
3.3. MCM warship MMS INFRA VLANs . . . . .	21
3.4. MCM warship IPMS sub-network architecture . . . . .	22
3.5. Functional information flow summary for IBMS network . . . . .	23
3.6. MCM warship IBMS sub-network architecture . . . . .	24
3.7. MCM warship ICS sub-networks architecture . . . . .	25
5.1. Implemented naval cyber range topology in EVE-NG . . . . .	35
5.2. DNS resolution diagram . . . . .	37
5.3. Ship simulator bridge view with Heads-Up Display (HUD) . . . . .	45
5.4. Ship simulator bridge view without HUD . . . . .	45
5.5. ASTERIX radar GUI . . . . .	46
5.6. Navico radar GUI . . . . .	47
5.7. Navigation instruments GUI . . . . .	48
5.8. SGS monitoring GUI . . . . .	49
5.9. WECDIS GUI . . . . .	50
5.10. WECDIS GUI with track autopilot set . . . . .	51
5.11. Phishing mail used as entry point for the malware . . . . .	54
5.12. Attacks to launch from the radar desktop machine by the cyber range manager . . . . .	54
5.13. Cyber Range Manager GUI with map and ship positions . . . . .	55
5.14. Cyber Range Manager GUI with ship list . . . . .	55
5.15. Attacks to launch from the IBMS server machine by the cyber range manager . . . . .	56
5.16. WECDIS under GPS spoofing attack . . . . .	56
5.17. ASTERIX radar under DOS attack . . . . .	57
6.1. Resource Usage on the EVE-NG Host by the Naval Cyber Range . . . . .	61
6.2. Setup with one large screen for ship simulation bridge view and briefings . . . . .	62
6.3. Setup with three machines for the trainees . . . . .	63
6.4. Setup with one machine for the manager . . . . .	63
6.5. Timeline of the cyber awareness scenario execution . . . . .	64
6.6. Setup explanation and mission briefing before the scenario . . . . .	65
6.7. Mail received by a trainee with tasks related to his function . . . . .	65
6.8. Completion of their respective tasks by the trainees . . . . .	66
6.9. Launch of the cyber attacks on the attack GUI by the cyber range manager . . . . .	66
6.10. Trainee reacting against a GPS spoofing attack on the WECDIS . . . . .	67
6.11. Trainee facing a DOS of his ASTERIX radar . . . . .	67
6.12. Removal of the malicious processes by the trainees . . . . .	68



## List of Tables

3.1.	MCM Warship Networks and Systems Overview . . . . .	17
3.2.	Sub-Network Systems and Protocols to implement . . . . .	26
5.1.	Summary of Modules Implemented per Host Virtual Machine . . . . .	42
A.1.	MCM Warship IBMS Sub-Networks and Systems Overview . . . . .	82
B.1.	Comparison Between Cloud Services and Owned Hardware During Development and Production . . . . .	83
D.1.	Summary of the Virtual Machines in the Simulated Network . . . . .	89
E.1.	Summary of Participant Feedback Responses . . . . .	105



## List of Abbreviations

AHRS	Attitude and Heading Reference System
AI	Artificial Intelligence
ARPA	Automatic Radar Plotting Aid
ASTERIX	All Purpose Structured Eurocontrol Surveillance Information Exchange
BDCS	Battle Damage Control System
BOD	Bridge Overhead Display
C&C	Command and Control
CCTV	Closed-Circuit TeleVision
CCU	Control Computing Unit
CIC	Combat Information Center
COMOPS	Operational Communication
DGNSS	Differential Global Navigation Satellite System
DMZ	DeMilitarized Zone
DNS	Domain Name System
DOS	Denial of Service
DPS	Dynamic Positioning System
DPS2	Dynamic Positioning System Level 2
DPS2	Dynamic Positioning System
DVL	Doppler Velocity Log
ECDIS	Electronic Chart Display and Information System
EIB	Electronic Information Board
EM Log	Electromagnetic Log
EO/IR	Electro-Optical/Infra-Red
FDS-Net	Fire Detection System Network
GFE	Government Furnished Equipment
GPU	Graphical Processing Unit
GUI	Graphical User Interface
GW	Gateway
HDR	Helo Deck Radar

HUD Heads-Up Display  
 HVAC Heat, Ventilation & Air Conditioning  
 HVAC Heat, Ventilation and Air Conditioning  
 IBMS Integrated Bridge Management System  
 ICCP Impressed Current Cathodic Protection  
 ICD Interface Control Document  
 ICS Integrated Communication Sub-System  
 IFF Identification Friend or Foe  
 INS Inertial Navigation System  
 INS Inertial Navigation System  
 INS Inertial Navigation System  
 INS Integrated Navigation System  
 INU Inertial Navigation Unit  
 IPMS Integrated Platform Management System  
 IT Information Technology  
 LPI Low Probability of Intercept  
 MAS Mine Avoidance Sonar  
 MFC Multi-Function Console  
 MFD Multi-Function Display  
 MIL GPS Military Global Positioning System  
 MISF Malware Information Sharing Platform  
 MMHS Military Message Handling System  
 MMS Mission Management System  
 MMS INFRA Mission Management System INFRAstructure  
 MQ Message Queue  
 MSK Masterclock System  
 MSR Multifunction Surveillance Radar  
 MTWAN Multi-Tactical Wide Area Network  
 MW Mine Warfare  
 NAT Network Address Translation  
 NCS Navigation Civil System  
 NDDS Navigation Data Distribution System  
 NTP Network Time Protocol  
 OSMS Onboard Signature Management System  
 OT Operational Technology

PKI    Public Key Infrastructure  
 PLC    Programmable Logic Controller  
 PPI    Plan Position Indicator  
 PW    Principal Warfare  
 RBAC   Role-Based Access Control  
 RSCP   Radar Status and Control Panel  
 RTU    Remote Terminal Unit  
 RWS    Remote Weapon System  
 SATCOM   Satellite Communication  
 SCC    Ship Control Center  
 SCG    Small Caliber Gun  
 SEWA   Sensor Weapon Systems  
 SGCS   Steering Gear Control System  
 SGS    Steering Gear System  
 SIEM   Security Information and Event Management  
 SMMD   Système de Mission Multi Drones  
 SPMS   Ship Proximity Management System  
 SRS    Sound Reception System  
 SSO    Single Sign-On  
 TPU    Tactical Processing Unit  
 UMISOFT   Unmanned MCM Integrated System Software  
 VCM    Video Control Management  
 VCMS   Voice Control and Monitoring System  
 VDR    Voyage Data Recorder  
 VLAN   Virtual Local Area Network  
 VM    Virtual Machine  
 WAIS   Warship Automatic Identification System  
 WECDIS   Warship Electronic Chart Display and Information System





# 1. Introduction

Modern warships have evolved into complex, networked platforms where critical operations, from propulsion and navigation to combat systems and logistics, depend on tightly integrated information and operational technologies. This transformation, while enhancing capabilities, has also introduced new vulnerabilities. As cyber threats grow in both sophistication and impact, the maritime domain (and naval forces in particular) face increasing pressure to develop effective training, awareness, and defence strategies. Yet, there remains a lack of realistic, mission-relevant environments in which operators can experience, understand, and respond to cyber incidents.

This thesis responds to that challenge by designing and implementing a simulation environment that emulates the digital infrastructure and traffic of a modern warship, based on a simplified yet representative architecture inspired by the complex systems of next-generation Mine Counter-Measure (MCM) vessels developed for the Belgian Defence. This abstraction process, balancing operational fidelity with research feasibility, constitutes a significant contribution in itself. The platform serves as a foundation for a Naval Cyber Range, enabling scenario-based training and controlled threat experimentation. Beyond its immediate use for cyber awareness, the simulation is developed with extensibility in mind, laying the groundwork for future research, particularly in AI-supported cyber defence. In bridging operational realism with technical modularity, this work contributes to addressing a critical gap in naval cybersecurity preparedness.

## 1.1. Background and Motivation

The increasing digitalization of maritime assets has given birth to a new era of operational efficiency and connectivity, but it has also introduced unprecedented cyber risks. Vessels, that were once isolated systems, now rely on integrated networks for navigation, propulsion, cargo management, communication, and combat operations. This convergence of IT (Information Technology) and OT (Operational Technology) has expanded the attack surface of ships and port infrastructures, creating significant security concerns for both commercial and military stakeholders.

One of the most infamous demonstrations of maritime cyber vulnerability occurred in 2017 with the NotPetya malware attack. Originally targeting Ukrainian infrastructure, NotPetya rapidly spread to global networks, including those of Maersk, one of the largest shipping companies in the world. The result was catastrophic: Maersk's operations were halted across 600 ports in 130 countries, with damages exceeding three hundred million dollars. [22, 42] The incident served as a wake-up call, revealing how collateral damage from state-sponsored attacks could cripple global maritime logistics. Other high-profile cases soon followed, including the 2018 cyber attack against China Ocean Shipping Company (COSCO) [21] and the 2019 ransomware attack targeting Norsk Hydro, a major maritime-linked industrial player. [36] These incidents highlight a troubling pattern of systemic vulnerability in maritime infrastructure and the increasing interest of cyber adversaries in targeting this sector.

In response to such threats, regulatory bodies have started to take action. The International Maritime Organization (IMO) introduced mandatory cybersecurity requirements in January 2021, compelling shipowners to integrate cyber risk management into their safety management systems. [24, 25] However, compliance alone does not guarantee preparedness. The complex interplay of legacy systems, proprietary protocols, and the lack of qualified cybersecurity personnel onboard means that many ships remain dangerously exposed.

Real-world cyber attacks have already impacted critical maritime components. GPS spoofing incidents, still observed in May 2025, have misled ship navigation in strategic zones such as the Black Sea [28,

37], while ransomware attacks have targeted major ports, including the 2021 breach at South Africa's Transnet port, which disrupted operations at container terminals and rail freight. [38] Moreover, as autonomous and remotely operated vessels begin to enter service, the attack surface expands to include AI navigation systems, satellite command links, and automated propulsion controls.

Despite these alarming developments, cybersecurity awareness and training in the maritime domain remain severely underdeveloped. Naval operators are often unprepared to detect, interpret, or respond to cyber incidents involving both IT and OT systems. In particular, there is a lack of structured, scenario-based training environments that reflect the reality of interconnected shipboard systems. Traditional cyber ranges and exercises tend to be generic and IT-centric, failing to account for the specificities of maritime contexts such as distributed control systems, deterministic data flows, and mission-critical isolation zones.

To fill this gap, Maritime Cyber Ranges are emerging as controlled environments for training, testing, and simulating cyber threats. A maritime variant must accurately reflect the layered architecture of ships, the hybrid nature of their IT/OT infrastructure, and the operational constraints of maritime missions. Warships, in particular, pose unique simulation challenges due to their classified systems, real-time operational requirements, and layered defence domains (e.g., bridge, combat, platform). Modelling such a vessel demands not only technical fidelity but also modular abstraction to maintain both realism and security.

In this context, this thesis contributes to the development of a realistic, extensible warship simulation environment. The platform aims to provide naval operators, engineers, and researchers with a safe space to rehearse cyber incidents, validate countermeasures, and explore vulnerabilities across network layers. Furthermore, with the growing interest in the application of Artificial Intelligence (AI) for threat detection and autonomous cyber defence [1, 10], the simulation lays the groundwork for future integration with AI training workflows. By generating realistic traffic, system behaviour, and threat scenarios, the cyber range becomes not only a training tool but also a testbed for machine learning models that require accurate, domain-specific input data.

As maritime systems continue to evolve toward hyperconnectivity and autonomy, the need for such platforms will only intensify. Without proactive simulation and preparedness, the next cyber incident may not merely delay a supply chain, it may compromise a nation's defence readiness.

## 1.2. Problem Statement

Modern warships, and in particular next-generation Mine Countermeasure (MCM) vessels, rely on an increasingly complex digital ecosystem composed of tightly integrated IT and OT systems. While these systems enhance operational capabilities, they also introduce critical cyber vulnerabilities that must be addressed through realistic training, testing, and research.

Yet, there is currently no publicly available, domain-specific simulation platform that reflects the unique structure, data flows, and threat exposure of such vessels. Traditional cyber ranges fail to capture the nuances of warship architectures, especially when it comes to deterministic communication patterns, embedded control systems, and mission-driven constraints. This lack of tailored, high-fidelity simulation tools represents a major barrier for naval cyber readiness and innovation.

At the same time, the classified and resource-intensive nature of real-world warship platforms makes direct experimentation infeasible for most research contexts. To bridge this gap, we must find a balance between fidelity and abstraction, preserving the key operational characteristics of the systems while simplifying their implementation for simulation and research purposes.

This thesis addresses the following research question:

**"How could we simulate, as close as possible from reality while simplifying for resource limitation purposes, the network and associated traffic of the new mine countermeasures warships of the Belgian army?"**

Answering this question is critical for enabling reproducible training scenarios, controlled cyber experiments, and ultimately, the development of AI-enhanced cyber defence systems adapted to naval environments.

### 1.3. Objectives and Contributions

The primary objective of this thesis is to design and implement a realistic simulation of the IT and OT networks of a modern warship, with a specific focus on Mine Countermeasure (MCM) platforms. This simulation aims to support cybersecurity awareness through scenario-based training while remaining extensible for future research applications.

To meet this goal, several sub-objectives are pursued:

- **Model key onboard systems** such as bridge operations, automation, platform management, and communication networks.
- **Simulate realistic network traffic** representative of routine operations and system interdependencies.
- **Integrate threat injection and monitoring mechanisms** to enable immersive cyber awareness scenarios.
- **Ensure modularity and scalability** to support adaptation to evolving research and operational needs.

This work yields the following tangible contributions:

- A fully operational **naval cyber range prototype**, including interfaces for visualization and interaction.
- A **modular simulation architecture** that emulates the digital ecosystem of a warship.
- A relevant **library of cyber threat scenarios** tailored to shipboard environments.
- Demonstrated **exportability** and **AI-readiness**, making the platform suitable for future automated detection and defence research.

### 1.4. Scope and Limitations

This thesis presents a research-grade prototype designed to simulate the IT and OT network environment of a modern warship. The platform serves as a proof of concept for cybersecurity awareness and scenario-based training but is not intended as a fully operational or certified training environment.

The scope of this work is limited to onboard ship systems. External maritime infrastructure such as port networks, satellite ground segments, and remote-operated mine warfare systems fall outside the perimeter of this study. While the simulation draws inspiration from next-generation Mine Countermeasure (MCM) vessels, many proprietary technologies and classified implementation details have been deliberately excluded or replaced by functional, open-source alternatives to ensure compliance and accessibility.

The simulated systems are simplified representations of real-world shipboard components. Not all subsystems have been implemented; instead, selected representative systems have been modelled to emulate the behaviour and interaction patterns of broader system categories. Similarly, cybersecurity scenarios are pre-scripted and do not involve real-time penetration testing or adversarial interaction.

Due to hardware constraints and budgetary considerations, the architecture has been optimized for modularity and scalability rather than completeness. Real-time AI components have not been integrated in the current version, though the platform is designed to support such extensions in future work.

Finally, this document does not disclose any sensitive or classified information pertaining to the actual network configuration or architecture of operational MCM warships, while still presenting the necessary concepts and a simplified network architecture.

## 1.5. Structure of the Thesis

This thesis is structured into nine chapters, each contributing to a logical progression from context and analysis to design, implementation, evaluation, and future directions. Each chapter builds upon the last to form a coherent response to the research question and to support the development of a realistic, adaptable, and forward-looking maritime cyber range.

- **Chapter 1 – Introduction** outlines the background, motivation, research problem, objectives, and scope of the study.
- **Chapter 2 – Literature Review and State of the Art** surveys the landscape of maritime cybersecurity, existing cyber ranges, and current simulation approaches. It identifies critical gaps, particularly the lack of realistic naval cyber training platforms accessible to European defence forces.
- **Chapter 3 – Mine Countermeasure Warship Network Architecture Analysis** provides a detailed examination of shipboard information systems, focusing on the digital architecture of Mine Countermeasure (MCM) vessels. It categorizes network domains, system functions, and communication protocols to define a feasible simulation model.
- **Chapter 4 – Design and Framework Selection** outlines the technical and operational constraints guiding the development. It justifies the choice of EVE-NG as simulation framework and defines core design principles to balance realism with modularity and resource efficiency.
- **Chapter 5 – Implementation of the Naval Cyber Range** details the construction of the simulated environment. This includes network setup, system emulation, traffic modelling, threat scenario integration, and the design of user interfaces for operators.
- **Chapter 6 – Testing and Evaluation** presents the validation strategy and results, covering functional testing, performance assessments, and cyber awareness training execution. It also evaluates the exportability and potential reuse of the platform.
- **Chapter 7 – Discussion** reflects on the degree to which objectives have been met. It analyses strengths, limitations, practical relevance for training, and potential for future research in maritime cyber domain, including AI-related experimentation.
- **Chapter 8 – Future Work and Improvements** proposes enhancements to cyber awareness training and enabling of maritime cybersecurity research. A long-term vision for scaling the cyber range is also discussed.
- **Chapter 9 – Conclusion** summarizes the contributions of the work, its significance, and the broader implications for maritime cybersecurity readiness.

## 2. Literature Review and State of the Art

### 2.1. Maritime Cybersecurity: A Growing Concern

As maritime systems grow more digital and interconnected, they also become increasingly exposed to cyber threats. This evolution is not limited to commercial shipping but critically affects naval platforms as well. Modern ship systems rely on both IT and OT components, ranging from propulsion and steering to radar and communications, often integrated into complex networks. While these integrations enable significant operational improvements, they also introduce expanded attack surfaces that adversaries can exploit.

One often overlooked issue is the fragmented development of these systems. Shipboard components are typically engineered and validated in isolated environments, making it difficult to detect vulnerabilities that only emerge during system integration. Traditionally, validating interoperability required physically assembling components, which was costly and logistically complex. Maritime cyber ranges address this challenge by enabling simulated system integration in controlled environments, offering a more efficient way to identify weaknesses early in the lifecycle.

Cybersecurity in maritime training remains another significant shortfall. Current educational pathways rarely include exposure to cyber incidents or threat response workflows, particularly those involving OT-specific risks. As vessels evolve into “systems of systems”, the range of failure scenarios that crews must be prepared for increases dramatically. Unfortunately, most operators are not trained to detect or mitigate such incidents under realistic mission constraints.

Moreover, maritime infrastructure has become a growing target for state and non-state actors. Shipboard systems often rely on legacy technologies that predate modern cybersecurity standards, limiting the applicability of contemporary defences. The attack surface now includes not just bridge systems and navigation sensors, but also maintenance networks, control panels and backend communication protocols. The challenge is compounded by the difficulty of patching or updating deployed systems, especially when ships are underway. [48]

Given these factors, the development of tailored maritime cyber ranges is not merely beneficial, it is essential. These platforms enable safe testing, training, and scenario-based exercises that reflect the operational complexity of modern naval systems. They allow multiple systems, simulated or real, to interact under realistic traffic and threat conditions, providing both technical insight and operational preparedness. For defence stakeholders, they offer a path to de-risking integration, enhancing cyber readiness, and ultimately ensuring mission continuity in an age of growing digital warfare.

### 2.2. Existing Maritime Cyber Ranges and Training Tools

The concept of developing cyber ranges specifically tailored to the maritime and naval domains is far from new. In fact, the results of prior research in this area are already being actively leveraged by the armed forces of various nations and international organizations for both training and research purposes. Several mature platforms now exist, each offering unique capabilities to simulate the hybrid IT/OT infrastructure of modern vessels and ports. This section presents and summarizes the core functionalities, scope, and technological features of some of the most prominent existing maritime cyber ranges, providing a foundation for comparison and contextualization of the work developed in this thesis.

### **2.2.1. Plymouth University Cyber-SHIP Lab**

The Cyber-SHIP Lab is not a cyber range in the traditional sense, but it remains highly relevant in the context of maritime cybersecurity initiatives. Developed by the University of Plymouth, the Cyber-SHIP Lab is a dedicated facility that brings together a wide range of IT and OT hardware components specifically used in the maritime domain. [47]

The facility supports the work of the Maritime Cyber Threats research group, whose objective is to build realistic maritime networks, spanning both ship and port infrastructure, using actual hardware. This enables the creation of physical twins of bridge networks and their associated operational control systems. By moving beyond virtual-only simulation, the lab offers unique capabilities for vulnerability testing on authentic maritime control devices. The insights gained from these experiments directly inform the development of cyber-resilient technologies intended to support secure maritime operations. [47]

Research conducted at the Cyber-SHIP Lab contributes to the formulation of cybersecurity best practices and policies for the maritime industry. These findings are typically applied to promote secure-by-design approaches in the development of next-generation maritime systems.

Widely regarded as a near world-leading facility in maritime cybersecurity, the Cyber-SHIP Lab owes much of its success to substantial support from industry, governmental bodies, and non-governmental organizations. [47] However, this level of realism and fidelity comes at a cost, such initiatives require significant financial investment, as well as access to and expertise in configuring authentic maritime systems. It is also worth noting that the facility's focus is primarily oriented toward commercial logistics vessels and does not extend to the unique operational requirements or cybersecurity challenges associated with naval warships in complex military environments.

### **2.2.2. European Union Cyber-MAR Project**

In 2019, the European Union launched an ambitious initiative in the field of maritime cybersecurity with the development of a cyber range specifically dedicated to the maritime logistics sector. The objective of this wide-scale project is to produce a comprehensive simulation environment that not only includes both port and vessel infrastructures, but also integrates a database of maritime-specific cyber threats alongside tools for decision support and risk analysis. [16]

A notable characteristic of this initiative is its hybrid nature. Like many high-quality cyber ranges, the Cyber-MAR project adopts a "hybrid" cyber range model, meaning that its simulated environment is directly connected to some real hardware systems. This approach was selected following research demonstrating that while real systems are superior for uncovering vulnerabilities and testing defensive mechanisms, simulated and emulated environments provide better scalability and repeatability for training programs. The hybrid model thus emerges as an effective compromise, enabling robust support for both operational research and cybersecurity training in the maritime domain. [43]

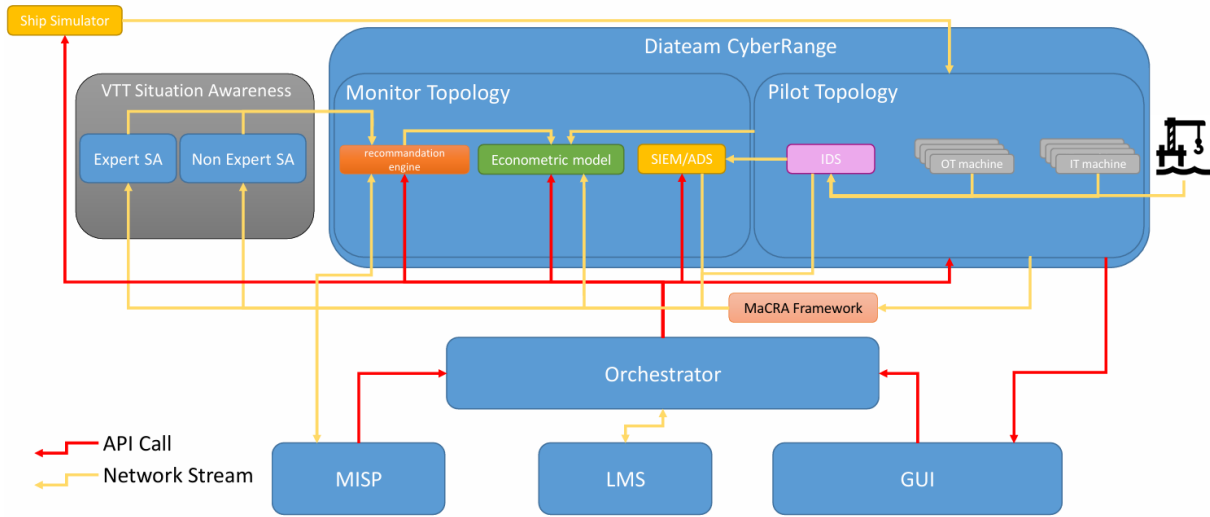


Figure 2.1. Cyber range architecture overview of Cyber-MAR [9]

As shown in Figure 2.1, which is derived from a Naval Group presentation of Cyber-MAR [9], the architecture of this cyber range incorporates the essential components of a comprehensive cyber attack simulation platform. Among these, several modules stand out as particularly relevant to the objectives of the present research:

- **Diateam CyberRange** (upper right, blue): This component is responsible for generating the virtualized training environment used by end-users. It also ensures the integration and interconnection between the simulated infrastructure and real-world IT and OT devices.
- **Ship Simulator** (upper left, yellow): This simulator replicates the behaviour and position of a vessel by producing realistic sensor data. It is interfaced with a physical rudder twin to reproduce the mechanics and control of the rudder system. This configuration effectively provides a functional model of both bridge systems and rudder control infrastructure. [8]
- **VTT Tools** (left, grey): These tools consolidate cyber incident evidence into a centralised platform for improved situational awareness.
- **Malware Information Sharing Platform (MISP)** (lower left, blue): MISP facilitates the recording and replaying of cyber attacks in a maritime context, enabling reproducible scenario execution.
- **Orchestrator** (centre, blue): Serving as the backbone of the architecture, the orchestrator synchronises all modules and ensures coordinated behaviour across the distributed simulation environment.

An important characteristic of the Cyber-MAR platform lies in its distributed nature. The infrastructure is not centralised in a single physical location, nor does it originate from a single research institution. Instead, it is the result of a collaborative effort involving several leading organisations in the field, including modules contributed by the Cyber-SHIP Lab [50] previously discussed in Section 2.2.1. To enable this level of collaboration, the Cyber-MAR project employs VPN-based connectivity to link cyber range components hosted at separate physical sites. This strategy not only allows for the pooling of computing resources but also supports the sharing of simulation, monitoring, and training functionalities, substantially enhancing scalability and realism. In practice, Cyber-MAR interconnects three physical testbeds, one of which is designed to be mobile. [43]

Some of the architectural principles used for the implementation of the Cyber-MAR project have directly inspired the design decisions of the cyber range developed in the context of this thesis. In Section 5.2, we will present the architecture of the implemented cyber range, which similarly features a dedicated ship simulator, a stand-alone attacker workstation that provide functions close to the ones of a MISP, and a naval cyber infrastructure managed through an orchestrator like the Diateam Cyber-Range.

### 2.2.3. U.S. Navy USS Secure Cyber Testbed

Since 2016, the U.S. Navy has been developing a dedicated virtual naval cyber testbed under the name USS Secure. The primary objective of this initiative is to enhance the cybersecurity posture of naval warships by providing a controlled environment to evaluate system vulnerabilities, conduct structured cyber training, and support certification of operational readiness. [12]

The USS Secure platform is classified as a hybrid cyber range, as it integrates virtual simulations with real maritime hardware components. This hybrid configuration enables operationally realistic testing by capturing the complexity and interconnectivity of modern warship environments. A core application of the range is in conducting red team versus blue team exercises, where offensive (red team) and defensive (blue team) cyber operators simulate real-world cyber conflict scenarios. These exercises are instrumental in both identifying weaknesses and assessing the effectiveness of response strategies under realistic operational stress. [46]

One of the key long-term goals of USS Secure is to provide a standardized platform for cyber certification activities. By virtually modelling entire naval platforms, the range facilitates holistic assessments, ensuring that interconnected systems are tested collectively rather than in isolation. This not only improves cyber resilience but also streamlines future readiness evaluations. [46]

Additionally, USS Secure supports forward-looking risk assessment by enabling vulnerability analysis on ships that have not yet been constructed. This approach allows stakeholders to simulate and validate the integration of systems from multiple vendors without incurring the logistical and financial overhead associated with assembling physical hardware. [45]

### 2.2.4. Maritime and Port Authority of Singapore (MPA) Maritime Testbed of Shipboard Operational Technology (MariOT)

The Maritime Testbed of Shipboard Operational Technology (MariOT) is an industrial-grade cyber-physical platform developed in Singapore to reinforce cybersecurity training and testing capabilities for maritime operational technology (OT) systems. Initiated by the Maritime and Port Authority (MPA) of Singapore, the project addresses growing concerns over the security of critical shipboard OT components. [40]

What distinguishes MariOT is its high degree of fidelity to real-world ship systems. The testbed replicates core shipboard functionalities such as navigation, propulsion, and power management systems, providing an environment that closely mirrors actual vessels. This realism allows for the simulation of cyber threat scenarios directly targeting these OT systems, thereby supporting the development and validation of effective incident response protocols. [39]

By training crews in realistic conditions and exposing them to potential cyberattack vectors, MariOT significantly contributes to enhancing the operational readiness of maritime professionals and the cyber resilience of critical OT infrastructure.

### 2.2.5. Genoa University Maritime cybersecurity Testbed (MaCySTe)

MaCySTe is an open-source project launched by the University of Genoa in 2023, with the aim of developing a virtual maritime testbed that faithfully reproduces the network infrastructure and core cyber-physical components of a classical ship. This maritime cyber range is intended for both the development and evaluation of countermeasures to cyberattacks on shipboard systems. [26]

The final deliverable of the MaCySTe project is made available as a public GitHub repository<sup>1</sup> containing the necessary code to deploy the platform on any recent Linux desktop machine with a minimum of 8 CPU cores, 12 GB of RAM, and 50 GB of available storage. [14]

The default simulation scenario positions the ship at the entry of the Genoa harbour. Several runtime configurations are proposed. The most basic one allows the user to control the ship either manually

---

<sup>1</sup><https://github.com/CRACK-MCR/MaCySTe>



via a control dashboard or through an autopilot. Users can also monitor the steering gear system, view radar data using two different visualizations, and track the vessel's movement on an Electronic Chart Display and Information System (ECDIS). Route waypoints can also be defined on the ECDIS for autopilot navigation. Additionally, the platform provides a visual bridge simulation interface. [26]

More advanced scenarios introduce a Graphical User Interface (GUI) for attackers, in combination with a Command and Control (C&C) server. These scenarios support the execution of cyberattacks targeting specific ship components. For example, attackers can sniff packets to determine the ship's location and inject high-frequency packets to falsify heading data or disrupt radar displays. It should be noted that in these simulations, malware is assumed to be already present on the Inertial Navigation System (INS), simplifying the attack vector to a container-based simulation that excludes delivery mechanisms. [26]

An additional scenario integrates network traffic monitoring capabilities. A Security Information and Event Management (SIEM) container, tailored for maritime operations, can analyse the simulated traffic and raise alerts when potential intrusions are detected.

The cyber range architecture is built around a set of Podman containers interconnected across different Podman networks, reflecting the segmentation of a traditional ship network. A simplified architectural representation from [26] is shown in Figure 2.2 .

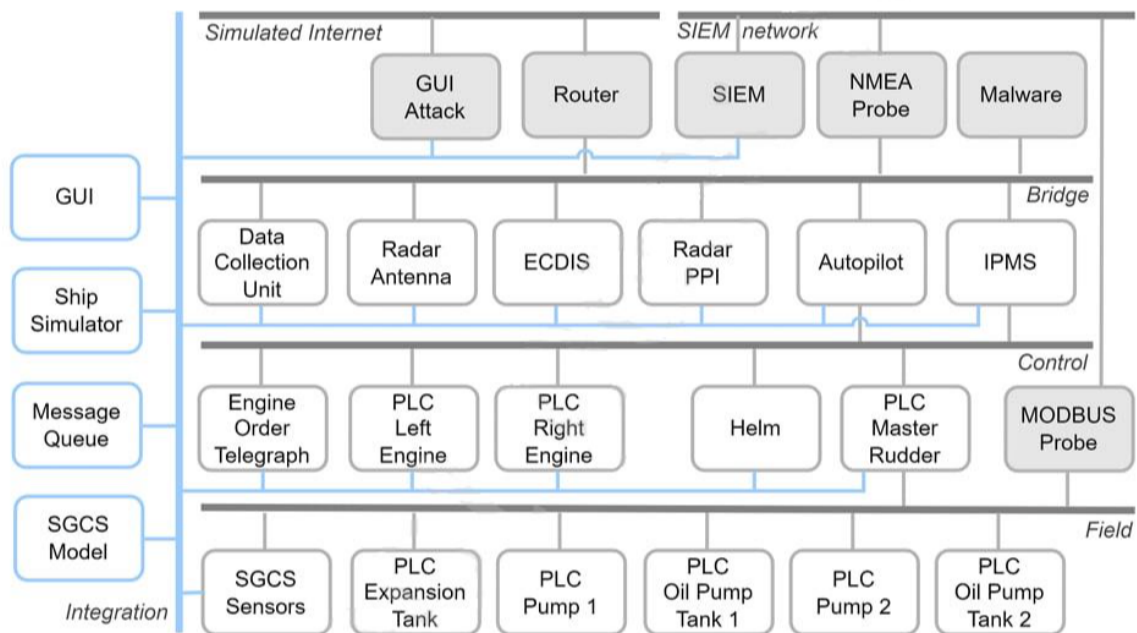


Figure 2.2. MaCySTe testbed containers architecture [26]

The shipboard simulation defines three main network segments:

1. **Bridge network:** The ship's main IT network, connecting to WECDIS and sensors such as radar systems.
2. **Control network:** Used for transmitting control messages to the rudder and engine components.
3. **Field network:** Dedicated to communication with the Steering Gear Control System (SGCS) and its associated Programmable Logic Controllers (PLCs).

Supplementary networks are also established to enable cyber range functionalities such as data injection, system monitoring, and attacker command interfaces.

A key architectural decision in MaCySTe is the inclusion of an **Integration network**, which hosts the core ship simulator. This simulation is based on the open-source Bridge Command project<sup>2</sup>, originally developed for seamanship training including navigation, radar use, and ship handling. [11] Within

<sup>2</sup><https://github.com/bridgecommand/bc>

MaCySTe, Bridge Command has been adapted to serve as a centralized dataset generator. [15] Its outputs, such as position, heading, and system telemetry, are published to a NATS message queue<sup>3</sup>, from which individual containers can subscribe to relevant data streams. This ensures consistency and realism in data exchange among all emulated components. [26]

As the only publicly available open-source maritime cyber range project to date, MaCySTe serves as a foundational framework for the cyber range developed in this thesis. Further details on how MaCySTe is integrated into the present work are provided in Chapter 5.

## **2.3. Cybersecurity Training Methodologies Using Cyber Ranges**

As highlighted in the previous section, numerous maritime cyber range projects have emerged over the past decades in response to the rising cyber threat landscape. This development is far from isolated. On a global scale, similar initiatives are being observed across various sectors where cyber vulnerabilities pose a significant operational risk.

In particular, the growing reliance on digital systems in both civilian and military infrastructures has led to the proliferation of multi-functional cyber ranges. These platforms are widely adopted by armed forces and critical industries to simulate, test, and train personnel in realistic cyber environments. Such training is not limited to cybersecurity specialists, it also includes conventional operators who interact daily with vulnerable digital systems. Through realistic and mission-relevant simulations, cyber ranges help ensure that both technical teams and end-users are better equipped to prevent, detect, and respond to cyber incidents.

This section presents the evolution and current trends in the use of cyber ranges for personnel training, with a particular emphasis on their growing role in cyber awareness. By examining how cyber ranges are leveraged across sectors to develop operational readiness and technical reflexes, we aim to extract best practices applicable to the maritime context. This analysis serves as a foundation for identifying the specific training needs and instructional methodologies best suited for the cyber awareness objectives of the naval cyber range developed in this thesis.

### **2.3.1. U.S. Army Persistent Cyber Training Environment (PCTE)**

One of the leading armed forces in the domain of cybersecurity training is, without any doubt, the U.S. Army. For several years, they have relied on their Persistent Cyber Training Environment (PCTE), a distributed platform specifically designed to train cybersecurity personnel. The PCTE offers realistic, hands-on training through virtualized simulations that replicate real-world cyber environments, allowing operators to build and test skills without exposing actual operational systems to risk.

This environment is particularly critical for the U.S. Navy's Cyber Mission Force teams, who must demonstrate specific capabilities and meet strict performance requirements to be declared at Full Operational Capability (FOC) by the U.S. Cyber Command. The use of the PCTE enables consistent, repeatable, and scalable training scenarios essential for certifying and maintaining mission readiness. [44, 41]

### **2.3.2. Cyber Simulation TRaining for Impacts to Kinetic Environment (CyberSTRIKE)**

More specifically in the context of naval systems, new training methodologies are being explored to enhance training effectiveness and completeness through the use of simulation and virtual environments. A notable initiative in this field is the Cyber Simulation TRaining for Impacts to Kinetic Environment (CyberSTRIKE), which focuses on incorporating realistic cyber effects on shipboard systems during training scenarios. Designed primarily for ship crews, and more specifically for naval commanders, this type of cyberspace training is referred to as "cyber-for-others". The core motivation behind CyberSTRIKE lies in the necessity of integrating the cyberspace domain into the broader operational picture

---

<sup>3</sup><https://nats.io/>

of the modern naval battlespace. Commanders must be prepared to make both offensive and defensive decisions that account for cyberspace operations in order to maintain an information advantage. [23] CyberSTRIKE enables the application of cyber and electronic warfare effects directly onto the simulated shipboard systems used by trainees. These effects may be manually injected by exercise facilitators or arise from battle damage assessments. A key strength of the CyberSTRIKE implementation is its ability to deliver cyber effects without requiring any modification to the simulated naval systems themselves. This is achieved by injecting, modifying, or blocking tactical messages exchanged between the systems and the simulation, thereby simulating the intended cyber impact. [23]

One of CyberSTRIKE's significant improvements over previous cyber-for-others solutions is its provision for trainees to independently detect and identify ongoing cyber attacks against naval systems. Once the cyber threat is identified, the command staff can practice mitigating the effects through decision-making and coordinated response actions. [23]

The cyber effects are also tailored to the experience level of the training audience. Novice trainees are confronted with more obvious manifestations of cyber attacks, while more advanced trainees are challenged with subtler effects that require greater analytical and situational awareness to detect. Each training scenario is accompanied by defined learning goals and suggested appropriate responses for each type of cyber effect. [23]

According to the 2024 CyberSTRIKE publication [23], two cyber effects have already been implemented:

1. Disruption of naval command and control systems, resulting in stale, duplicated (ambiguous), or mis-located tracks.
2. An attack on commercial shipboard identification systems, producing a misleading or inconsistent maritime traffic picture, thus hindering battlespace operations.

Further refinements and expansions of the CyberSTRIKE platform are planned, with ongoing efforts aimed at improving the software design and increasing the library of possible simulated cyber effects on naval systems.

Key principles from the CyberSTRIKE training methodology have been adopted in this thesis's cyber awareness scenario. Notably, trainees are placed in a broader operational context where they must react to cyber effects while maintaining focus on mission objectives. Additionally, scenario complexity is adjusted to match the experience level of the target audience, ensuring relevant and effective training outcomes.

### **2.3.3. European Union Cyber-MAR project**

The maritime cyber range developed in the context of the Cyber-MAR project has already been described in Section 2.2.2. Nevertheless, the global project does not only focus on the design of a cyber range, but also on the research and development of more efficient training methodologies in the field of maritime cybersecurity.

The training provided by Cyber-MAR is intended for two categories of actors: security professionals, to raise their awareness and improve their cyber defence skills, and non-security professionals or the general public (e.g., ship builders, crew members), to train them to face cyber threats without necessarily having the technical background to deal in depth with the issues. To this extent, the Cyber-MAR cyber range provides an environment with dedicated computing infrastructure to execute effective scenarios for all types of trainees. [43]

In order to ensure that the developed training program is easy to share and deploy, standard pilot scenario descriptions and definitions have been established. The training is performed by presenting a scenario with a chosen cyber attack and providing insight into both the attacker and defender sides of the incident. The crew of the port or the ship must then respond to the attack accordingly. A second aim of the project is to estimate the impact of cyber attacks from an economic perspective and to support prompt decision-making related to risk management. [16]

On the official website of the project [27], three distinct scenarios are currently described:

1. A cyber attack scenario featuring a remote access attack on the IT and OT infrastructure of Valencia port authority's electrical grid. The attack begins with a phishing email to gain access to the OT manager's computer. It then cuts off the port's power supply and simulates a ransomware attack targeting all workstations within the port infrastructure.
2. A scenario in which an attack is downloaded and propagated through the IT infrastructure of a ship, ultimately compromising the vessel's control systems to deviate its course. The attack spreads from shore-based systems to onboard control systems.
3. A scenario demonstrating an initial attack on the SCADA system of the port container terminal, resulting in a train collision, followed by a larger attack that wipes out all IT and OT devices on the port's network.

Furthermore, the training of trainees is supported by scoring mechanisms and other means of measuring performance. For cyber-physical training, performance scoring is primarily based on achieving specific objectives, such as successfully changing the vessel's course despite cyber interference. For more cybersecurity-oriented training, performance evaluation is often conducted through analysis of logs generated during the execution of the scenario. [43]

The key takeaway from the Cyber-MAR training methodology lies in the design of their attack scenarios. Rather than isolating single incidents, trainees are exposed to a full cyber attack sequence, from initial compromise to lateral movement and eventual disruption of operational technology. This comprehensive and realistic structure will be adopted in the cyber awareness scenario developed in this thesis, ensuring a coherent simulation of an escalating threat. Although Cyber-MAR also demonstrate the relevance of performance scoring to evaluate responses, this feature will not be implemented in the current version of the project. Nonetheless, Section 8.1 discusses its potential inclusion in future iterations.

## **2.4. Gaps and Opportunities Identified in Current Research**

In the context of the naval cyber range developed in this thesis, a number of gaps and opportunities have been identified based on the research reviewed in the previous sections. These insights will serve as guiding principles for the design and implementation phases of the project. The aim is twofold: to address key shortcomings observed in current naval cyber range solutions, and to capitalise on best practices and innovations found in existing literature and technological approaches. Throughout the remainder of this work, the project will strive to bridge these gaps while leveraging the identified opportunities to deliver a realistic, modular, and extensible naval cyber training platform.

### **2.4.1. Non-existence of Naval Cyber Range Usable by the Belgian Defence**

A key observation emerging from the literature review is the notable absence of the Belgian Defence in initiatives related to naval or maritime cyber ranges, despite its advanced naval capabilities. This is particularly relevant in light of Belgium's forthcoming acquisition of new Mine Countermeasure (MCM) warships, which will integrate a broad array of cutting-edge technologies and interconnected systems.

Additionally, Belgium holds a critical position in global trade through the Port of Antwerp, one of the largest ports in the world and a major logistical and industrial hub for Europe. These strategic assets underscore the urgent need for a cyber-secure maritime and naval infrastructure.

Given this context, the development of a naval cyber range tailored to the specific needs of Belgian naval and maritime systems clearly represents a gap in current capabilities. This thesis seeks to address this gap by designing and implementing a cyber range dedicated to the new Belgian MCM warships, establishing a foundational tool for future training and research within Belgian Defence.

### 2.4.2. Cost of High Quality Maritime Cyber Ranges

As highlighted in Section 2.2, the majority of existing maritime cyber ranges are based on high-end architectures, often involving extensive infrastructure and specialized facilities. These platforms offer advanced simulation fidelity, broad scalability, and operational realism. However, they also come with substantial financial costs. Such projects are typically only feasible through international collaborations or with the support of large organizations such as NATO or the European Union.

This reality underscores the need to explore more accessible alternatives, smaller-scale naval cyber ranges that can be independently deployed by individual nations. While these solutions may not match the comprehensive capabilities of large international platforms, they have the potential to significantly enhance national training efforts and research opportunities in maritime cybersecurity. By providing a foundation for local development and experimentation, these lightweight cyber ranges can serve as vital tools for strengthening cyber resilience in the naval domain.

### 2.4.3. Cyber Ranges Incorporating Hardware Devices

Another notable challenge observed in existing maritime cyber ranges is their reliance on real ship-board hardware components. While the inclusion of physical devices undeniably enhances the realism and fidelity of the testbed, making it suitable for advanced research such as penetration testing and vulnerability assessment, it also significantly increases the complexity of integration. Such setups require extensive configuration efforts and deep technical knowledge, often necessitating close collaboration with equipment vendors.

Moreover, the availability of maritime-specific hardware presents a major limitation. These components are not only costly but also tend to be vendor-specific, with proprietary configurations that limit customization and reusability. In many cases, only the manufacturers themselves possess the necessary expertise to configure and operate these systems effectively.

For these reasons, there is a pressing need to further explore and develop fully simulated naval testbeds. Such platforms, if well-designed, can still support educational and training objectives while providing a robust foundation for cybersecurity research. A simulated approach offers greater flexibility, lower costs, and broader accessibility, qualities that are essential for scalable and sustainable maritime cyber defence development.

### 2.4.4. Converging Architecture in Existing Maritime Cyber Ranges

According to the available literature regarding maritime cyber ranges, a clear trend emerges with respect to the architecture of the simulation environment. This convergence across various initiatives is the result of prior research, extensive testing, and operational feedback. Consequently, it presents a valuable opportunity for the present project: to evaluate and potentially apply a similar architectural structure in the design of the naval cyber range developed in this thesis.

Most of the existing maritime cyber ranges share a set of core architectural components. These typically include:

- A **ship simulator**, responsible for generating coherent and realistic navigation and sensor data that drive the simulated shipboard systems;
- A **virtual network environment**, which emulates the actual network architecture of a vessel, replicating both IT and OT traffic flows;
- A **cyber range control and monitoring module**, enabling observation, attack injection, and scenario management;
- A **platform or orchestration layer**, which hosts and interconnects all the cyber range components in a coherent and scalable framework.

The recurrence of this structure across multiple independent projects underlines its effectiveness and relevance. As such, it provides a strong starting point for the architecture of the naval cyber range proposed in this study.

### 2.4.5. Training Methodologies

Across the literature, there is a clear consensus that the most effective methodology, whether for cybersecurity professionals or general ship personnel, relies on immersive training built around realistic scenarios in which cyber threats emerge dynamically. These scenarios allow trainees not only to respond to technical incidents, but also to maintain operational focus and decision-making under stress. As the educational objectives of this thesis align with those of the referenced projects, a similar structure is adopted in the design of the developed cyber awareness scenario. Based on this and on the insights from existing maritime cyber range projects, particularly Cyber-MAR and CyberSTRIKE, this thesis adopts a scenario-based, hands-on training approach tailored to cyber awareness in a naval context.

Key elements that will be taken into consideration during the development of the training scenario include:

- Exposure to a complete cyber attack sequence, covering compromise, lateral movement, and disruption of operational technology, rather than isolated incidents.
- Integration of cyber threats within a broader mission narrative, requiring trainees to react while maintaining operational objectives.
- Adjustment of scenario complexity to the experience level of the training audience.

While performance scoring is recognised as a promising tool for evaluating training effectiveness, it is not implemented in the current version but is considered for future improvements (cf. Section 8.1).

### 2.4.6. Open-source MaCySTe Project

The MaCySTe project, described in Section 2.2.5, already begins to address several of the previously identified gaps in the field of maritime cyber range development. It delivers a fully simulated maritime testbed capable of generating network traffic that closely mimics real-world shipboard communications. Designed to operate on relatively modest hardware, the solution remains both affordable and accessible, making it a promising starting point for academic and research-oriented applications.

However, MaCySTe is primarily intended for cybersecurity research rather than training and is structured to run on a single machine, thereby restricting its usability to a single user. While it does provide the simulation of various maritime cyber threats, it lacks the foundational infrastructure required to support the execution of cyber awareness training scenarios. Specifically, it does not include essential features such as a management console, predefined attack sequences embedded within guided missions, or isolated virtual machines for the trainees.

In addition, although the current implementation of MaCySTe, based on Podman containers and networks, is lightweight and portable, it already demonstrates a relatively high level of architectural complexity. This complexity can form a bottleneck for future scalability and extension, especially when more advanced functionalities or systems are to be integrated. Moreover, since the entire environment is container-based, integrating certain types of network devices or more heterogeneous system architectures could prove difficult. The lack of a graphical interface for managing and deploying the containers further increases the configuration burden and hinders the creation of more elaborate and dynamic network topologies. Finally, the architecture itself is intentionally generic and does not reflect the specific operational context of naval platforms or warship environments, which is essential for the objectives of this thesis.

Despite these limitations, the open-source nature of the MaCySTe project makes it a valuable repository of simulated shipboard components. Several of these components will be selectively adapted and integrated into the naval cyber range developed in this thesis. The methodology and technical details of this integration are presented in Chapter 5.

### 3. Mine Countermeasure Warship Network Architecture Analysis

The previous chapter reviewed existing maritime cyber range initiatives, highlighting significant gaps in realistic naval training environments and underscoring the necessity for Belgian Defence to contribute to the development of domain-specific platforms. Building upon these observations, the present chapter focuses on the cyber environment of the new Belgian Mine Countermeasure (MCM) warships, with particular attention to the architectural and functional characteristics most relevant to simulation. The objective is to determine the core features of MCM warship networks in order to guide the design of a tailored naval cyber range that faithfully reflects their operational realities.

In the context of this study, the naval cyber range to be designed is expected to serve as a virtual implementation of the new Mine Countermeasure (MCM) warship of the Belgian Navy. To support this objective, a crucial first step is to analyse in detail the actual architecture of the vessel's onboard network. One of the greatest challenges in this process lies in simplifying the ship's highly complex and classified network topology into a usable form. The resulting abstraction must strike a careful balance: sufficiently realistic to enable effective training and research, yet simple enough to ensure efficient implementation and scalability within a simulated cyber range.

To this end, this section first outlines the various sub-networks that constitute the warship's architecture. For each sub-network relevant to simulation, a simplified model is proposed, designed to preserve key functional characteristics while reducing implementation complexity. Subsequently, additional considerations and simplifications related to the virtualisation and emulation of such a system are presented. This process leads to the final definition of the architecture that will be implemented in the naval cyber range developed during this study.

It is important to emphasise that the architectural insights presented in this section are based extensively on internal technical documents provided by the Naval Group, the manufacturer of the ships. These documents are classified as *"restricted distribution"* in the context of this study. As such, no diagrams, schematics, or excerpts from these materials may be reproduced or disclosed in this thesis. Nevertheless, the overview and technical interpretation offered here draw upon the following references: [3, 4, 5, 6, 7].

To give a sense of the effort involved in this simplification task, the content of this section represents a synthesis of more than 1400 pages of technical documentation concerning the Belgian Defence's MCM warships.

#### 3.1. Overview of Warship Information Systems

Modern warships rely on both Information Technology (IT) and Operational Technology (OT) systems to support their missions. IT systems handle data processing, communication, and administrative tasks, enabling functions such as messaging, logging, and command support.

OT systems, by contrast, are responsible for monitoring and controlling physical shipboard operations, including propulsion, navigation, and weapon systems. The term Operational Technology broadly covers SCADA, industrial control systems, and cyber-physical components that directly interact with real-world processes.

The distinction reflects a key difference: IT manages information flow, while OT interfaces with critical hardware. Increasing interconnection between these domains introduces new vulnerabilities, requiring integrated approaches to maritime cybersecurity.

### 3.1.1. Ship Networks Listing

On modern ships in general [35] and thus also on the MCM warships of Belgian Defence, [6] we find the following main networks:

- **Bridge Network:** Manages navigation equipment and lantern/deck light controls.
- **Safety Network:** Supports fire detection, public announcement systems, CCTV security, water-tight doors, and stability systems.
- **Platform/Control Network:** Controls engine operations, power generation and distribution, cargo monitoring, deck equipment, HVAC (Heat, Ventilation & Air Conditioning) systems and hotel services.
- **Administrative Network:** Facilitates voyage planning, ship maintenance management, and administrative tasks.
- **Public Network:** Provides data network access for crew and passengers, primarily for general internet use.

In addition to these common networks, MCM warships also include additional specific networks:

- **Principal Warfare (PW) Network:** Interconnects and hosts the legacy weapon systems.
- **Mine Warfare (MW) Network:** Interconnects and hosts the specialised weapon systems and sensors dedicated to the mine warfare.
- **Four Government Furnished Equipment (GFE) Encrypted Networks :** Provides encrypted communication at different level of classification (National Secret, Coalition Secret, Mission Secret and National Restricted).
- **Red ICS Network:** Delivers Operational communication at classified level.
- **Black ICS Network:** delivers interfaces with all external communications means on-board.

### 3.1.2. Ship Systems Overview

To provide an overview of the onboard technological capabilities of the new MCM warships, Table 3.1 presents a non-exhaustive summary of the systems belonging to the ship's primary networks.

Network	System	Role
Integrated Platform Management System (IPMS)	Propulsion Control	Control of shaft speed from the Ship Control Center (SCC), Bridge, and Dynamic Positioning System (DPS).
	Steering Gear	Operation of two electronically synchronized rudders powered independently.
	Power Management and Distribution	Management of power generation and distribution through redundant Programmable Logic Controllers (PLCs).
	Impressed Current Cathodic Protection (ICCP)	Reduction of hull corrosion and control of the ship's electrical signature.
	Degaussing System	Reduction of magnetic signature via degaussing coils controlled through a Web-based interface.
	Heat, Ventilation and Air Conditioning (HVAC)	Management of ventilation and air conditioning, integrated with fire-fighting and automatic shutdown systems.
	Fire Detection System Network (FDS-Net)	Fire detection and fighting system communicating through a redundant Ethernet network.
Continued on next page		



Network	System	Role
	Fluid Systems	Management of compressed air, JP-5 fuel, sewage, and other fluids via Modbus TCP/IP protocol.
Integrated Bridge Management System (IBMS)	Navigation Sensors	Acquisition of environment data, position, vessel detection, and weather parameters.
	Navigation Systems (WAIS, SRS, SPMS, VDR, INS)	Ship navigation support, proximity management, and voyage data recording.
	Navigation Civil System (NCS)	Predicts environment and positioning, displays navigational information and aids navigation.
	Integrated Navigation System (INS)	Gathers and distributes enhanced navigation and weather data throughout the ship.
	Dynamic Positioning System Level 2 (DPS2)	Automatic ship movement control for route tracking, station keeping (hovering), and joystick maneuvers.
	Masterclock System (MSK)	Distributes synchronized time data across all ship systems.
Principal Warfare (PW)	Multifunction Surveillance Radar (MSR)	Provides multifunction surveillance capability, tracking both air and surface targets.
	Identification Friend or Foe (IFF)	Distinguishes between friendly and hostile targets using electronic interrogation.
	Helo Deck Radar (HDR) — Low Probability of Intercept Radar (LPI)	Ensures radar stealth while monitoring helicopter operations on deck.
	Electro-Optical/Infrared (EO/IR)/Laser Sensor	Provides visual and thermal imaging for surveillance and targeting.
	Small Caliber Gun (SCG)	40mm naval gun used for close-range defense against surface and air threats.
	Gun Computer	Fire control system managing targeting and operation of naval guns.
	Remote Weapon System (RWS)	12.7mm remotely controlled machine gun system for surface threat engagement.
	Mine Avoidance Sonar (MAS)	Detects and assists in navigation around naval mines.
	Radar Status and Control Panel (RSCP)	Interface to monitor and configure the ship's radar systems.
Mine Warfare (MW)	Multi Mission Drone System (SMMD)	Management of multiple unmanned underwater or surface drones for mine warfare operations.
	Unmanned MCM Integrated System Software (UMISOFT)	Software platform integrating unmanned mine countermeasure (MCM) systems.
	Onboard Signature Management System (OSMS)	Reduces ship acoustic, magnetic, and electric signatures to minimize detection risk.
	Video Control Management (VCM)	Video monitoring and management system for operational and mission-critical visual feeds.

**Table 3.1.** MCM Warship Networks and Systems Overview

## 3.2. Network Architecture on MCM Warships

As previously mentioned, the complete network architecture of the MCM warships cannot be fully disclosed within the scope of this study. To nevertheless provide the reader with the essential understanding of the ship's onboard network implementation, the explanations and schematic representations presented in this document will focus solely on the most relevant and illustrative aspects of the architecture. These have been carefully selected to convey the necessary technical insights while ensuring that no proprietary or sensitive information from the manufacturer is compromised.

### 3.2.1. Conceptual Organisation of the Networks

The different networks composing the complete network architecture of the MCM warships have already been introduced in Section 3.1.1. This section aims to describe, in the specific context of the new Belgian MCM warships, the interconnections between these networks and to provide further insights into the internal structure of each major shipboard network.

A central concept in the network architecture of MCM warships is the existence of a backbone referred to as the Mission Management System INFRAstructure (MMS INFRA) Network. As illustrated in Figure 3.1, this core network acts as the primary conduit linking all sub-networks and serves as a filtration bottleneck for inter-subnet communications. The MMS INFRA network hosts critical infrastructure such as main servers, core routers, and principal firewalls. For redundancy purposes, MCM warships are equipped with two physically separated server rooms.

Given the military threat context in which these ships operate, all network components are designed with full redundancy, both in communication paths and in capacity, ensuring continued operability in the event of hardware failure or attack.

The Principal Warfare (PW) and Mine Warfare (MW) networks discussed in Section 3.1.1 are embedded within the MMS INFRA network, as can be seen in Figure 3.1. Despite this integration, they serve distinct operational roles and are structured through dedicated Virtual Local Area Networks (VLANs). The internal mechanisms specific to the PW and MW networks are further detailed in Section 3.2.2.

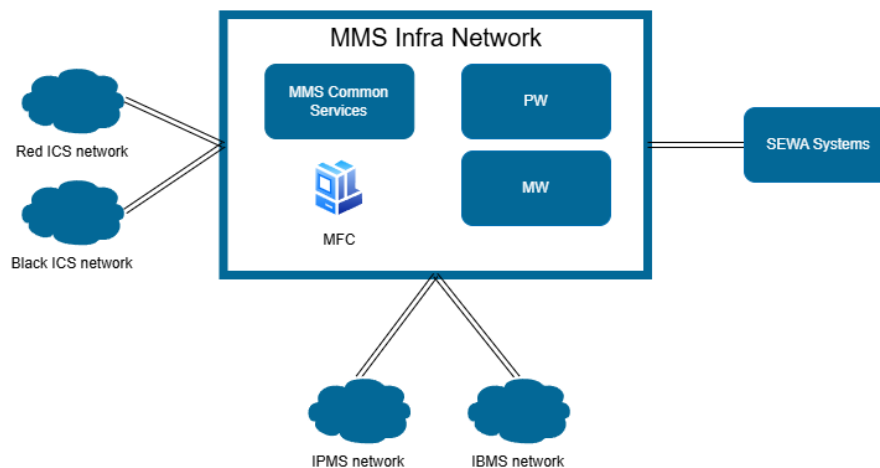


Figure 3.1. MCM warship network architecture overview

Sub-network connections to the MMS INFRA network are implemented either via legacy routers or through specialised gateway devices. Extensive use of VLANs within each sub-network ensures strong and granular segmentation based on communication purpose and system function, thereby reinforcing both operational clarity and cybersecurity.

Another core architectural principle is the centralisation of application hosting. Most applications do not run directly on end-user devices but are hosted on Virtual Machines (VMs) located in the server

rooms. Role-Based Access Control (RBAC) is enforced through Microsoft Active Directory, whereby users and computer accounts are grouped by operational function. These group memberships define "App Permissions", which are subsequently translated by each application into specific access rights and roles.

Consequently, end-user terminals, referred to as Multi-Function Consoles (MFC) or Multi-Function Displays (MFD), are not tied to specific roles or software. Any user can access their required tools from any terminal, provided the appropriate permissions are in place. This architecture offers both operational flexibility and robust disaster recovery: in the event of a VM failure, techniques such as load balancing, VM migration, or snapshot restoration can be employed to maintain mission continuity.

### 3.2.2. Mission Management System INFRAstructure (MMS Infra) Network

As mentioned earlier, the MMS INFRA network acts as the backbone interconnecting all major sub-networks of the ship. In addition to this central role, it also hosts a wide range of critical IT systems, including servers, storage units, firewalls, and network infrastructure components.

Figure 3.2 presents a simplified representation of the MMS INFRA network architecture. This diagram abstracts away redundancy mechanisms and groups similar subsystems for clarity. For instance, the various sensors and weapon systems listed in Table 3.1 are collectively represented as a single entity labelled "SEWA systems" (Sensor Weapon Systems). Additionally, elements not directly relevant to cybersecurity or to the training objectives of this study have been omitted.

As shown in Figure 3.2, the central networking component is the Inter-VLAN Supercore Router, which connects the main MMS INFRA infrastructure to a DeMilitarized Zone (DMZ). Two firewalls reinforce network segmentation and traffic inspection: the Inter-VLAN Firewall for intra-MMS traffic, and the Interco Firewall for regulating communications between MMS and external or peripheral networks.

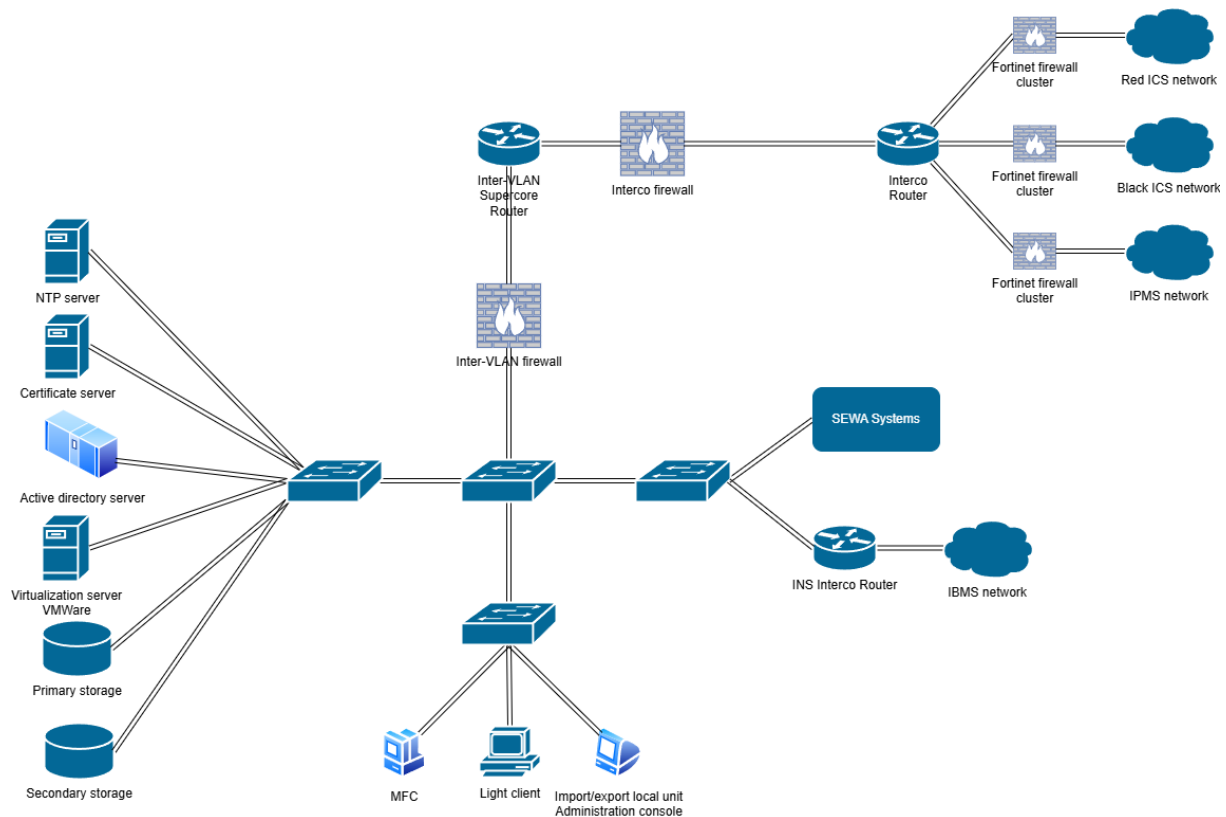


Figure 3.2. MCM warship MMS INFRA network architecture

Following the principles of the real MCM warship network design, the simplified architecture shown in Figure 3.2 enforces the following traffic flow rules:

1. All communications between the Black ICS, Red ICS, and IPMS networks must pass through the Interco Router and are filtered by the Inter-system Fortinet Cluster of Firewalls.
2. Communications between separate VLANs within the MMS INFRA network, such as between SEWA systems and inter-MMS hosting components, are routed through the Inter-VLAN Super-core Router and filtered by the Inter-VLAN Firewall.
3. Internal VLAN traffic within individual sub-networks such as the IPMS IT, Black ICS, Red ICS, and IBMS networks is managed according to the specific security and operational requirements of each sub-network.

## **MMS INFRA Hosted Common Services Systems**

The MMS INFRA network hosts a number of Common Services that are essential for the correct operation of other shipboard systems. While these services will not be described in full detail, their presence is acknowledged here due to their relevance in supporting functionalities of other subsystems discussed later in this document.

The Common Services include the following technologies:

- Active Directory: as explained above, this solution provides Role-Based Access Control of users to many onboard systems.
- Single Sign-On (SSO) authentication: is used in combination with Active Directory in order to provide automatic mutual authentication between MFC and servers.
- Internal Public Key Infrastructure (PKI): generates and manages certificate lifecycle onboard.
- Import/Export Local Unit: ensures data traceability, manages the lifecycle of data in transit, and controls the integrity and safety of data originating from removable media.
- Network Time Protocol (NTP) servers: synchronizes the clocks of devices across the network to ensure accurate and consistent timekeeping for coordinated operations, logging, and security.

## **Storage**

The data storage capabilities of the MCM warship are fully integrated within the MMS INFRA network. Storage infrastructure is organized into two categories: primary storage, offering high-performance capabilities for mission-critical applications, and secondary storage, designed to provide large-capacity data retention. For both categories, an instance is deployed in each of the ship's two server rooms. This architecture ensures system-wide redundancy, data persistence, and synchronous replication between storage instances, thereby enhancing fault tolerance and operational continuity in the event of component failure.

## **MMS INFRA Hosted PW/MW Systems**

The MMS INFRA network hosts the systems associated with the Principal Warfare (PW) and Mine Warfare (MW) functions. To maintain a segmented architecture that minimizes single points of vulnerability while ensuring high service availability during onboard operations, the MMS INFRA network employs a comprehensive VLAN-based segmentation strategy. This segmentation is applied not only at the network level but also extends to servers, virtual machines, and storage components.

A demilitarized zone (DMZ) principle is applied to all communications involving Sensor and Weapon (SEWA) systems to isolate each SEWA device from the internal VLANs of the MMS network. This isolation ensures that only predefined control commands, authorized in the applicable Interface Control Documents (ICD), are permitted between PW software or virtual machines and their respective SEWA systems.

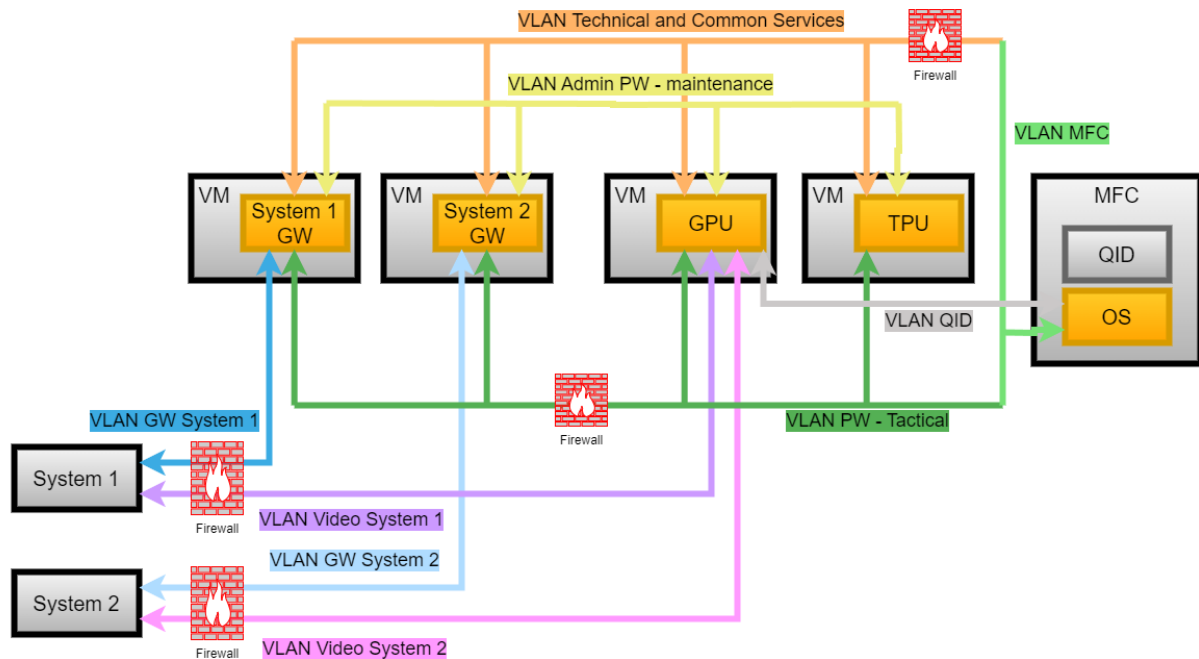


Figure 3.3. MCM warship MMS INFRA VLANs

Figure 3.3 illustrates a simplified VLAN configuration for SEWA systems. The architecture comprises four key components: SEWA systems (e.g., System 1 and System 2), dedicated Gateway (GW) virtual machines, PW/MW VMs equipped with Graphical Processing Units (GPU) or Tactical Processing Units (TPU), and Multi-Function Consoles<sup>1</sup> (MFC).

In this setup, the end-user interacts with the system via the MFC, communicating with PW/MW VMs through the VLAN MFC. These VMs, when issuing command-and-control messages to a SEWA system, transmit them through VLAN Tactic to the associated gateway in the DMZ. Traffic is first filtered by the MMS firewall. Each gateway VM has exclusive access to the VLAN associated with its target SEWA system (e.g., VLAN GW System 1, VLAN GW System 2). The gateway validates the messages at the application layer (Layer 7) against the corresponding ICD. Upon successful validation, the messages pass through the MMS firewall once again and are routed to the target SEWA system.

As also depicted in Figure 3.3, raw video flows utilize dedicated VLANs per SEWA system. These flows, being less critical, bypass Layer 7 inspection and are only filtered at Layer 4 using the MMS firewall, ensuring efficient data transmission while preserving security constraints.

### 3.2.3. Integrated Platform Management System (IPMS) Network

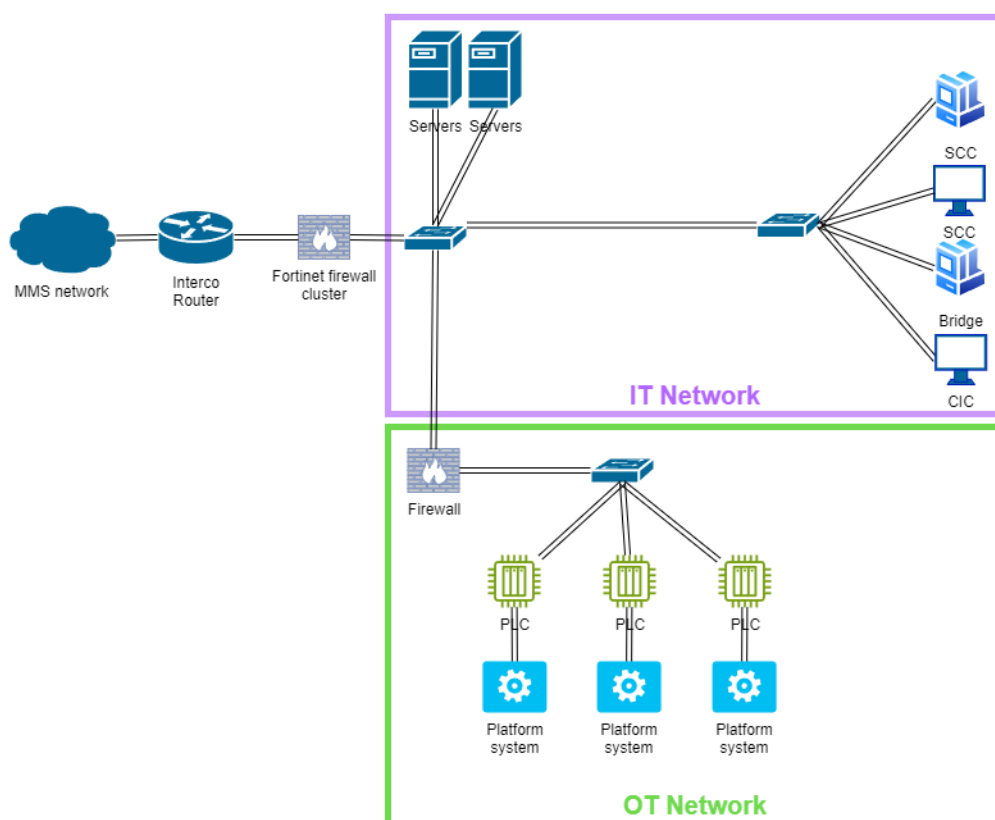
The IPMS (Integrated Platform Management System) sub-network is responsible for the monitoring, command and control of all physical capabilities of the warship, including propulsion, rudder steering, and associated subsystems. This sub-network is connected to the MMS INFRA network through the Interco Router.

The IPMS sub-network is further divided into two distinct physical partitions:

- An **IT partition** for supervision tasks and server-related components.
- An **OT partition** for automation and control system functions.

As with the MMS INFRA network, strict segmentation is applied between IT and OT components. Additionally, multiple VLANs are defined to isolate and manage the various functional areas within each partition.

<sup>1</sup>Multi-Function Consoles run their own Operating System (OS) and are equipped with a Quick Input Device (QID).



**Figure 3.4.** MCM warship IPMS sub-network architecture

### IT IPMS sub-network

As shown in Figure 3.4, the IT IPMS sub-network provides connectivity to devices located in the Ship Control Center (SCC), the Combat Information Center (CIC), and on the Bridge.

Normal control and monitoring operations are conducted from two dedicated SCC workstations and one workstation located on the Bridge. Additionally, two Electronic Information Boards (EIBs), one positioned in the SCC and the other in the CIC, are responsible for displaying the Battle Damage Control System (BDCS).

As further illustrated in Figure 3.4, the server room hosts multiple servers connected to the IT IPMS network to provide the following core functionalities:

- Auxiliary System and Mobility
- Security System and Electrical System
- Remote Diagnostic Capabilities
- Storage
- Virtualisation Services (hosting VMs for Multi-Function Console access)

### OT IPMS sub-network

The OT IPMS sub-network connects the ship's Programmable Logic Controllers (PLCs) to their respective physical systems for monitoring and control. As illustrated in Figure 3.4, these PLCs interface directly with platform systems across the vessel.

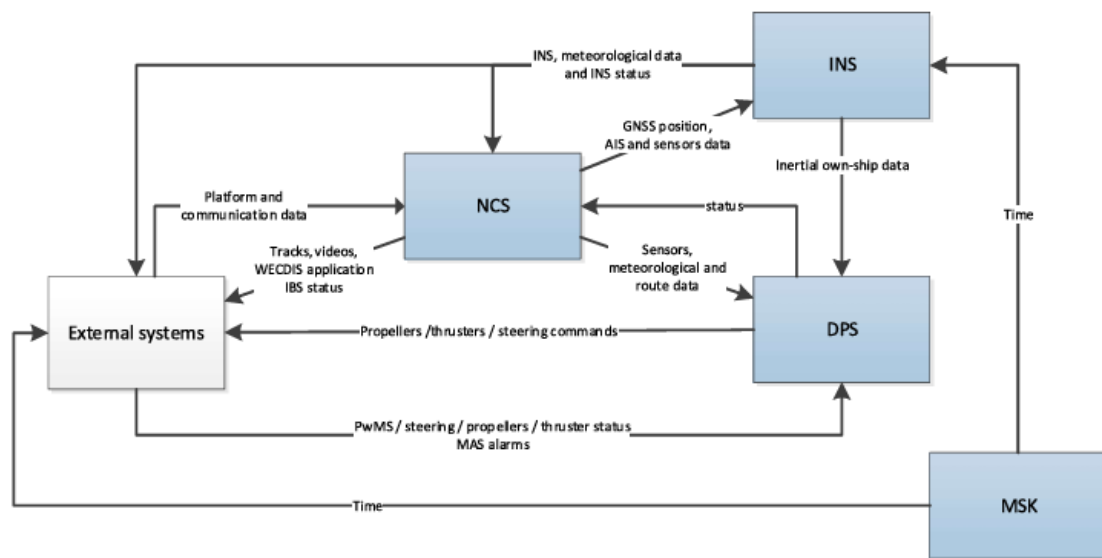
To organize and secure communications, the OT network applies a dedicated VLAN for each primary PLC domain: Auxiliary, Security, Electrical, and Propulsion. This segmentation enhances reliability and facilitates fault isolation.

### 3.2.4. Integrated Bridge Management System (IBMS) Network

The Integrated Bridge Management System (IBMS) is composed of four interconnected subsystems, each fulfilling a specific role to support safe and effective vessel navigation and control:

1. **Navigation Civil System (NCS):** Provides all required navigation sensors for safe operation, as well as distribution systems and onboard displays for navigation and weather data.
2. **Inertial Navigation System (INS):** Delivers accurate and continuous navigation and weather information.
3. **Dynamic Positioning System (DPS2):** Integrates an autopilot that uses IBMS sensor data to follow pre-set routes (e.g., in the WECDIS) or avoid mine locations communicated by the MAS. It directly controls the electrical propulsion, rudders, and thrusters, and supports multiple modes including track following, heading keeping, course following, hover keeping, joystick mode, and auto track.
4. **Masterclock System (MSK):** Distributes time data and ensures synchronization across onboard systems, including all NTP servers on the MMS INFRA network.

Although each sub-system serves a distinct function, they are highly interconnected to meet the IBMS's integrated operational objectives. An overview of the functional information flow between the subsystems and with external components is illustrated in Figure 3.5.



**Figure 3.5.** Functional information flow summary for IBMS network

As the IBMS is responsible for aggregating and processing navigation sensor data, it includes numerous sensors ranging from standard civil devices to highly specialized military-grade systems. A non-exhaustive list of these components is available in Table A.1 of Appendix A.1.

The actual network topology of the IBMS is complex, with many direct inter-system links beyond standard network paths. To maintain clarity and simplicity in the simulation model, direct physical links are omitted in the network diagram, and all systems are instead represented within a single flat network structure. The simplified architecture of the IBMS network, incorporating all four subsystems, is shown in Figure 3.6. For brevity, the various sensor devices are collectively labelled as "Sensors" in the diagram.

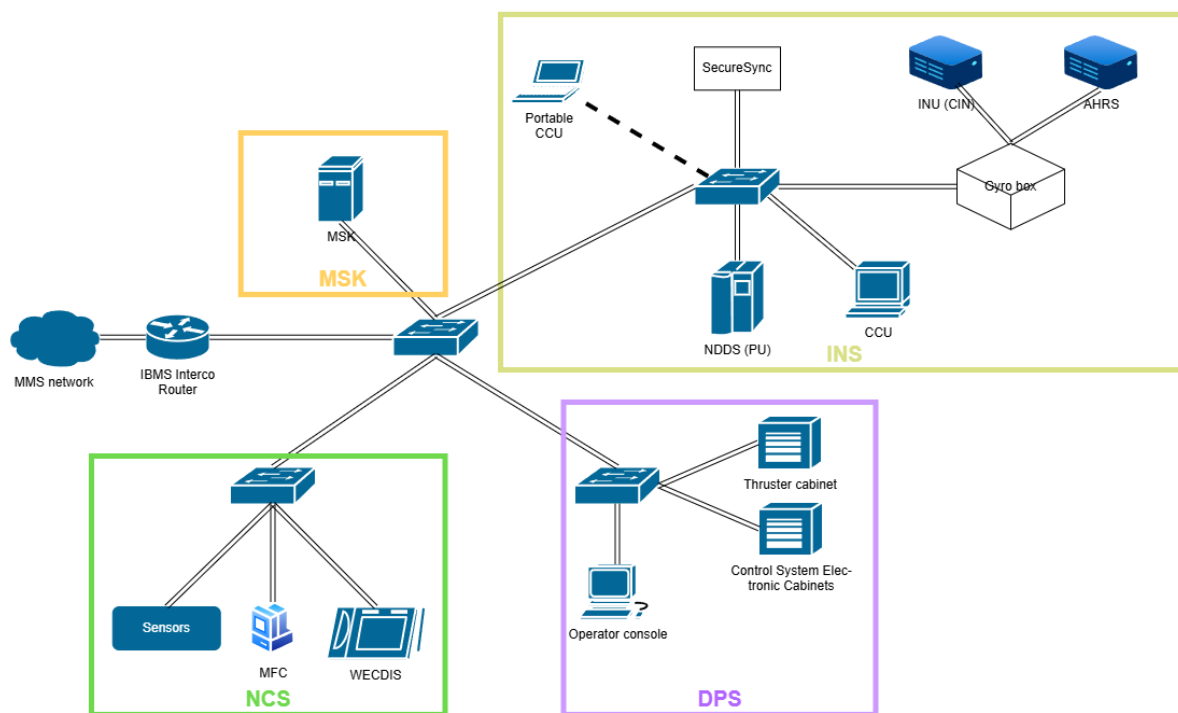


Figure 3.6. MCM warship IBMS sub-network architecture

### 3.2.5. Integrated Communication Sub-System (ICS) Network

The Integrated Communication Sub-system (ICS) is a multipart assembly comprising various communication components and services. It is structured into two main categories: the COMOPS (Operational Communication) and Internal and Regulatory Communications. COMOPS is based on the TactiCall ICS, offering a comprehensive solution for both internal and external communications aboard the vessel. The Internal and Regulatory Communications handle functions such as entertainment, SPT (Sound Powered Telephone), PA (Public Address), and GMDSS (Global Maritime Distress and Safety System). Even if some of its functions interface with COMOPS, the Internal and Regulatory subsystem is not relevant from a cybersecurity perspective and is therefore excluded from the scope of this study.

The ICS is logically segmented into two networks:

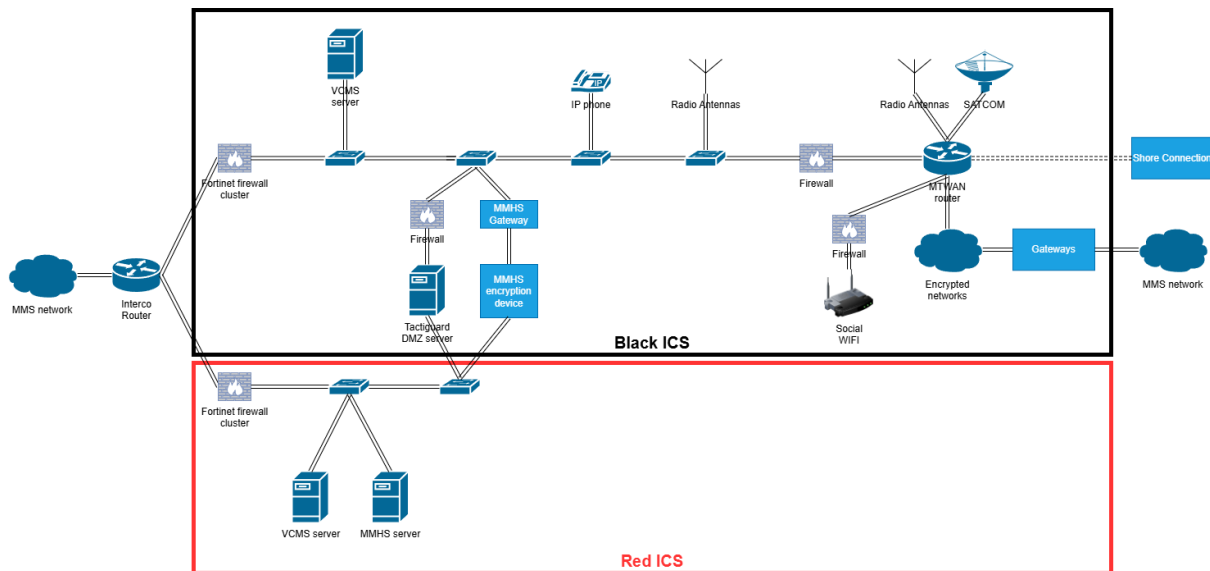
- **Black ICS Network:** handles common military communication;
- **Red ICS Network:** manages classified (National Secret) military communications.

Figure 3.7 presents a simplified architecture of the ICS with its Red and Black sub-networks.

The main capabilities of the ICS include Voice Communications, Communication Management, Data Transmission, Radio Frequency Bearers, and Support Systems. Core components supporting voice communications are the TactiCall servers, voice terminals, and the TactiCall Management Terminal, referred to as the Voice Control and Monitoring System (VCMS).

As shown in Figure 3.7, each sub-network (Black and Red) includes its own VCMS servers. The VCMS is the primary communication system management tool: it configures users, controls access rights, and monitors subsystem health. It also relays a synthetic communication system status overview to the Principal Warfare suite, and enables remote configuration of radios, telephone permissions, and contact directories.





**Figure 3.7.** MCM warship ICS sub-networks architecture

External voice communication is supported through several interfaces, including Mobile Telephony, Satellite Communication (SATCOM), and direct port-based shore links. Tactical and data communications are handled via secure radio systems.

An essential security element of the ICS architecture is the Tactiguard server, which serves as a secure gateway between the Black and Red ICS networks. This component ensures that classified information remains protected, with encrypted channels enforced when transmitting such data externally.

For Military Message Handling System (MMHS) communications, the ICS includes dedicated servers, decryption devices, and MMHS gateways. These elements filter, encrypt, and decrypt classified messages, which are then transmitted over external channels such as SATCOM or radio.

Also illustrated in Figure 3.7 is the Multi-Tactical Wide Area Network (MTWAN) router. This device serves as a critical bridge between internal communication networks (e.g., Black ICS, encrypted channels) and external tactical communication systems (e.g., radios, satellite terminals).

For highly classified transmissions, isolated encrypted networks are used in conjunction with Government Furnished Equipment (GFE) gateways to interface with the MMS INFRA network.

Finally, social internet access for non-military communication is routed directly through the MTWAN, bypassing the secured ICS infrastructure.

### 3.3. Simplification Choices for Simulation Purposes

The simplified network architectures presented in Sections 3.2.2, 3.2.3, 3.2.4, and 3.2.5 already represent a significant abstraction from the real-world network topologies of the Belgian MCM warships. However, to ensure a lightweight, scalable, and implementable first version of the naval cyber range, further simplifications are necessary. These adjustments aim to retain the essential operational features and architectural logic of the ship's digital systems while reducing technical overhead and deployment complexity.

The simplification process focuses specifically on retaining elements unique to naval systems and discarding or abstracting more generic IT infrastructure that, while important in full-scale deployment, are not central to the pedagogical or experimental objectives of this project. This naval-specific focus ensures that the cyber range remains extensible: common IT services can be reintroduced later based on the simplified templates and topologies already defined.

The following simplifications will be applied throughout the remaining design and implementation phases of the naval cyber range:

1. **Firewalls are not considered:** Network segmentation and filtering logic are assumed but not technically enforced in the simulation.
2. **VLANs are not implemented:** Inter-VLAN routing and associated rules are abstracted to simplify network design.
3. **Multi-Function Consoles (MFCs)** are replaced by standard Linux desktop machines, providing similar interaction capabilities through generic interfaces.
4. **Common MMS INFRA services** not specific to naval architecture (e.g., Active Directory, print services, software deployment tools) are omitted.
5. **Sensor and weapon systems (SEWA)** are partially represented: radar capabilities are implemented as a representative example for these components.
6. **The Masterclock (MSK)** subsystem for time synchronization is not considered in the initial prototype.
7. **Encrypted communications** are excluded from the simulation; all communication is assumed to occur over trusted channels.
8. **The Military Message Handling System (MMHS)** is omitted, as it is specific to classified operational workflows.
9. **External communication through the Black ICS network** is simplified into a standard public internet connection for testing and demonstration purposes.

These simplifications strike a balance between realism and feasibility, enabling the construction of a functional, modular, and extensible naval cyber range that remains closely aligned with the core characteristics of real-world MCM warship networks.

### 3.4. Relevant Devices and Corresponding Communication Protocols

By applying the simplifications listed in Section 3.3 to the simplified MCM warship network architecture developed in Section 3.2, the systems to be implemented, along with their main communication protocols, are summarized in Table 3.2.

Network	System	Protocol
MMS INFRA Network	Virtualisation server	TCP
	Radar	Standard ASTERIX category 240, Proprietary Navico BR24
	Radar GUI webserver	Standard ASTERIX category 240, Proprietary Navico BR24, TCP
IPMS Network	PLCs for thruster	Modbus
	Thruster controller	TCP, Modbus
	PLCs for rudder (steering gear system)	Modbus
	Rudder controller	TCP, Modbus
	Control panel GUI webserver	TCP
IBMS Network	INS data generator	NMEA 0183
	WECDIS	NMEA 0183, TCP
	Autopilot	NMEA 0183, TCP

**Table 3.2.** Sub-Network Systems and Protocols to implement

It is noteworthy that the majority of the selected systems rely on maritime-specific communication protocols. Among the most prominent:

- **NMEA 0183** is one of the most widely adopted standards for data communication between marine electronics and navigation instruments. It is developed and maintained by the National Marine Electronics Association and shares a functional lineage with NMEA 2000. [29, 34]
- **Navico BR24** is a proprietary protocol used in Navico Broadband radars. Although not officially documented, several reverse-engineered implementations are publicly available. [17]
- **ASTERIX** (All Purpose Structured Eurocontrol Surveillance Information Exchange)<sup>2</sup> is widely regarded as a universal standard for the exchange of surveillance data. It is commonly used for radar and sensor communications across civil and military domains. [19]

The reliance on these maritime communication standards ensures that the developed naval cyber range reflects realistic operational behaviours, further strengthening its suitability for both training and research in maritime cybersecurity.

### 3.5. Requirements for a Realistic Yet Feasible Simulation

Designing a simulation of a warship's digital environment requires a careful balance between operational realism and implementation feasibility. The following requirements were identified to ensure that the simulation remains both technically achievable and representative of real-world naval systems:

- **System Representativeness:** The simulation must emulate key shipboard domains, such as navigation, platform control, and communication, by modelling representative systems that reflect actual behaviours and interdependencies.
- **Network Accuracy:** The topology should mirror the segmented structure of naval networks, including distinct IT and OT zones, while abstracting sensitive or classified design elements.
- **Protocol Fidelity:** Communication between systems must incorporate protocols commonly used in maritime platforms (e.g., NMEA, Modbus, TCP/IP) to ensure realistic data exchanges.
- **Traffic Realism:** Simulated traffic should reflect typical operational flows, with deterministic patterns and scheduled communications characteristic of embedded ship systems.
- **Threat Scenario Integration:** The platform must support the injection and monitoring of scripted cyber incidents to facilitate scenario-based awareness and response training.
- **Modularity and Scalability:** The architecture should enable flexible system substitution and future expansion, supporting research evolution and hardware limitations.
- **Resource Efficiency:** The environment must be executable on limited hardware, requiring lightweight system emulations and selective abstraction.
- **Security and Compliance:** No classified, proprietary, or cryptographic components may be used. All elements must be based on open standards or safe approximations.

These requirements guided the selection of tools, modeling strategies, and implementation choices throughout the project, ensuring the simulation remains both credible and usable within academic and defense-oriented research contexts.

---

<sup>2</sup>ASTERIX: All Purpose Structured Eurocontrol Surveillance Information Exchange



## 4. Design and Framework Selection

Now that a clear network topology to simulate has been developed in Chapter 3, it is necessary, prior to implementation, to select a simulation framework that best aligns with the constraints and requirements of the naval cyber range to be developed.

This chapter begins with a discussion comparing the use of locally owned hardware versus cloud-based infrastructure as the foundational platform for the cyber range. Following this analysis, the essential features and simulation capabilities required from the chosen framework are outlined in accordance with the goals of the project. Finally, the most suitable framework is identified, and its functionalities and deployment within the project context are described further.

### 4.1. Design Goals and Constraints

Taking into account the research question defined in Section 1.2, the systems identified for implementation in Section 3.4, and the constraints imposed by the available research budget and technical resources, a number of requirements and limitations can be formulated to guide the selection of a suitable cyber range framework.

These considerations cover four key domains: the hardware resources required for the project, the feasibility and implications of using cloud-based solutions, the essential features that the selected framework must support, and the specific needs related to the simulation of shipboard systems within the virtual environment.

#### 4.1.1. Available Resources

For the purpose of this research, a dedicated server has been made available to host the naval cyber range. This hardware establishes the upper bound of available computational resources for the design and deployment of the cyber range, without the need to rely on external cloud-based solutions (an alternative further discussed in Section 4.1.2).

The technical specifications of the available server are as follows:

- **Model:** Dell Inc. Precision 5820 Tower X-Series
- **Processor:** 24 CPUs – Intel(R) Core(TM) i9-10920X CPU @ 3.50GHz
- **Memory:** 128 GB RAM
- **Storage:** 10 TB

#### 4.1.2. Possibility of a Cloud Solution

Nowadays, many practical solutions no longer rely exclusively on owned hardware. Instead, they leverage Infrastructure as a Service (IaaS) or other cloud services to benefit from enhanced scalability, easier maintenance, and potential global accessibility. Table B.1 in Appendix B.1 provides a comparative summary of the advantages and disadvantages between cloud-based and owned hardware solutions. The appendix also includes a discussion evaluating the relevance of each factor in the context of this specific project. To ensure completeness, the comparison is conducted for both the development and production phases, since the cyber range is currently under development but intended for continued use in research and training.

Before drawing conclusions regarding the adoption of a cloud-based solution, it is instructive to assess the pricing of a cloud service offering resources equivalent to the available physical hardware presented in Section 4.1.1. A review of various providers shows that prices range from approximately 240€ per month for 32 vCPU and 64 GB RAM on LifeinCloud<sup>1</sup> to over \$1000 per month for a comparable configuration on AWS<sup>2</sup>. This price evaluation clearly demonstrates that cloud services offering similar resource capacity to the available hardware represent a significant ongoing cost. Therefore, any move to a cloud-based solution would require strong justification based on substantial added benefits.

In conclusion, as detailed in Appendix B.1, the most viable and cost-effective approach for the current development phase is to use the provided owned hardware. This strategy will involve configuring the base infrastructure, installing a VPN for remote access, and implementing reliable snapshot and backup mechanisms. Should the project later transition into production use for routine training, the potential adoption of a cloud-based deployment should be re-evaluated based on its maturity and evolving operational requirements.

### 4.1.3. Framework Required Features

Taking into account the research question, the final goal of the research, lessons learned from similar existing projects in the literature and the available hardware, the selected framework must meet the following essential requirements to support the design, deployment, and management of cyber range scenarios:

1. **Ease of Deployment and Maintenance:** The platform should allow quick installation and straightforward maintenance procedures.
2. **Remote Access Support:** Users must be able to connect to the cyber range remotely.
3. **Scalability:** The framework must support the future extension of computing and networking resources.
4. **Exportability:** The project should be exportable in a lightweight and portable format.
5. **Cost-Effective Licensing:** Preferably open-source or free, or available with a low-cost license suitable for academic or development use.
6. **Realistic Access Model:** Users must interact with virtual machines as though they were physical devices, including terminal and graphical access.
7. **Custom Machine Images:** The platform must allow importing and running custom virtual machine images.
8. **Network and Device Simulation:** It should include features to simulate complex network topologies and network devices (e.g., routers, switches).
9. **Graphical Interface:** A GUI should be available for management and administration of the project.
10. **Snapshot and Rollback:** Ability to save and restore virtual machine states to support scenario reset and iteration.
11. **Multi-User Support:** Support for isolated environments per user or team for concurrent scenario execution.

---

<sup>1</sup><https://lifeincloud.com/pricing/>

<sup>2</sup><https://aws.amazon.com/ec2/pricing/on-demand/>

#### 4.1.4. Simulation Needs

Taking into account the research question, the final goal of the research, lessons learned from similar existing projects in the literature and the available hardware, the cyber range scenarios executed within the framework must support the following simulation features:

1. **Configurable Networking:** Full control over the network configuration of each virtual machine.
2. **Custom Resource Allocation:** Ability to define CPU, RAM, and storage resources per machine based on scenario needs.
3. **Graphical User Interface Access:** Support for GUI environments when required.
4. **Support for Monitoring Tools:** Integration or compatibility with traffic analysers, IDS/IPS, and logging solutions.

#### 4.2. Selected Frameworks and Technologies: Justification and Integration

Following the extensive comparison of available frameworks provided in Appendix B.2, **EVE-NG** (Emulated Virtual Environment – Next Generation) has been selected as the most suitable platform for this project. This choice is based on EVE-NG's ability to strike an effective balance between realism, scalability, and resource efficiency, three essential criteria for building a naval cyber range within constrained technical and operational conditions.

Unlike other available solutions, EVE-NG offers accurate emulation of detailed network behaviours, which is critical for creating a convincing and operationally relevant naval cybersecurity training environment. Its modular architecture also enables the integration of future technologies and scenarios, supporting the long-term adaptability of the platform.

In addition to these strategic advantages, EVE-NG fulfils several practical requirements that further justify its selection:

1. It combines virtual machine and network device emulation within a unified and intuitive graphical interface.
2. It supports custom images, remote access, and realistic Layer 2/3 networking, aligning well with the framework feature requirements and simulation needs formulated in Sections 4.1.3 and 4.1.4.
3. It enables easy exportation, scenario maintenance, and horizontal scalability, while being freely available through its Community Edition.
4. It is distributed as a full operating system solution, simplifying installation and deployment on a single hardware host.
5. For potential future extensions, EVE-NG includes built-in clustering capabilities that allow deployment across multiple physical machines.

Taken together, these features, combined with lower resource requirements and an accessible user interface, position EVE-NG as the optimal technological foundation for the naval cyber range developed in this thesis.

Aside from the Community Edition, EVE-NG Pro Edition offers additional features like multi-user support, project folders, advanced node settings, nodes snapshots, etc. However, since the project is currently in the early development phase with only one main user and the possibility to perform manual backup of the files, the Community Edition already meets all required capabilities and avoids unnecessary upfront costs. In case of additional functionality in the future, the Pro license upgrade (150€ without VAT) is a simple download-based process requiring no full reinstallation.





## 5. Implementation of the Naval Cyber Range

Building upon the network topology simplification presented in Chapter 3 and the framework analysis and selection discussed in Chapter 4, this chapter details the practical implementation of the naval cyber range.

The first part of the chapter describes the deployment of the simplified Mine Countermeasure (MCM) warship network architecture within the EVE-NG framework. It covers the virtual infrastructure layout, the network configuration, the implementation of necessary services and the configuration of virtual machines.

Following this, the chapter outlines the mechanisms used to emulate ship behaviour and generate coherent data streams. This includes coherent ship data generation and real-time distribution across the simulated environment.

The implemented solution to simulate all shipboard systems and their interconnection is then presented. The structure of the project files is detailed, the key components and services required for execution are summarised, and the graphical user interfaces (GUIs) available for ship interaction are introduced.

Finally, the chapter presents the implementation of cyber threats within the simulated environment, detailing how attack vectors are introduced and how training scenarios are structured for cyber awareness exercises. This includes the orchestration of multi-step attack chains, the integration of monitoring tools, and the expected training response.

This implementation marks the transformation of design concepts into a functional naval cyber range tailored for both training and research in maritime cybersecurity.

### 5.1. Network Topology Setup

#### 5.1.1. EVE-NG Installation

The first step in building a simulated network for the cyber range is the installation and configuration of the selected framework. As discussed in Section 4.1.2, the framework is deployed on a dedicated server made available for this research, with hardware characteristics detailed in Section 4.1.1. This server is connected to the Internet via an Ethernet interface.

The EVE-NG installation process is well documented in the official EVE-NG manual [18]. Several installation options are offered depending on the deployment environment, including VMware Workstation or Player, VMware ESXi, Google Cloud Platform, or bare-metal (BM) installations. Given the availability of a dedicated hardware server for this project and to eliminate the overhead of additional virtualization layers, the bare-metal installation method has been selected.

For this installation method, EVE-NG is provided as a complete operating system image in ISO format. The process is similar to that of a typical Linux server installation and is detailed in Section 3.3.1 of the EVE-NG documentation [18].

Following the installation of the operating system, a VPN is configured on the server to enable secure remote access from external networks. This setup ensures that the cyber range can be accessed and administered remotely while maintaining network isolation and security, as outlined previously in Section 4.1.2.

### 5.1.2. Images Installation

In the default configuration, EVE-NG does not include virtual machine or network device images. Users are required to manually upload the images of the systems they wish to utilize within their EVE-NG labs. For the implementation of the naval cyber range, Ubuntu-based virtual machines have been selected due to their open-source nature, broad community support, and lightweight footprint, qualities that make them particularly suitable for scalable simulation environments.

For the simulation of networking infrastructure, Cisco IOL (IOS on Linux) devices have been adopted. These devices emulate Cisco IOS running on a Linux-based kernel, providing the functionality of traditional Cisco hardware routers and switches while maintaining compatibility within the EVE-NG framework.

The complete list of required images for the naval cyber range, along with the installation procedure, is provided in Appendix C.1.

### 5.1.3. MCM Warship Network Architecture Implementation

#### Design Choice: Hybrid Use of Virtual Machines and Containers

The core strategy adopted for implementing the simulated warship network relies on a hybrid approach that combines virtual machines provided by EVE-NG with lightweight containers managed by Podman. This methodology offers a significant reduction in resource consumption compared to a full virtualization model, while preserving a high degree of realism in system behaviour and network interaction.

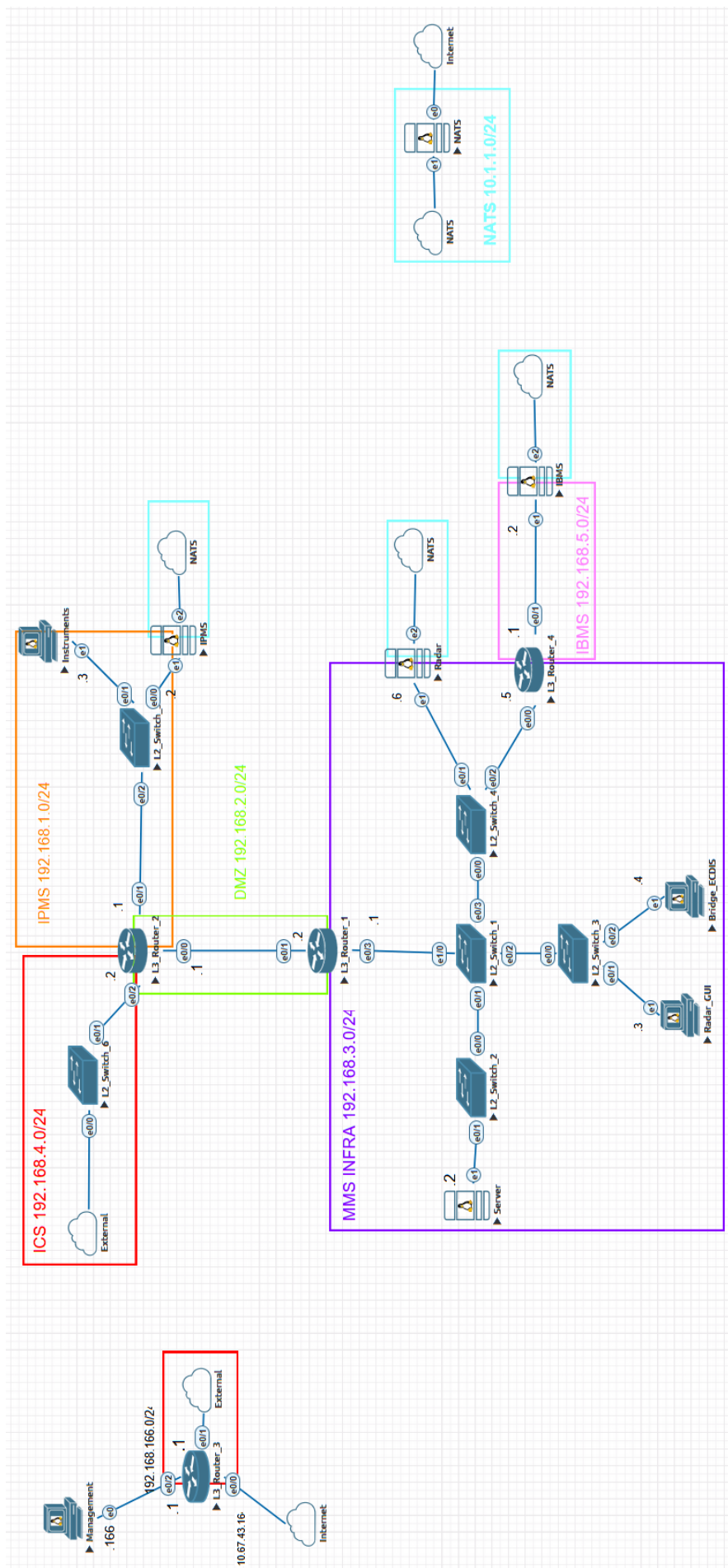
Each container is designed to emulate a specific system or service within the ship's architecture and is assigned a unique IP address within the simulated network. These containers behave like stand-alone devices and can communicate with virtual machines and other containers seamlessly. From the perspective of the end user or any external observer analysing the network, for example through packet capture, the configuration is entirely transparent. This architecture dramatically increases the scalability of the simulation, allowing the deployment of dozens of devices without overwhelming system resources.

#### Network Topology in EVE-NG

Figure 5.1 illustrates the high-level topology of the simulated network implemented in EVE-NG. We clearly distinguish the sub-network of each shipboard domain, as developed in Chapter 3.

The simulated warship environment is structured around a segmented network architecture that mirrors the separation of functional domains found in modern naval platforms. Each sub-network corresponds to a specific operational or technological domain, and is assigned a dedicated IP address range to ensure isolation, clarity of purpose, and realism in traffic modelling.

- **Integrated Platform Management System (IPMS)**  
Manages platform-related systems (propulsion, steering and autopilot).
- **Demilitarized Zone (DMZ)**  
Serves as a buffer zone between external access points and the internal protected systems. In reality, this subnet is used to host a firewall.
- **Mission Management System Infrastructure (MMS INFRA)**  
Hosts core mission services, including virtualization servers, radar systems, DNS server and mail server.
- **Integrated Communication Sub-System (ICS)**  
Handles communication interfaces between ship systems and external networks, providing gateway to the internet.
- **Integrated Bridge Management System (IBMS)**  
Covers navigation systems, sensors, WECDIS, and other bridge-related components.



**Figure 5.1.** Implemented naval cyber range topology in EVE-NG

- **NATS Simulation Layer**

Delivers data from the ship simulator to the relevant network components/containers. The complete explanation of this design principle is given in Section 5.2

A list of all virtual machines deployed within the simulation environment, along with their relevant configuration information and resource allocation is available in Table D.1 of Appendix D.1. Each VM is associated with a specific sub-network and serves a functional role in the emulated warship architecture.

## Network Configuration Files

As explained in Section 5.3, the whole final product to setup the naval cyber range is packed inside a GitHub repository, accessible at <https://github.com/LaquayL/RMA-Naval-Cyber-Range>. Its structure is further described in Section 5.3.

One of the root directories, `network_configuration/`, contains all necessary files related to the network configuration of the lab. Thanks to these, the lab can be fully recreated on a fresh EVE-NG machine.

The following network configuration files are provided:

- `nodes_configuration/cisco/`: provide the exported configuration of all Cisco routers and switches of the lab. EVE-NG allows to create Cisco nodes with a specific startup config.
- `nodes_configuration/netplan/`: gathers the netplan file `50-cloud-init.yaml` of each Ubuntu machine of the network. Configuration of a fresh virtual machine inside a new naval cyber range lab can be done by importing the corresponding netplan file in the machine under the folder `/etc/netplan/` and applying the configuration file using the command `sudo netplan apply`.
- `nodes_configuration/DNS/`: contains the configuration file of the DNS service running inside the "Server" machine. The complete operation of the DNS resolution in the EVE-NG network is explained later in this section.
- `lab_configuration/`: describes the EVE-NG lab topology under `.unl` format. This file is the one to be imported in a new EVE-NG machine in order to build the naval cyber range topology inside a new lab. This file also contains the startup configs of the routers and switches, as mentioned above. It means that importing this file into EVE-NG provides the whole network topology and configure the routers and switches but does not configure the ubuntu machines.

## Internet Access

Each machine within the simulated network is provided with access to the internet to enable browsing, external service interaction, and updates where necessary. This connectivity is established through the use of a special network node labelled "Internet", configured in Management (Cloud0) mode within the EVE-NG environment. This configuration bridges the internal lab network to the first NIC of the EVE-NG host machine, allowing external connectivity.

While the Cloud0 mode is typically used to grant management access to simulated nodes from a host machine outside of the EVE-NG environment [18], it is deliberately repurposed in this simulation. Instead of linking directly to an individual virtual machine, the Cloud0 node is connected to the simulated router "L3\_Router\_3". This router performs Network Address Translation (NAT) for all internal machines, thereby acting as the default gateway and enabling secure outbound traffic from the cyber range to the internet.

An exception to this architecture is the "NATS" machine. As detailed in Section 5.2, the NATS sub-network is fully isolated from the rest of the simulated environment. To ensure it still benefits from internet access, the NATS machine is equipped with a dedicated interface connected directly to its own instance of a Management (Cloud0) node. This allows it to reach external services independently, without traversing the shared simulation gateway or compromising the integrity of the isolated sub-network.

## DNS (Domain Name System) Resolution in the Simulated Network

Proper DNS resolution is essential to enable both internal service discovery and external internet browsing through human-readable domain names. In the context of the simulated warship network, two key requirements must be met: (1) support for external domain resolution to enable browsing and service access, and (2) internal name resolution for services hosted within the simulation environment.

A specific constraint arises from the placement of the EVE-NG host within a secured research network. Common public DNS resolvers such as Google's 8.8.8.8 or Cloudflare's 1.1.1.1 cannot be used directly, as outbound DNS queries are filtered by the research institution's firewall. Instead, all external DNS queries must be relayed through the internal DNS resolver of the research network. While it would be technically feasible to hardcode this resolver into each simulated machine, such a solution is fragile, non-scalable, and violates good network management practices.

To address these challenges, a layered DNS resolution mechanism has been implemented. A summary of the DNS resolution flow is provided in the diagram on Figure 5.2. The virtual machine designated as "Server" hosts a local DNS service using the `dnsmasq` package. This service is configured<sup>1</sup> to resolve domain names for internal services defined within the simulation (e.g., local applications or containerized services). For all other queries (i.e., external domain names) `dnsmasq` forwards the DNS requests to the simulated gateway router.

The gateway router itself is configured as a DNS forwarder, transparently relaying all DNS traffic to the authorized DNS resolver of the research network. Consequently, all machines within the simulation (except the "NATS" machine) are configured to use the "Server" VM IP address as their DNS resolver.

This setup offers several advantages:

- Internal services are resolvable locally, reducing latency and dependency.
- External DNS queries are handled securely and compatibly with institutional policies.
- Machines are only configured with one internal IP for DNS, maintaining simplicity and modularity.

This architecture ensures that DNS resolution is functional, scalable, and compliant with both the constraints of the host environment and the requirements of a realistic cyber range.

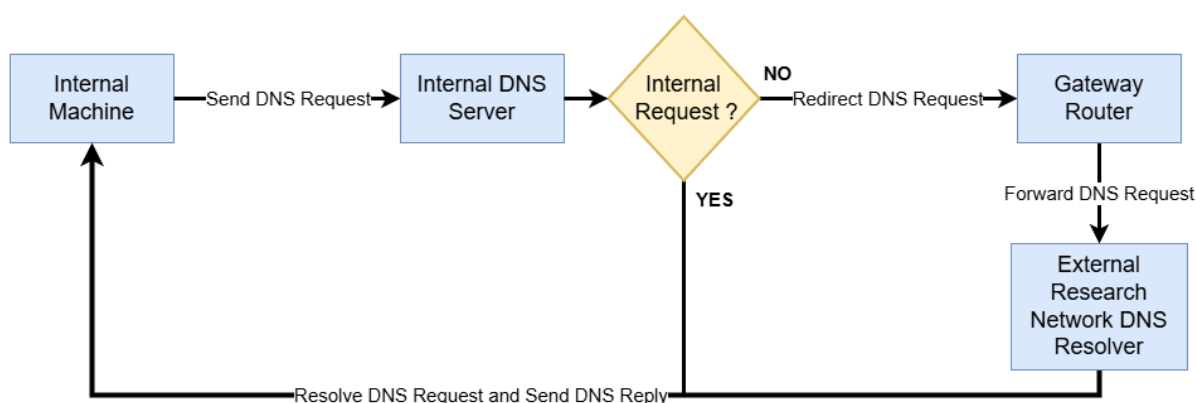


Figure 5.2. DNS resolution diagram

<sup>1</sup>The configuration file of the internal DNS service is available in the folder `network_configuration/nodes_configuration/DNS/` of the project GitHub repository and has to be installed in `/etc/dnsmasq.d/localsites.conf` on the "Server" VM.

## Internal Mail Infrastructure for Scenario Communication

As described in Section 6.3, communication between trainees and the cyber range manager during the execution of the cyber awareness scenario is conducted through a simulated mail channel. This setup introduces the need for a fully operational local mail server within the emulated network, along with properly configured mail clients on the trainee workstations.

The mail server, hosted on the "Server" virtual machine, is implemented using Postfix and Dovecot. It handles all mail traffic within the EVE-NG environment. The complete installation and configuration steps for the mail server are provided in Appendix C.2.1.

To minimize the resource footprint on the Ubuntu desktop machines allocated to the trainees, Claws Mail has been selected as the default mail client. This lightweight solution offers an efficient graphical user interface and supports standard email features. In order to render HTML content, such as clickable links contained in mails, a dedicated Claws plugin is installed and configured. Detailed installation instructions for both the client and plugin can be found in Appendix C.2.2.

On the "Management" virtual machine used by the cyber range supervisor, Thunderbird is used instead of Claws Mail. This choice enables the manager to compose and send HTML-rich mails, including formatted content and embedded links. Despite the difference in software, the configuration process remains similar to that of the Claws Mail client.

The configured internal mail addresses available across the simulated network are as follows:

- `instruments@mail.mcm`
- `radar@mail.mcm`
- `wecdis@mail.mcm`
- `management@mail.mcm`

## Web Browser Optimization for Desktop VMs

Due to limited computing resources available on the Ubuntu desktop virtual machines used in the cyber range, the use of Firefox as the default web browser often results in performance issues. These include delayed responsiveness, interface lag, and in some cases, complete browser crashes, especially when interacting with complex web interfaces such as GUIs or map-based applications.

To address these problems, Falcon<sup>2</sup> has been selected as a lightweight alternative. Falcon provides a significantly smoother user experience by reducing resource consumption while maintaining a fully functional graphical interface. It supports all essential web features required for the cyber awareness scenario, including HTTPS, JavaScript, and internal GUI access.

Additionally, Falcon is easily installable from the Ubuntu Software Center in its Snap package version, making deployment simple and consistent across all trainee workstations. This substitution ensures stability and usability during training sessions without compromising functionality..

## 5.2. Traffic Simulation Methodology and Data Flows

### 5.2.1. Problem of Distributed Data Generation

A critical aspect of designing the naval cyber range lies in defining how to generate and distribute coherent, realistic shipboard data to the various onboard systems requiring it. Many of these systems rely on sensor outputs or control signals that are interdependent. An initial approach could have involved embedding autonomous data generation mechanisms within each system. However, due to the high degree of inter-system dependency, this decentralized method would not ensure consistency or realism across the simulation.

---

<sup>2</sup><https://www.falcon.org/>

### 5.2.2. Centralized Simulation Approach

To address this challenge, the approach adopted in previous projects such as Cyber-MAR and MaCySTe (see Sections 2.2.2 and 2.2.5) was selected. These projects demonstrated the effectiveness of a centralized ship simulation model: one core system generates all necessary ship data in a single location, which is then distributed to the respective simulated components. This ensures coherence and temporal synchronization across all subsystems.

The implementation used in this thesis is based on the architecture proposed by the MaCySTe project. [26] The solution must meet the following requirements:

- Generate consistent and realistic operational data for a virtual ship.
- Distribute relevant subsets of this data to multiple systems in the simulation.
- Operate transparently to end users of the cyber range.
- Prevent interference between data transport and emulated shipboard network traffic.

### 5.2.3. Implementation Using Bridge Command

To fulfil these requirements, the open-source software Bridge Command [11] is used as the central simulation engine. Bridge Command provides real-time maritime simulation capabilities, including configurable scenarios, navigational settings, and environmental parameters. Additionally, it provides a GUI of the simulation showing a view from the deck of the ship. The application is compiled and deployed using Flatpak, and minor modifications are introduced to expose internal simulation variables such as position, heading, speed, radar, GPS, propulsion, and steering values.

### 5.2.4. Data Distribution via NATS Message Queue (MQ) and JetStream Key-value Store

For the distribution layer, a NATS Message Queue (MQ) is implemented. NATS provides asynchronous, event-driven communication and allows each subscriber system to receive only the data streams it needs. For persistent state variables (such as speed, heading, and position) the NATS server is configured in JetStream mode, maintaining the latest value for each variable and ensuring efficient dissemination to consumers. [32]

To isolate simulation data traffic from the main ship network emulation, all virtual machines hosting onboard systems are equipped with an additional network interface linked to the dedicated NATS sub-network. Containers representing the systems themselves also inherit this interface, ensuring that traffic used for sensor and control data exchange does not interfere with shipboard packet captures or scenario execution.

Lastly, to address compatibility issues between NATS and EVE-NG's Cloud network mode, a distributed cluster of NATS instances is deployed. Two virtual machines (IPMS and IBMS) host containers acting as NATS relays. These instances are configured in clustered mode, enabling message replication and multi-location distribution across the network. [31] This architecture ensures reliability and consistency in data propagation, regardless of the point of subscription or network conditions within the simulation.

## 5.3. Code and Configuration Files

### 5.3.1. Code Distribution and Development Workflow

To centralize all code files and network configuration assets, GitHub has been selected as the primary distribution platform for the project. As discussed in Section 5.4, many modules and containerized components are derived from or adapted based on the codebase of the open-source MaCySTe project. In order to comply with the licensing terms of that project, the repository is distributed under the *GNU Affero General Public License (AGPLv3)*.

Beyond licensing compliance and public access, this distribution method also provides significant benefits during the development phase. The GitHub repository is cloned directly onto the relevant Ubuntu virtual machines within the EVE-NG simulated network that host containerized services. When updates to the code are made locally on an external development machine, changes can be easily deployed across the simulation environment by simply executing a `git pull` command. This approach streamlines the workflow and avoids compatibility issues between isolated development environments and deployed virtual systems.

The complete project repository is available on GitHub at the following link:

**<https://github.com/LaquayL/RMA-Naval-Cyber-Range>**

### 5.3.2. Repository Structure

As discussed earlier, the project developed in this thesis builds upon several components from the MaCySTe project<sup>3</sup>. [26] As a result, the structure of both repositories shares notable similarities. The GitHub repository of this project is organized into distinct categories of files, each serving a specific role. The repository is structured as follows:

```
.
├── network_configuration/
│   ├── lab_configuration/
│   └── nodes_configuration/
├── src/
│   ├── configs/
│   ├── containers/
│   ├── flatpaks/
│   ├── pods/
│   ├── scenarios/
│   │   └── oo-modules/
│   ├── scripts/
│   ├── alloc.Makefile
│   ├── Makefile
│   └── settings.Makefile
```

The first part of the repository is dedicated to the network configuration files. The description of them has already been made in Section 5.1.3.

The second portion of the repository holds all the resources necessary for building and running the containerized modules as well as the Bridge Command Flatpak.

At the root of the repository lies the `Makefile`, which acts as the entry point for building and deploying project components. Depending on the command invoked, this file allows users to build container images, launch or stop containers, and compile and run the Bridge Command simulation. The `settings.Makefile` contains general settings, including the chosen Bridge Command scenario (in the future, multiple environment settings sets can be defined in the project files of the Bridge Command simulation).

Each virtual machine in the EVE-NG topology is intended to use the project on a different way (different containers, IP addresses, Podman networks...). Each virtual machine is thus linked to a specific "usage scenario" of the project, represented by a subdirectory within the `scenarios/` folder. The scenario name corresponds to the hostname of the virtual machine within the EVE-NG network. During deployment, the active scenario is passed to the `Makefile` using the variable `SCENARIO_NAME=<machine_name>`.

---

<sup>3</sup>MaCySTe GitHub repository: <https://github.com/CRACK-MCR/MaCySTe>



Each scenario defines a set of modules sourced from the `00-modules/` directory. These modules typically represent containers and associated Podman networks to be instantiated on the machine. Each module contains files that define pods name corresponding to the module and interface configurations. Static IP addresses for container interfaces are allocated during deployment based on the mappings specified in `alloc.Makefile`.

Pods configurations are organized under the `pods/` directory, with each pod having its own subdirectory containing a `pod.yaml` file. This file includes metadata for each container such as container image, environment variables, port mappings, and network associations.

Some pods require additional configuration files at runtime. These are stored in the `configs/` directory and mounted into the containers as needed.

Before deployment, container images must be built. The `containers/` directory includes one subdirectory per image, containing the necessary build context, source code and instructions.

Since Bridge Command is a full desktop application rather than a containerized service, it has a dedicated folder inside the `flatpaks/` directory. This folder contains the build manifest, patches (as referenced in Section 5.2), and scenario-related ship simulation settings used to compile the Flatpak from source.

Finally, the `scripts/` directory contains various scripts and malware files used during the execution of cyber attack scenarios described in Section 5.7.

## 5.4. Software Development and System Components

### 5.4.1. Components Implementation

As mentioned earlier, the open-source maritime cyber range project MaCySTe [26], originally designed as a containerized solution running on a single machine for maritime cybersecurity research, offers a wide array of valuable components simulating shipboard systems. Due to their relevance and reusability, many of the components implemented in the present project are adapted versions of these MaCySTe modules.

The primary challenge of this thesis was not to develop all components from scratch, but rather to restructure and decouple them in a way that allows their distribution across multiple virtual machines, each representing different domains of the warship's digital architecture. This required maintaining the necessary interconnections between distributed modules, while preserving consistency and interoperability within the simulated network.

Table 5.1 provides a consolidated overview of all components deployed in the environment. It specifies which virtual machine each component runs on, briefly describes its role within the system, and identifies the original source from which the component was derived or adapted.

Host VM	Module Name	Role Description	Source
NATS	nats	Main cluster instance of combined NATS MQ and JetStream key-value store	NATS <sup>4</sup> [30]
IPMS	nats_relay_1	Relay cluster instance of combined NATS MQ and JetStream key-value store	NATS
	engine_sim_plc (left and right)	Engine fictitious PLCs (Modbus store) relaying the set values to the NATS MQ	MaCySTe <sup>5</sup> [26]
	engine_telegraph (left and right)	Engine telegraphs relaying simulation values from the MQ to an attached Modbus slave	MaCySTe
	steering_gear_physics	A physical model for the Steering Gear System (SGS)	MaCySTe
	sgs_pump (1 and 2), sgs_oil (1 and 2), sgs_oil_tank, sgs_master	PLCs modeling the SGCS sub-systems for the SGS simulator	OpenPLC <sup>6</sup> [2]
	helm	Rudder actuator relaying the set values to the NATS MQ	MaCySTe
	autopilot	Interacts with WECDIS and NATS to provide autopilot navigation	MaCySTe
	sgs_hmi	HMI allowing monitoring of the SGS simulator	Fuxa <sup>7</sup> [20]
	gui_instruments	GUI for controlling the autopilot, rudder, and engines	MaCySTe
IBMS	nats_relay_2	Relay cluster instance of combined NATS MQ and JetStream key-value store	NATS
	rtu (ai, gp, he, ii, ra, sd and ti)	NMEA demuxes (RTUs) taking data from the MQ to simulate ship sensors	MaCySTe
	ecdis_opencpn	Provides WECDIS and radar plugin support	OpenCPN [33]
	autopilot_forwarder	Forwards autopilot messages from OpenCPN to the autopilot via TCP	Custom
Radar	radar_converter (ASTERIX and Navico)	Acts as radar antenna, transmitting MQ radar data via ASTERIX/Navico protocols	MaCySTe
Server	ppi (ASTERIX and Navico)	GUI with Plan Position Indicator (PPI) radar display	MaCySTe and OpenCPN
Management	gui_attack (radar and WECDIS)	GUI to monitor and launch cyber attacks against radar/WECDIS	MaCySTe
	websocket_to_websocket (radar and WECDIS)	Manages WebSocket connections between attack GUI and malwares running during cyber awareness scenarios	MaCySTe

**Table 5.1.** Summary of Modules Implemented per Host Virtual Machine

<sup>4</sup><https://github.com/nats-io>

<sup>5</sup><https://github.com/CRACK-MCR/MaCySTe>

<sup>6</sup>[https://github.com/thiagoralves/OpenPLC\\_v3](https://github.com/thiagoralves/OpenPLC_v3)

<sup>7</sup><https://github.com/frangoteam/FUXA>

### 5.4.2. Podman Networks Implementation

The container network architecture inherited from the original MaCySTe project was no longer applicable in the context of a distributed, multi-VM naval cyber range. As a result, the entire organization of container-to-network mappings was restructured to support a more realistic and scalable topology, where each container could be attached to the appropriate interface of its host virtual machine.

Podman supports various networking modes, each offering different characteristics in terms of isolation, performance, and integration with the host. For this project, the `macvlan` network driver was selected. In this mode, each Podman network is linked to a specific interface of the host virtual machine, and containers connected to it behave like independent devices on the same Layer 2 segment. Each time a container is started, it is assigned a new MAC address, making it visible as a distinct node on the network.

To ensure deterministic network behaviour and simplify integration with the simulated shipboard topology, all containers are launched by the Makefile with a fixed IP address using the `-ip` argument. These IP addresses are centrally managed in the `alloc.Makefile` file, which allocates unique static addresses for each container interface across the entire project.

It is important to note a practical consideration with this configuration: due to the use of `macvlan` networks and static IP addresses, restarting a container too quickly after shutting it down can lead to network communication issues. Specifically, upstream routers may retain stale ARP entries, still associating the container's IP with its previous MAC address. Since the container will receive a new MAC address upon restart, this mismatch can prevent proper routing of traffic. To mitigate this, a short delay should be observed between shutdown and restart operations to allow ARP caches to expire or be flushed (in the current router configurations, ARP persistence has been set to 30 seconds).

### 5.4.3. Container Management

As discussed in Section 5.3, a Makefile is used as the primary entry point for managing the containers and associated project files. It abstracts many complex tasks and simplifies the deployment and maintenance of the simulation components. For this purpose, a set of make commands are available to the user in order to manage the deployment of the project. A non-exhaustive list of the most useful commands for container management during development and execution is available in Appendix D.2.

## 5.5. Modularity and Extensibility of the Project Structure

As examined in Section 5.3, the repository structure of the project has been carefully designed to ensure modularity, scalability, and ease of management. This design not only facilitates current development and simulation efforts, but also supports future extensions with minimal effort.

The use of scenario-specific directories for each virtual machine allows new hosts to be added seamlessly. To include a new virtual machine in the simulation, one simply needs to define a new scenario directory containing a `config.Makefile` with the desired modules. Similarly, moving a module from one machine to another requires only relocating the corresponding module name between scenario `config.Makefile` and updating static IP addresses and any required external variable bindings.

Creating a new module is also straightforward. The following steps summarize the necessary actions to integrate a new module into the architecture:

1. If required, create a directory under `containers/` to define and build a custom container image.
2. Add a `pod.yaml` file under `Pods/` specifying the container configuration, including image, environment variables, and exposed ports.
3. Define a corresponding module directory under `oo-modules/`, detailing the container's interface definitions and any external variable dependencies.
4. Register static IP address entries for the new module interfaces in `alloc.Makefile`.

In addition to modular container and network management, the Bridge Command simulation environment allows for the creation of multiple cyber awareness scenarios involving different mission types, geographic locations, environmental conditions, or ship positions. To define a new simulation context, users can create dedicated subdirectories within the `scenarios/` and `worlds/` folders of the Bridge Command project structure. In the case of scenarios in new regions, corresponding navigation charts can be downloaded on OpenSeaMap<sup>8</sup> and placed in the `opencpn/charts` folder of the `configs` directory. Switching between simulation contexts is easily achieved by updating the `BC_SCENARIO` variable in the root `settings.Makefile`, allowing for flexible testing and training use cases.

## 5.6. Graphical Interfaces for User Interaction

For the purpose of cyber awareness training, several graphical user interfaces (GUIs) are made available to the trainees. These interfaces allow each crew member to interact with and monitor the various shipboard systems in a realistic and user-friendly manner. Three crew functions are modelled in the cyber range, each corresponding to a specific operational role and associated with a dedicated desktop virtual machine (VM) within the EVE-NG network architecture.

As shown in Table 5.1, the containers responsible for serving these GUIs are not hosted directly on the Ubuntu desktop machines used by trainees. Instead, they run on Ubuntu server VMs located in different segments of the simulated network, depending on the domain to which their functionality belongs. This reflects the broader architectural decisions discussed in Chapter 3, which introduced the simplification model of a Mine Countermeasure (MCM) warship's digital infrastructure.

To provide seamless access to these interfaces, internal name resolution is handled by the DNS infrastructure described in Section 5.1.3. Trainees can access the appropriate GUI from their web browsers using simple domain names mapped to their respective services. A full list of accessible GUI links is presented in Appendix D.3.

Although the web interfaces are technically accessible from any trainee workstation, each crew member is assigned a specific subset of GUIs according to their designated role. This assignment ensures clarity of scope during the scenario and allows each trainee to focus on the functions relevant to their area of responsibility.

This section details the graphical interfaces assigned to each role, the functionalities they provide, the type of information trainees must monitor, and the interaction mechanisms available through each GUI. Finally, the cyber range includes a dedicated "Management" desktop VM deployed outside the simulated ship network within the EVE-NG topology. This machine is reserved for the cyber range manager and has unrestricted access to all other systems. It hosts a specialized GUI that enables the manager to launch and control the cyber attacks during training sessions. While the usage of this attack GUI is briefly presented in this section, its technical implementation and role within the full cyber awareness scenario are discussed in more depth in Section 5.7.

### 5.6.1. Ship Simulator Display

As demonstrated in Sections 5.2.2 and 5.2.3, Bridge Command is used as the central ship simulator to generate coherent and realistic ship data for distribution across the cyber range. Originally designed as an interactive 3D training software, Bridge Command also provides a graphical bridge view of the simulated vessel from the perspective of the operator. [11]

In the present implementation, this interactive interface is not accessible to the trainees; no user can directly control the ship through the simulator. However, the cyber range manager may choose to project the simulation view on a large screen visible to all participants. This contributes to the overall immersion of the exercise, reinforcing the perception that the trainees are operating a real ship rather than merely interacting with abstract system interfaces.

---

<sup>8</sup>[https://www.openseamap.org/index.php?id=openseamap&no\\_cache=1&L=1](https://www.openseamap.org/index.php?id=openseamap&no_cache=1&L=1)

By default, the simulation window is overlaid with a Heads-Up Display (HUD), which presents a summary view of critical operational data, such as position, heading, speed, radar Plan Position Indicator (PPI), and steering gear status. This data corresponds to the information simultaneously available to trainees through their dedicated GUI interfaces. An example of the simulation view with the HUD enabled is shown in Figure 5.3.



**Figure 5.3.** Ship simulator bridge view with Heads-Up Display (HUD)

To adapt the level of information exposure, the HUD can be toggled off using the “Hide” option in the interface. This allows the manager to enforce role-specific information flow, ensuring that trainees rely solely on their assigned graphical interfaces. Figure 5.4 illustrates the bridge view with the HUD disabled and the visual perspective oriented to the right side of the ship.



**Figure 5.4.** Ship simulator bridge view without HUD

It is also important to note that the bridge view display of the ship simulation is relatively resource intensive. To optimize system performance, particularly while using the naval cyber range for cyber research purposes or during scenario executions that do not require visual immersion, the graphical interface can be disabled. This is achieved by setting the `BC_HEADLESS` variable to `1` in the `settings.Makefile` file. In this headless mode, the simulation still runs and generates relevant ship data, but without rendering the 3D bridge environment.

### 5.6.2. Radar Operator

Two different radar display interfaces are provided in the cyber range to reflect distinct implementations of radar visualization used in modern maritime systems. Each interface uses data from a different radar protocol.

#### ASTERIX Radar

The first radar GUI, shown in Figure 5.5, is a custom interface originally developed in the MaCySTe project. It visualizes radar data received through the ASTERIX protocol, a standardized format commonly used maritime surveillance data. In this interface, the radar image remains north-aligned, meaning that the top of the Plan Position Indicator (PPI) display always corresponds to the geographic north. In the upper-left corner of the interface, the user is provided with controls to configure radar range (selectable between 3 and 12 nautical miles (NM)) and to adjust the radar gain. Adjusting gain is particularly useful in scenarios with significant clutter or noise, allowing the trainee to improve readability of the radar display by filtering weak or irrelevant echoes.

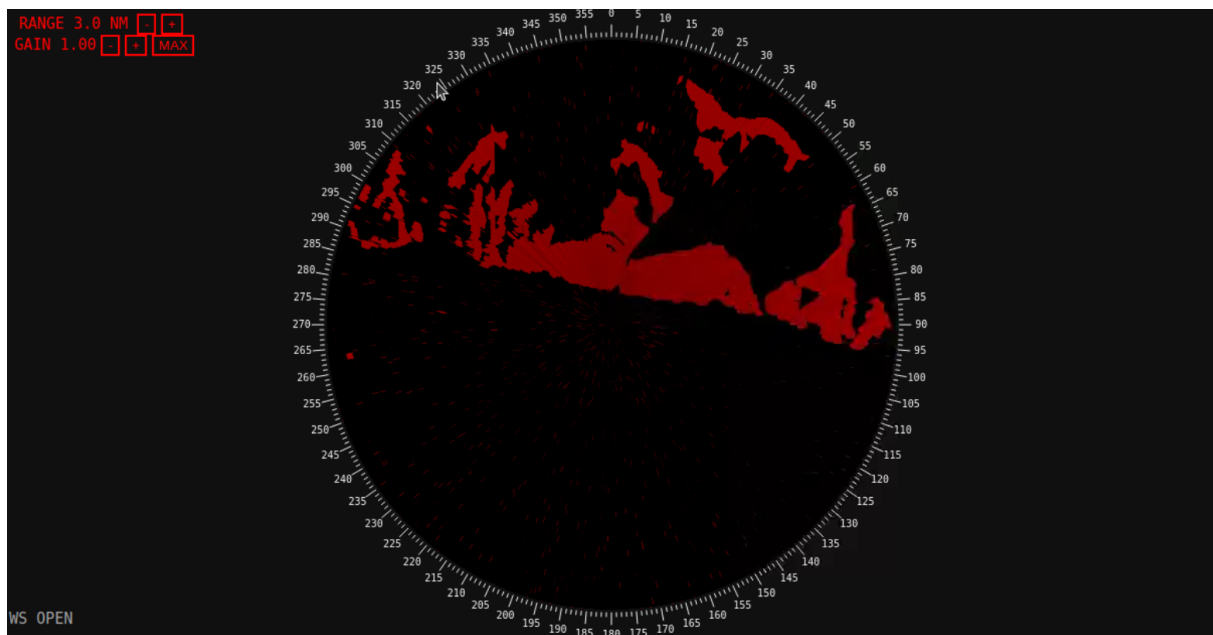


Figure 5.5. ASTERIX radar GUI

## Navico Radar

The second radar GUI, shown in Figure 5.6, is implemented using the Navico radar plugin integrated into the OpenCPN container (which is the same software environment used for the WECDIS system). This interface displays radar data through the proprietary Navico protocol, which was implemented in MaCySTe based on the reverse-engineering insights described in [17].

Unlike the ASTERIX-based display, the Navico interface is ship-aligned, meaning that the top of the radar PPI represents the bow of the ship, and the bottom corresponds to the stern. The “+” and “-” buttons at the bottom of the interface allow users to switch the display range between 3 and 12 NM.

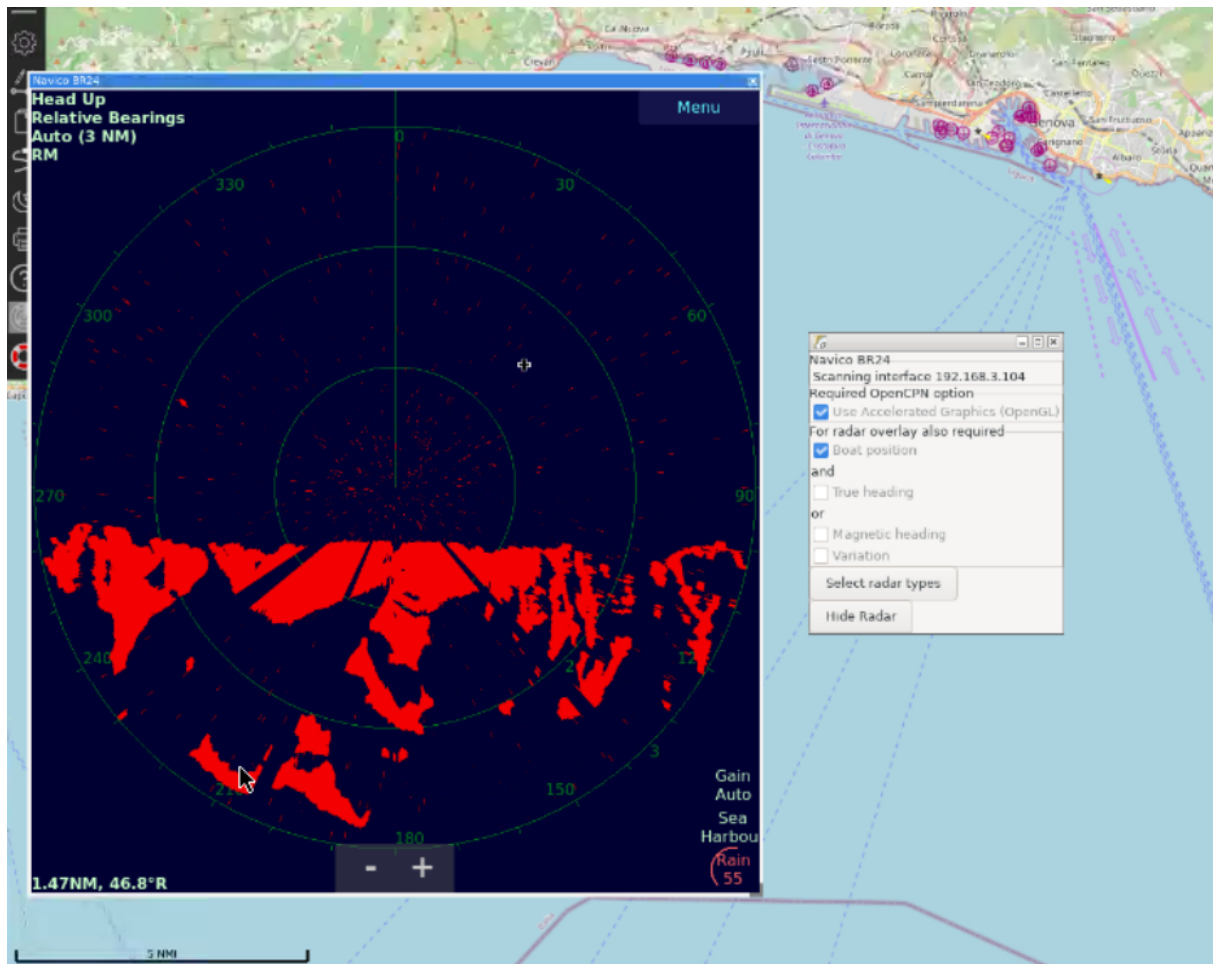


Figure 5.6. Navico radar GUI

### 5.6.3. Engine Operator

The engine operator is responsible for two primary tasks: (1) controlling the ship's movement using the navigation instruments, and (2) monitoring the Steering Gear System (SGS) via a Human-Machine Interface (HMI) implemented with FUXA.

#### Navigation Instruments GUI

The navigation instruments GUI for the engine operator is shown in Figure 5.7. This interface is divided into three main panels: the autopilot, the rudder controller, and the engine telegraphs.

In manual piloting mode (when the autopilot panel is inactive/dark), the trainee can control the ship's heading by setting the rudder angle and adjust speed by independently regulating the power of the left and right engines.

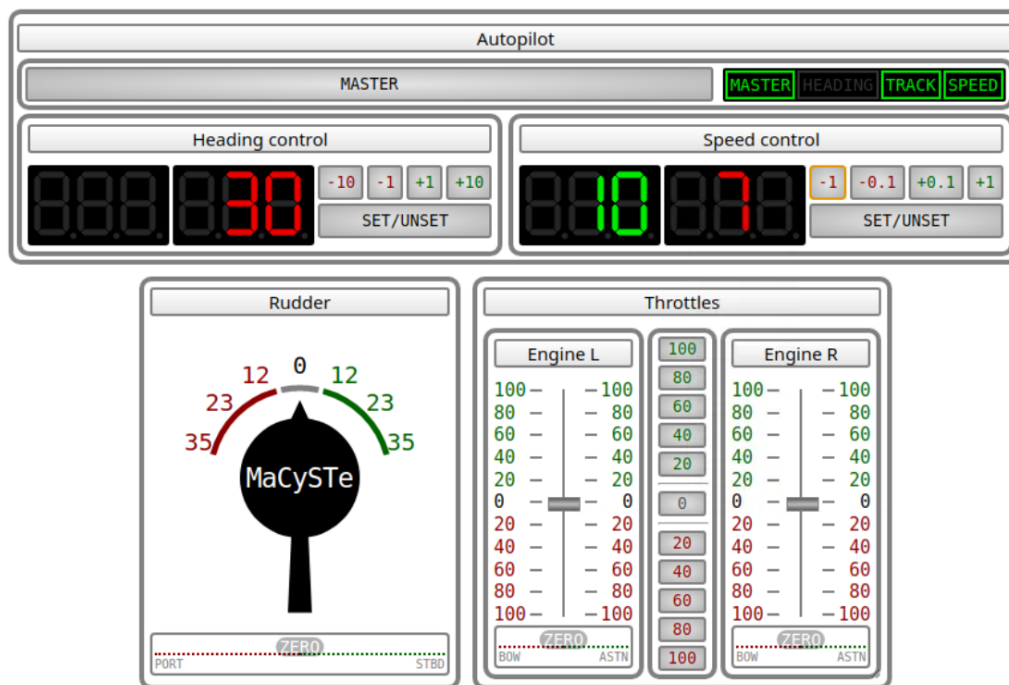


Figure 5.7. Navigation instruments GUI

**Rudder Panel** The rudder is controlled via a helm interface. The trainee can interact by dragging the helm button to the desired angle or by clicking directly on predefined angle values. The rudder can rotate from 35° to port (left) to 35° to starboard (right). A coloured bar beneath the helm shows the current percentage of the desired rudder angle relative to the maximum.

**Throttle Panel** In the throttle panel, the user can control the power percentage applied to the left and right engines independently by dragging the respective levers. Alternatively, clicking on the numeric labels directly sets the power. To synchronize both engines, the central ladder can be used to apply the same power level to both engines. As with the rudder, a coloured bar below each telegraph indicates the set power percentage.



**Autopilot Panel** Activating the autopilot is done via the “Master” switch, turning the panel status bar green with the label MASTER. The autopilot offers three modes of control: speed, heading, and track.

- **Speed control:** The trainee sets a target speed in knots, appearing in red. Upon clicking “SET/UNSET,” the value is applied in green, and “SPEED” appears in green in the autopilot status bar.
- **Heading control:** A target heading in degrees ( $0^\circ$  = North, increasing clockwise up to  $360^\circ$ ) can be selected in red. Clicking “SET/UNSET” applies it in green, and “HEADING” appears in green in the autopilot status bar.
- **Track control:** If heading control is disabled<sup>9</sup>, the WECDIS operator (see Section 5.6.4) can enable track mode, causing the ship to automatically adjust its heading to follow a designated path. When detected, “TRACK” appears in green in the autopilot status bar.

Further technical details on the rudder, throttle, and autopilot functionalities can be found in the MaCySTe. documentation [13]

### Steering Gear System GUI

The SGS simulation, as adapted from the MaCySTe project [26], models a steering system based on two independent electro-hydraulic circuits, each containing a pump. The system is visualized and monitored using the HMI shown in Figure 5.8.

The trainee can activate or deactivate each pump using the dedicated buttons. Although the rudder is typically controlled via the navigation instruments GUI, a desired rudder angle can also be set within the SGS HMI using a slider.

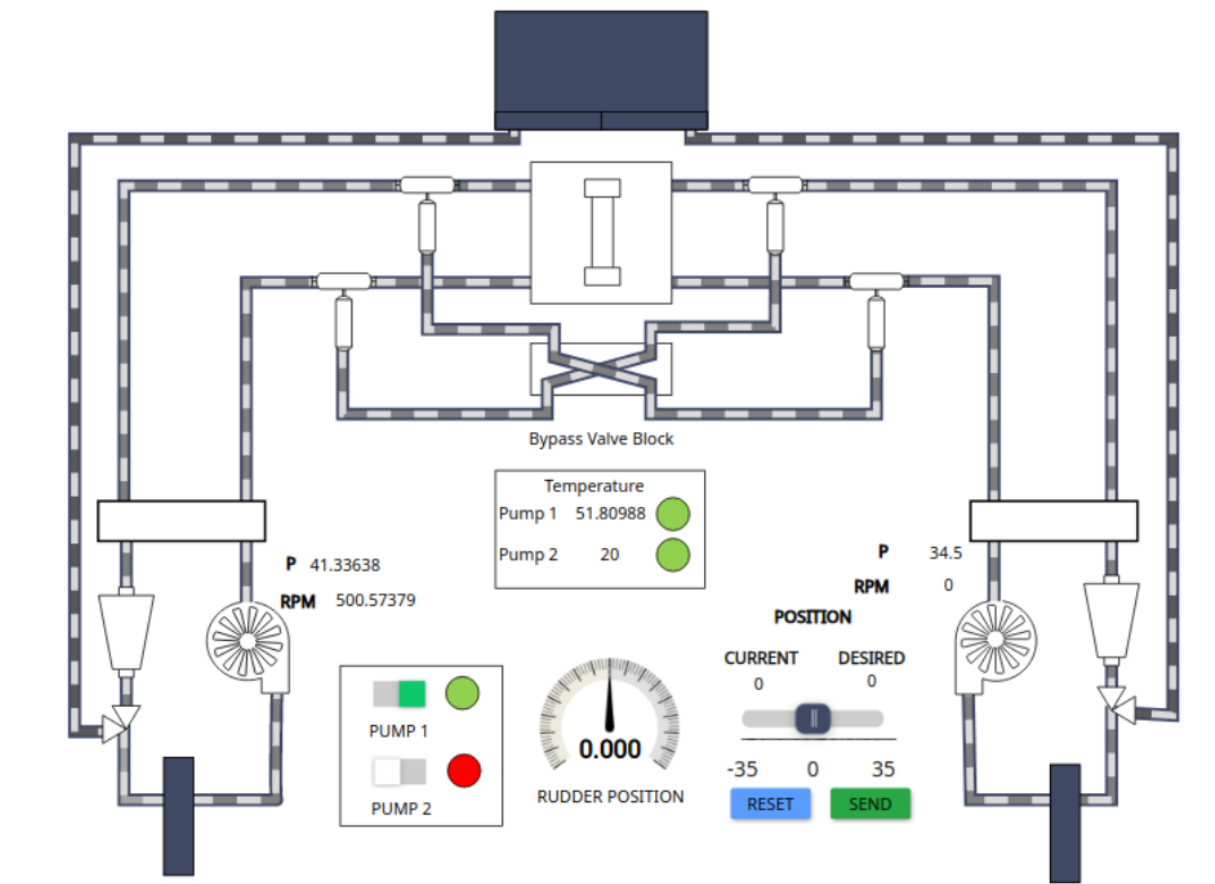


Figure 5.8. SGS monitoring GUI

<sup>9</sup>If heading control is enabled but a waypoint source provides a route compatible with track mode, the “TRACK” light will blink orange to indicate a switch is possible. [13]

Key operational parameters visible in this interface include:

- Desired vs. actual rudder angle.
- Flow status of each pump
- Temperature of each pump.
- Rotation speed in revolutions per minute (RPM).
- Hydraulic pressure (P) in each circuit.

By default, only one pump is active, which is sufficient for normal operation. If both pumps are deactivated, the rudder defaults to a neutral position ( $0^\circ$ ), regardless of the desired command. Rapid changes in rudder angle may cause pump overheating, triggering visual alarms. To prevent this in such operation cases, the secondary pump can be activated to relieve the load and reduce thermal stress. [13]

#### 5.6.4. WECDIS Operator

The Warship Electronic Chart Display and Information System (WECDIS) implemented in this project is based on the open-source navigation software OpenCPN. [33] This system serves as the primary interface for the navigation officer to monitor ship positioning, situational awareness, and track-following operations.

The interface provides the operator with a comprehensive view of key navigational elements overlaid on a maritime chart. These include:

- **Own ship position:** represented by a red ship icon.
- **Heading and speed:** indicated by a dashed white line (heading) and a red dashed extension (relative speed) from the vessel's bow.
- **Other vessels:** represented by yellow ship icons, each labeled with its AIS code, corresponding to ships defined in the active Bridge Command simulation scenario.

WECDIS interface is shown in Figure 5.9.



Figure 5.9. WECDIS GUI

As described in Section 5.6.3, the WECDIS operator has the ability to define a navigation waypoint for use with the autopilot's track-following mode. This is done by right-clicking at the desired location on the chart and selecting the "Navigate To Here" option from the context menu. A red line will then appear on the map, showing the planned route, while the navigation data is displayed in the upper right corner of the interface.

When track mode is active, the autopilot system will continuously adjust the ship's heading to follow the defined route. An example of the WECDIS interface in track mode is provided in Figure 5.10.

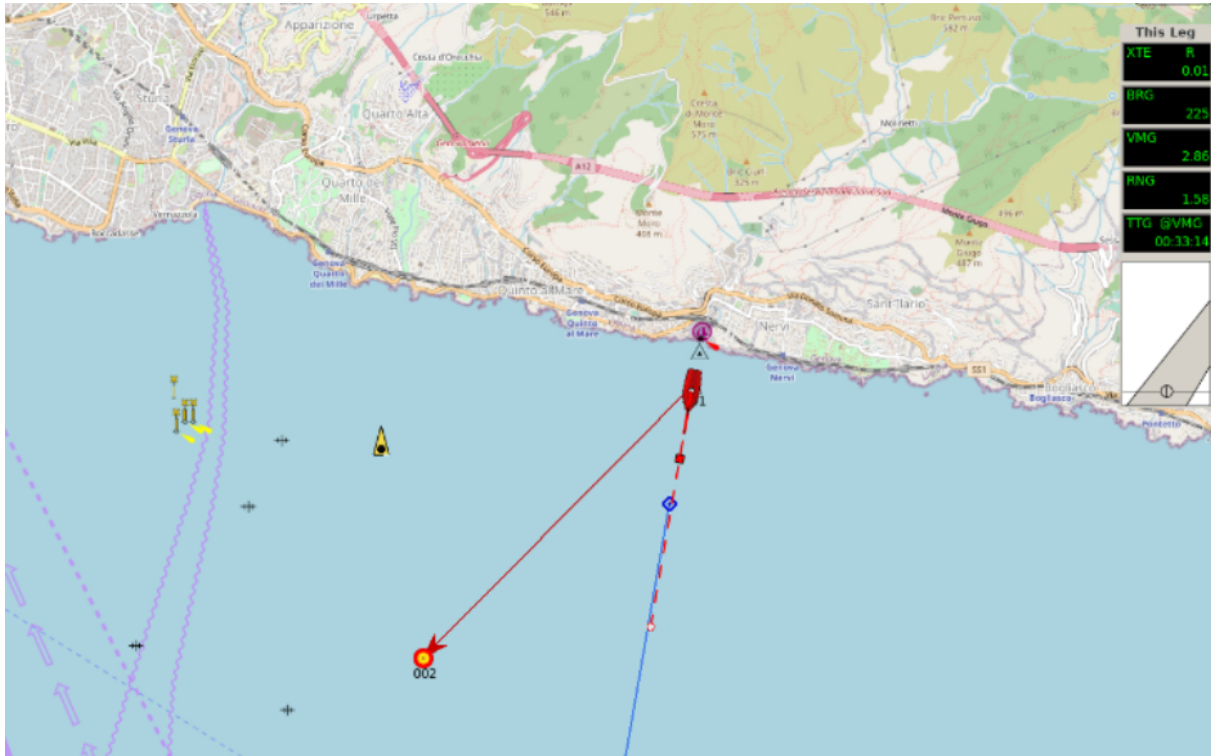


Figure 5.10. WECDIS GUI with track autopilot set

### 5.6.5. Cyber Range Manager

On a dedicated virtual machine, the cyber range manager is provided with access to a graphical user interface (GUI) designed specifically to control the execution of cyber attacks during awareness training scenarios. This interface is served locally by a web server running within a container on the manager's virtual machine. For security and containment reasons, the attack GUI is only accessible from this machine and cannot be reached from other systems within or outside the simulated network.

The interface itself is adapted from the MaCySTe project and has been customized to meet the specific requirements of the training scenarios developed in the current project. It serves as a centralized command and control (C&C) platform, enabling the range manager to initiate, coordinate, and observe various cyber threats introduced during a scenario.

In the current implementation, one instance of the attack GUI is configured for each target machine that may later host and launch a malware payload. In the present case, two instances are associated respectively with the radar desktop machine and the IBMS server. This modular structure allows the manager to independently manage attack vectors based on the targeted subsystem.

This structure and methodology also offer significant benefits in terms of modularity and scalability. Should new cyber awareness scenarios be developed, additional C&C containers can easily be defined within a new scenario file for the management machine. By simply launching the appropriate scenario configuration for the manager's virtual machine, these newly instantiated containers enable access to an alternative set of target machines, along with a distinct set of cyber attacks tailored to the new scenario.

context. This flexibility supports the progressive enrichment of the cyber range and encourages the reuse and extension of existing components for evolving training objectives.

While the GUI includes several panels and functionalities, its primary function is to streamline and supervise the execution of scenario-driven cyber events. The detailed design and progression of the cyber awareness scenario, including how these attack interfaces are used in practice, are discussed further in Section 5.7.

## 5.7. Integration of Cyber Threats/Attacks

To validate the architecture and practical usability of the naval cyber range developed in this project, a dedicated cyber awareness scenario has been designed and implemented. This scenario serves as a proof-of-concept, showcasing the range's potential to support training objectives in a realistic and operationally relevant environment.

The primary aim of the scenario is to illustrate how the cyber range can be used to raise awareness among shipboard personnel about IT and OT threats, attack propagation, and the importance of detection and response procedures. It provides a concrete example of how the range can simulate adversarial actions, system compromises, and operational disruptions in a controlled training context.

This section presents a detailed explanation of the scenario's objectives, structure, and progression. It also provides insights into the technical implementation and the various user interactions involved throughout the exercise.

### 5.7.1. Design and Implementation of the Malware

The design principle for implementing cyber attacks within the naval cyber range is based on the deployment of a single, modular malware component capable of supporting multiple execution modes. Depending on the host machine where the malware is launched via its installer, the program automatically selects the appropriate mode. This selected mode determines the Command and Control (C&C) server to which the malware connects, as well as the specific library of attacks that will be made available to the cyber range manager through the attack GUI.

The malware directory is organized as follows:

```
.
├── __main__.py
├── cc_over_ws.py
├── nmea.py
├── settings.py
├── attacks/
│   ├── attack1.py
│   ├── attack2.py
│   └── ...
```

The malware implementation is adapted from the `malware_ship_side` container originally developed in the MaCySTe project. [26] The Python-based structure has been retained, as it provides an intuitive and flexible foundation for expanding the attack library. To add a new attack, a developer simply needs to create an additional Python script within the `attacks/` subdirectory.

The configuration file `settings.py` contains definitions for all supported modes and associated parameters, along with global variables used throughout the malware's operation.

The file `__main__.py` serves as the entry point for execution when triggered by the installer. It is within this script that the name of the running malware process is defined, which play an important role later when trainees must find the malicious processes.

The module `cc_over_ws.py` handles all C&C communication using WebSocket connections. It is also responsible for providing the available attacks to the manager based on the current mode selected at runtime.

Finally, the `nmea.py` script operates independently of the main malware loop and is dedicated to sniffing any available NMEA packets traversing the host's network interface. These packets are relayed to the C&C server to enrich the attacker's situational awareness, enabling the GUI to visualize ship positions, including the victim and nearby vessels, along with their AIS codes from the Bridge Command simulation.

This architecture, which combines multiple execution modes with a flexible attack library, provides a powerful and extensible platform. It allows cyber attacks to be launched from any designated virtual machine, targeting any system, with precise control over behaviour and parameters. This modularity is essential for adapting the cyber range to evolving training needs and research objectives.

### 5.7.2. Cyber Attack Sequence

In the context of the cyber awareness proof-of-concept, a realistic yet manageable cyber attack scenario has been implemented. The goal is to expose trainees to plausible adversarial behaviour that mirrors real-world tactics while ensuring that the attack remains simple enough to be detected, analysed, and remediated within the limited duration of a training session.

To meet this objective, the scenario unfolds as follows:

1. **Phishing and initial infection:** The trainee, operating from the radar desktop virtual machine, receives a phishing email containing a malicious link (cf. Figure 5.11). Upon clicking the link, an installer is downloaded and executed directly on the trainee's system.
2. **Malware installation and execution:** The installer retrieves the malware source code from a remote server and stores it on the local disk. It then launches the malware as a background process with the noticeable name `"I_control_your_ship"`. Once initialized, the malware connects to the associated Command and Control (C&C) interface. From there, the cyber range manager has access inside the radar attack GUI to a library of potential attacks to launch from the infected radar desktop machine (cf. Figure 5.12).
3. **Lateral movement:** The malware enables the range manager to propagate the infection to the IBMS server. Once this second instance of the malware connects to the C&C server, the interface updates with additional capabilities. Because the IBMS sub-network handles NMEA traffic, the GUI now gains access to positional and identification data of the simulated vessels. This is reflected by the appearance of ship icons on the dynamic map (cf. Figure 5.13) and a list of ships and their AIS (cf. Figure 5.14).
4. **GPS spoofing attack:** From the compromised IBMS server, the manager initiates a GPS spoofing attack. This manipulation affects the position displayed on the WECDIS, falsely relocating the ship to a location on land (cf. Figure 5.16). The attack is triggered from the IBMS-specific C&C interface (cf. Figure 5.15).
5. **Radar denial of service:** Later in the scenario, the manager launches a Denial of Service (DOS) attack targeting the ASTERIX radar system. The radar operator interface becomes saturated (cf. Figure 5.17).

This scenario highlights common phases of a real cyber intrusion, including social engineering, malware execution, lateral movement, and the disruption of critical OT systems. It also provides the trainees with clear opportunities to identify anomalies, perform system forensics, stop malicious processes, and restore affected services within a realistic but controlled environment.

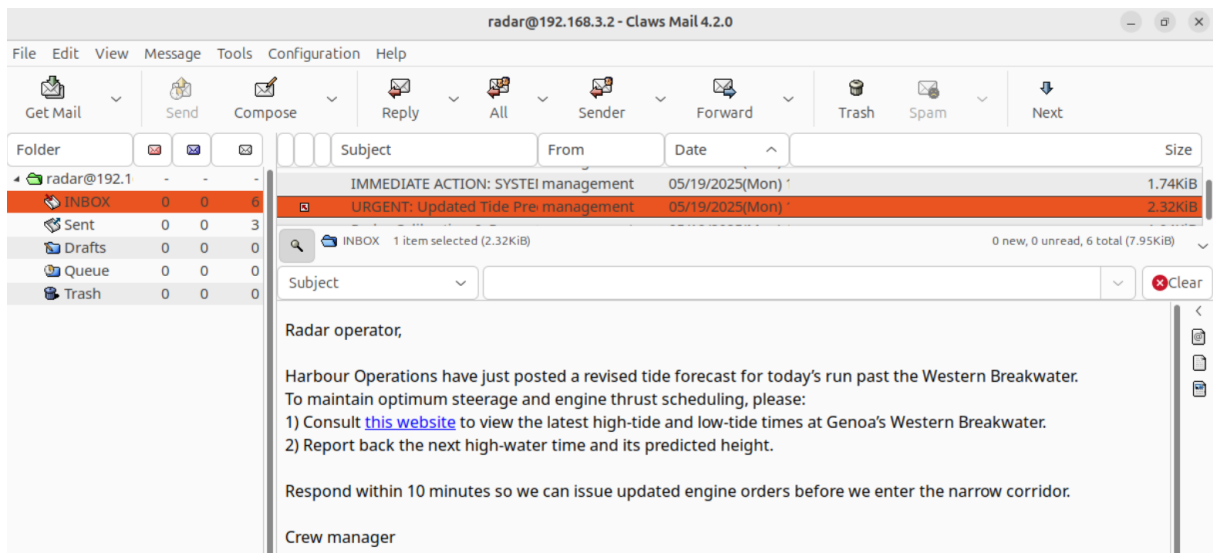


Figure 5.11. Phishing mail used as entry point for the malware

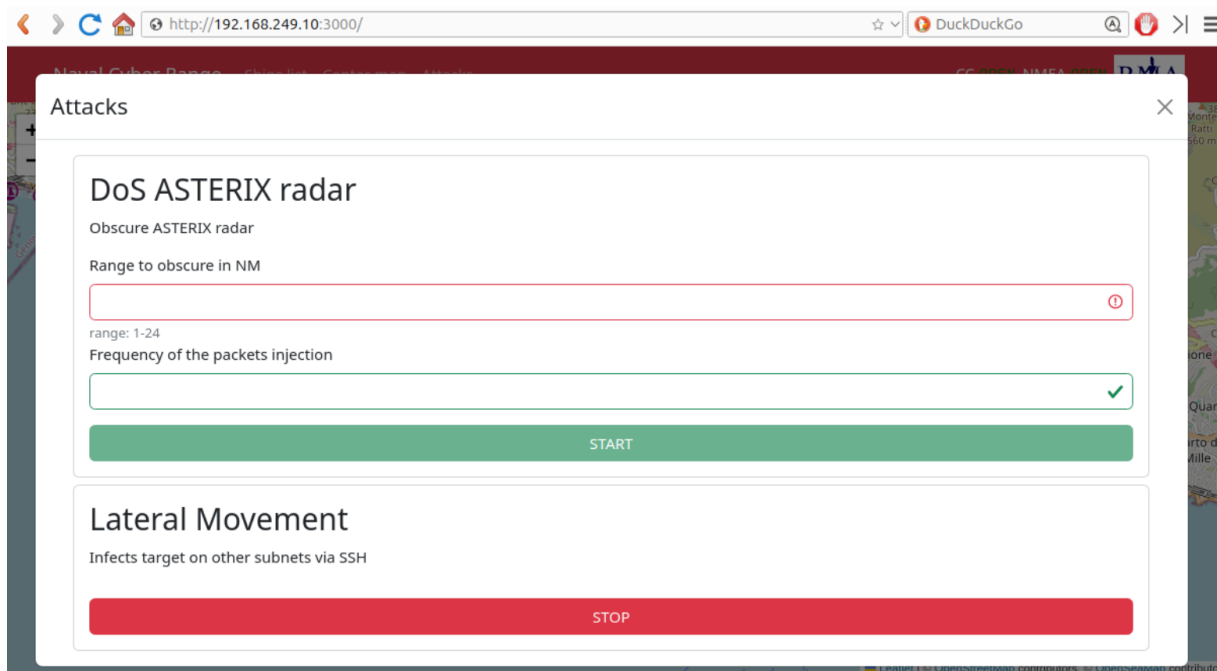


Figure 5.12. Attacks to launch from the radar desktop machine by the cyber range manager



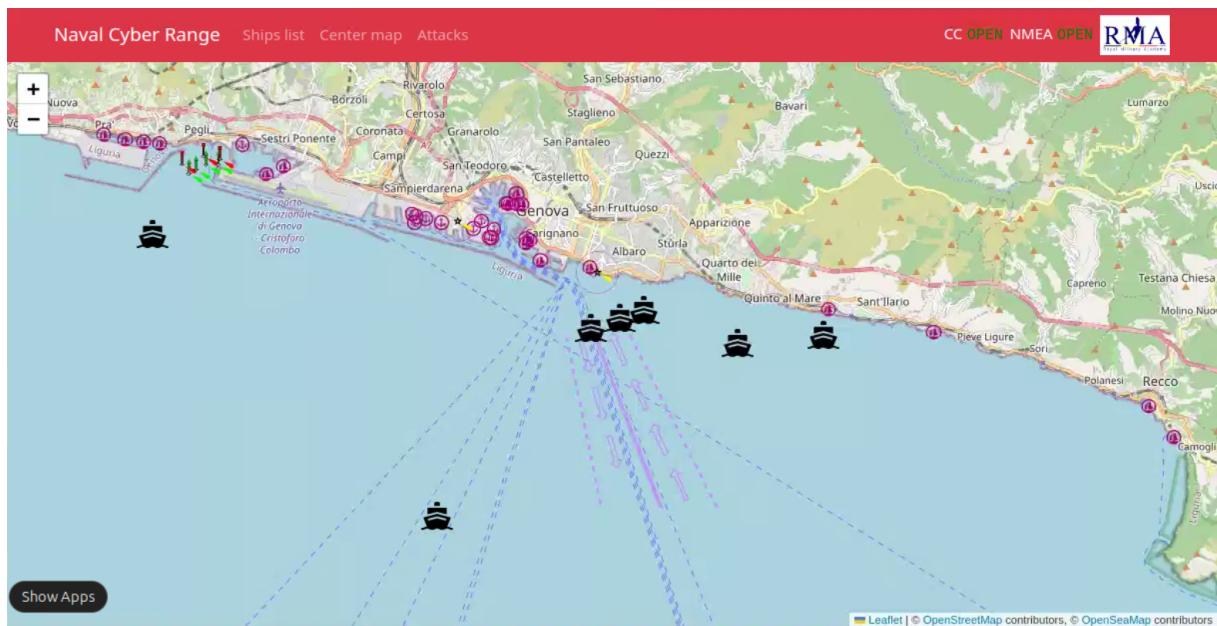


Figure 5.13. Cyber Range Manager GUI with map and ship positions

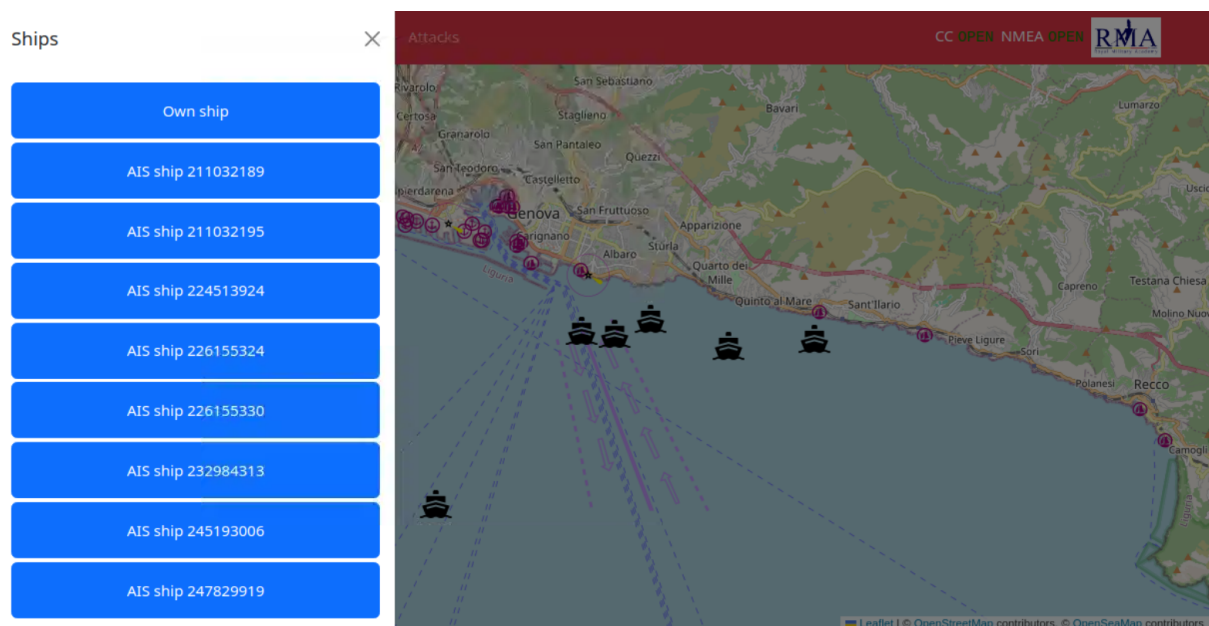
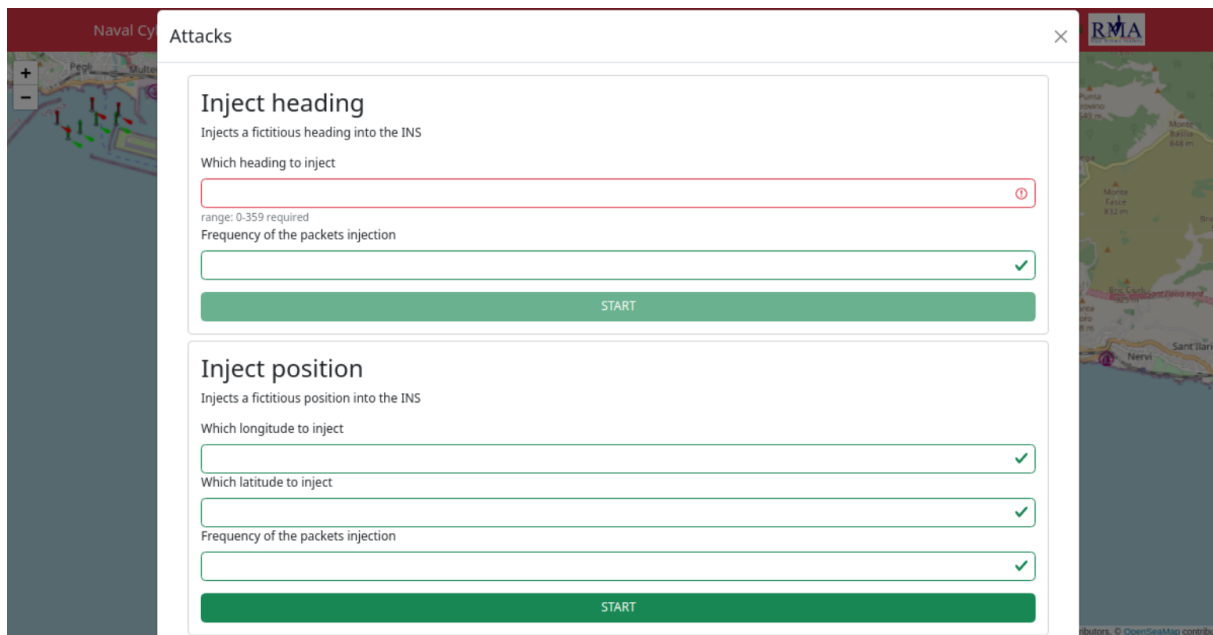
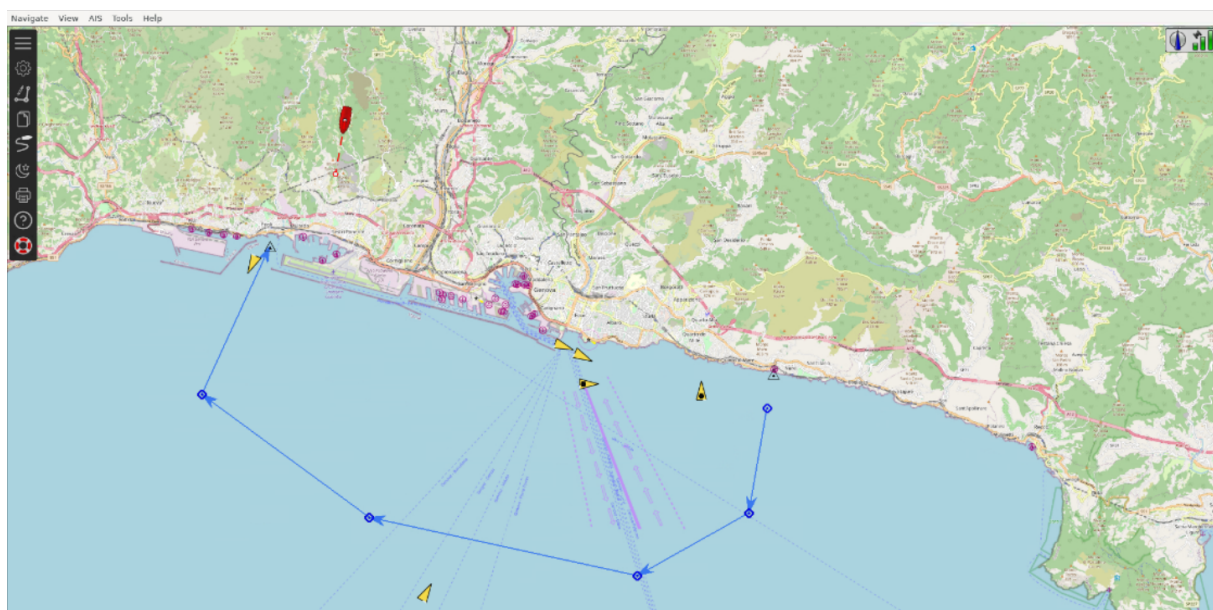


Figure 5.14. Cyber Range Manager GUI with ship list



**Figure 5.15.** Attacks to launch from the IBMS server machine by the cyber range manager



**Figure 5.16.** WECDIS under GPS spoofing attack



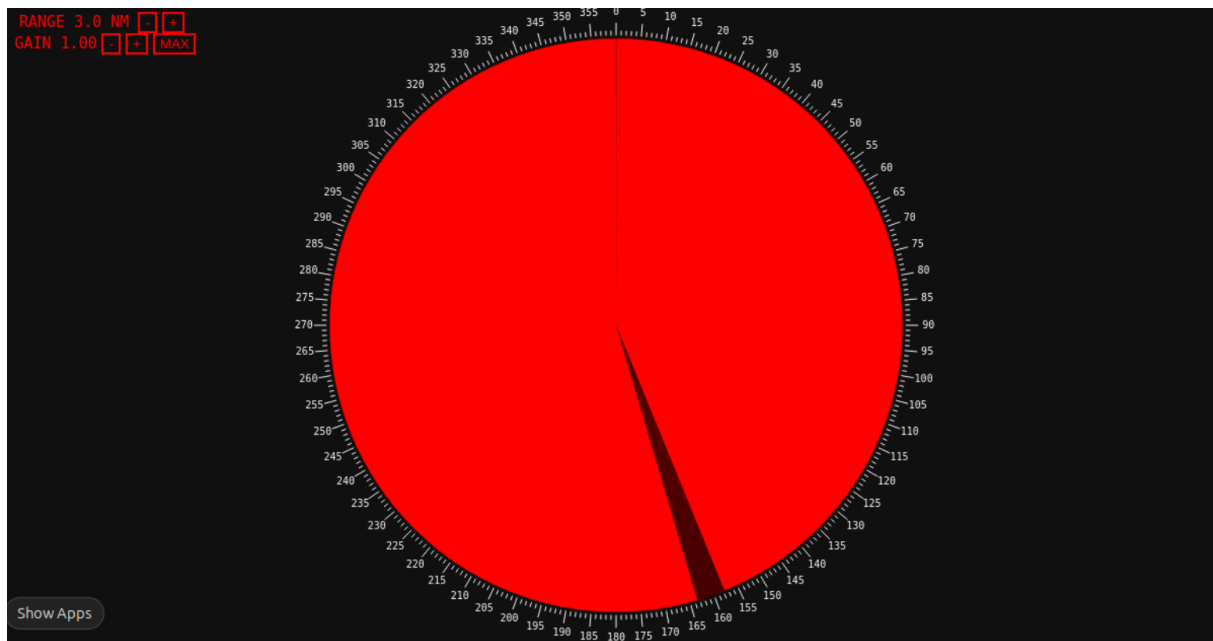


Figure 5.17. ASTERIX radar under DOS attack

### 5.7.3. Expected Trainee Response and Forensic Investigation

Following the execution of the GPS spoofing and radar Denial of Service (DOS) attacks, the trainees are expected to perform a series of actions to detect, neutralize, and analyse the intrusion. These actions form a critical part of the learning outcomes, reinforcing technical reflexes and investigative procedures essential in responding to cyber threats within operational environments.

#### Detection and Removal Objectives

To effectively mitigate the simulated malware attack, the trainee is expected to follow a sequence of response actions:

1. **Detect the malicious process:** Begin by identifying any suspicious processes running in the background. In this scenario, the malware disguises itself under an unconventional process name.
2. **Halt the malicious activity:** Once the suspicious process is confirmed, it must be promptly terminated to prevent further execution or spread within the system.
3. **Investigate malware-related files:** The infection typically results in the download and storage of malicious components on the local file system. These artifacts should be located as part of the containment phase.
4. **Handle the malware files appropriately:** Depending on the investigation scope, the malicious files should either be securely deleted or preserved in a controlled environment for deeper forensic examination.

#### Forensic Investigation (Advanced)

To enhance understanding of the attack's origin and behaviour, trainees should conduct a basic forensic analysis by reviewing system activity logs:

1. **Determine the source of infection:** Investigate how the malware was initially introduced, typically by identifying download activity through tools commonly used to retrieve remote files.
2. **Reconstruct the malware timeline:** Examine relevant system logs to trace the sequence of events tied to the malware's execution, installation, and any system-level interactions it may have triggered.



## 6. Testing and Evaluation

### 6.1. Functional Testing and Validation

The latest version of the project has undergone comprehensive testing to verify that all core functionalities operate as expected across the simulated cyber range. The following subsections present the validated components of the infrastructure, the graphical interfaces, and the cyber attack scenario.

#### 6.1.1. Infrastructure and Networking

- Each virtual machine functions correctly and delivers the services described in Section 5.1.3.
- All virtual machines can access the internet through the simulated network's NAT gateway router.
- Network connectivity is fully operational: all machines within the simulation can ping each other.
- Email communication between trainee desktop VMs and the cyber range manager is functional via the internal mail server.
- Scenario files specific to each VM correctly start and stop the required containers.
- Graphical interfaces are accessible via direct IP addresses or domain names resolved by the local DNS server.
- The cyber range manager is the only participant able to access the restricted attack GUI.
- The ship simulation within the NATS virtual machine works as intended and successfully injects relevant data into the message queue and JetStream key-value store.
- Containers requiring access to simulation data can retrieve it correctly from the message queue and key-value store.
- Containers communicate with each other where inter-container interaction is necessary.

#### 6.1.2. Graphical User Interfaces

All graphical user interfaces (GUIs) were tested for correct user interaction and data flow. The following behaviours have been confirmed:

- The ship simulator correctly displays the vessel's position, the surrounding environment, and nearby ships. The HUD display can be toggled off.
- ASTERIX and Navico radar GUIs present accurate radar imaging based on the ship's surroundings.
- Radar interfaces allow functional interaction with range and gain controls.
- In the Navigation Instruments GUI, the helm and throttle controls effectively adjust the rudder angle and engine power, modifying the ship's heading and speed.
- Autopilot mode can be successfully activated for both heading and speed control; the ship adjusts accordingly.
- The Steering Gear System (SGS) GUI provides real-time status of system components. Changes made via the navigation GUI are reflected in the SGS, and the pumps activate as required. Both pumps can be independently enabled and disabled.

- The WECDIS interface displays the current state of the ship accurately and allows seamless map navigation.
- Waypoints can be set in WECDIS, enabling autopilot tracking mode. The autopilot detects this and adjusts ship movement accordingly. Navigation Instruments GUI correctly displays the TRACK status.

### 6.1.3. Cyber Attack Scenario

The cyber awareness scenario, described in Section 5.7, has also been fully tested. The following outcomes were confirmed:

- The cyber range manager can send HTML-formatted phishing mails using Thunderbird.
- Trainees correctly receive the mail and the embedded phishing link is rendered properly by Claws Mail's HTML plugin.
- Clicking the phishing link redirects to an external site, from which a malware installer is downloaded and executed.
- The installer downloads the malware source code to disk and runs the process under the name `I_control_your_ship` in the mode associated with the host machine.
- The malware connects to the command and control server and displays the correct attack options in the manager's GUI depending on the infected host.
- Each attack (lateral movement, radar DOS, GPS spoofing) launched by the manager has the intended effects.
- Restoration and cleanup commands executed by trainees successfully terminate the malware and restore system functionality.

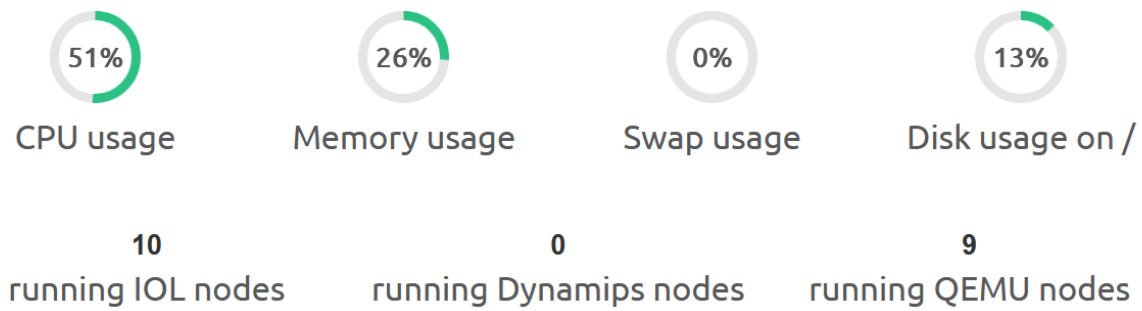
## 6.2. Performance Evaluation and Resource Usage

An important aspect in assessing the viability of the proposed naval cyber range is its performance with respect to system resource consumption. Among the different resources, CPU availability is the most limiting factor in the current implementation.

Within EVE-NG, each virtual machine is executed as a fully emulated operating system, inherently requiring a minimum dedicated CPU allocation. While the use of Podman containers has allowed the project to minimize the number of necessary virtual machines, the full deployment of the simulated lab still requires a total of 20 CPU cores to support the existing VMs.

Allocating more CPU per VM, particularly for the Ubuntu desktop machines used by the trainees, would improve overall responsiveness and stability. Furthermore, increased CPU capacity would also allow the addition of new machines, enabling the support of more crew roles or system functionalities. However, as indicated in Section 4.1.1, the current hardware platform provides only 24 physical CPU cores, making further expansion currently unfeasible.

Figure 6.1 illustrates the estimated system resource usage as reported by EVE-NG during the normal operation of the naval cyber range. This includes all virtual machines and network devices displayed in the topology presented in Figure 5.1, as well as all containers launched on their respective hosts with the ship simulation running.



**Figure 6.1.** Resource Usage on the EVE-NG Host by the Naval Cyber Range

As shown in the figure, CPU usage maintains an average around 50%, with observed peaks exceeding 75% during intensive operations. In contrast, both RAM and disk storage usage remain stable and within safe operational thresholds, with respectively 26 and 13 percent of usage. This confirms that the allocated 128 GB of RAM and 10 TB of disk capacity are more than sufficient to support the platform's needs under current conditions.

These performance observations suggest that, while CPU availability is the primary bottleneck for scaling, the memory and storage configurations are appropriately dimensioned for future feature expansion or increased scenario complexity.

### 6.3. Cyber Awareness Training Session and Evaluation

To evaluate the usability and effectiveness of the developed naval cyber range for cyber awareness training purposes, a dedicated training session was organized with a group of volunteer trainees. A complete cyber awareness scenario was prepared for this session, incorporating the full attack sequence described in Section 5.7.

This hands-on session served as a valuable opportunity to assess not only the functional state of the cyber range but also its practical application in a training context. It provided insights into several critical dimensions, including:

- The overall usability and accessibility of the cyber range platform from the trainee perspective;
- The technical robustness and ease of access to the cyber range virtual machine environment with a dedicated training setup;
- The logistical flow and practical management of the scenario during a live training session;
- The effectiveness, clarity, and engagement of the cyber awareness scenario in achieving its learning objectives.

Feedback and observations gathered during this session serve as an important foundation for improving both the scenario design and the underlying infrastructure. It marks a significant step in validating the cyber range as a useful tool for structured awareness training and future research.

#### 6.3.1. Cyber Awareness Training Setup and Deployment Environment

For the duration of the cyber awareness training session, a dedicated setup was deployed in the IT laboratory of the Cylab department at the Belgium Royal Military Academy. This room is equipped with a large six-panel display wall and a local network composed of multiple Ubuntu desktop machines. A key advantage of this environment is that these machines can directly access to the research network, which allows seamless access to the EVE-NG server hosting the naval cyber range.

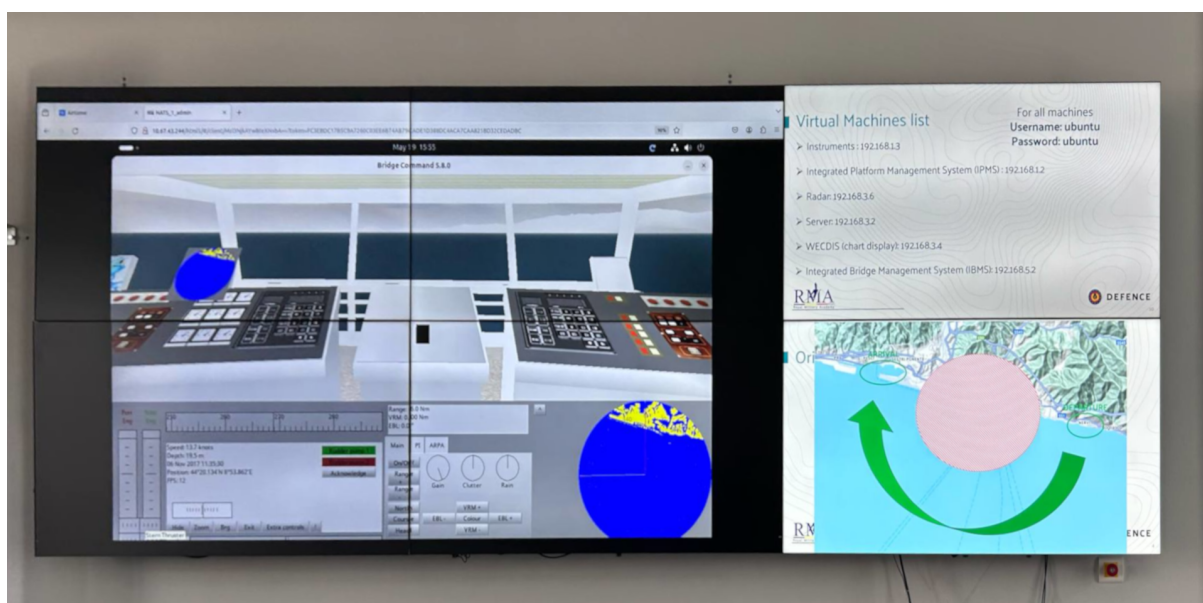
While the EVE-NG Professional Edition allows multiple users to connect to the same lab simultaneously, this feature is not available in the Community Edition used for the project. Nevertheless, a workaround was implemented: by opening the EVE-NG lab on a single machine and sharing the URLs and access tokens of the virtual machines, web browsers of other computers can still access VMs. In practice, a host management file was prepared and transferred to the other machines via a USB key<sup>1</sup>.

It should be noted that to avoid conflicts or unpredictable behaviour, a given virtual machine within the simulation should only be accessed by a single hardware machine at a time.

## Training Session Setup

The following configuration was used during the training session:

- Four panels of the large display wall were used to present the **bridge view of the ship simulator**, providing trainees with an immersive visual experience of the simulated maritime environment (see the left side of Figure 6.2).
- Two panels of the large display wall were reserved for displaying **briefings and scenario-relevant information**, such as threat intelligence updates or mission guidance (see the right side of Figure 6.2).
- Three Ubuntu desktop machines were allocated to **trainees**, each representing a specific **crew role within the naval cyber range** (see Figure 6.3).
- One Ubuntu desktop machine was used by the **cyber range manager** to access the EVE-NG interface, supervise the virtual machines, and operate the scenario control tools within the management VM (see Figure 6.4).



**Figure 6.2.** Setup with one large screen for ship simulation bridge view and briefings

<sup>1</sup>This method allows participants to access the environment using a pre-authenticated session link, bypassing the need for concurrent logins within EVE-NG.



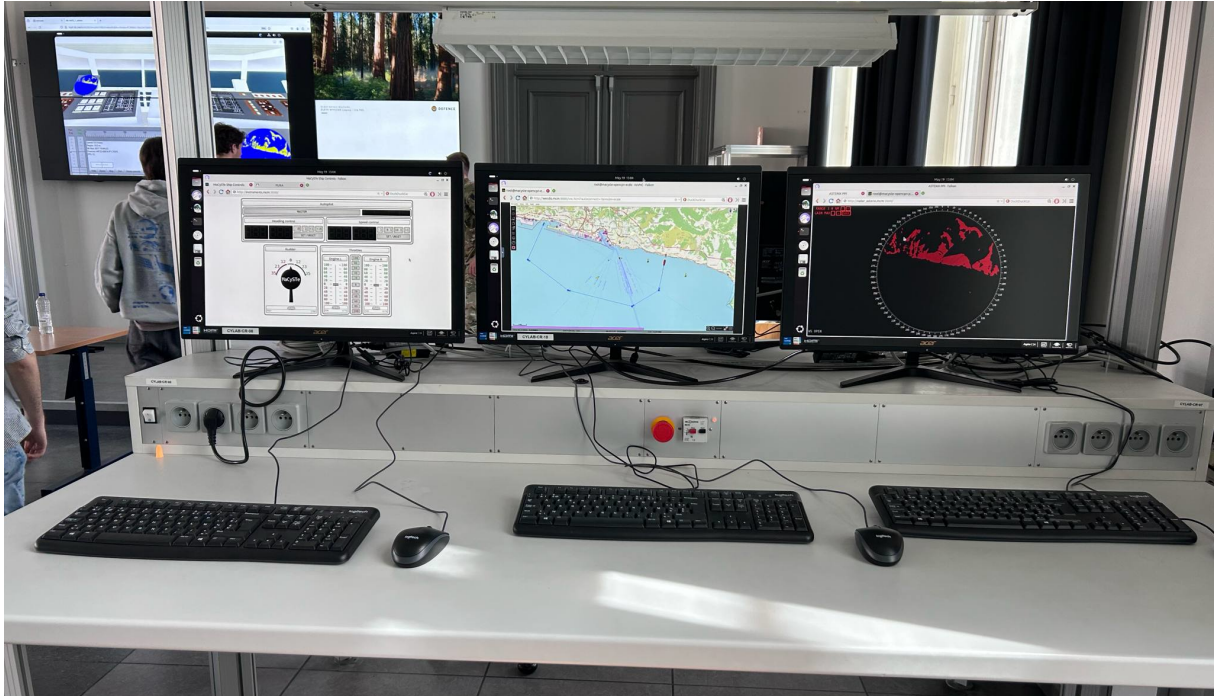


Figure 6.3. Setup with three machines for the trainees

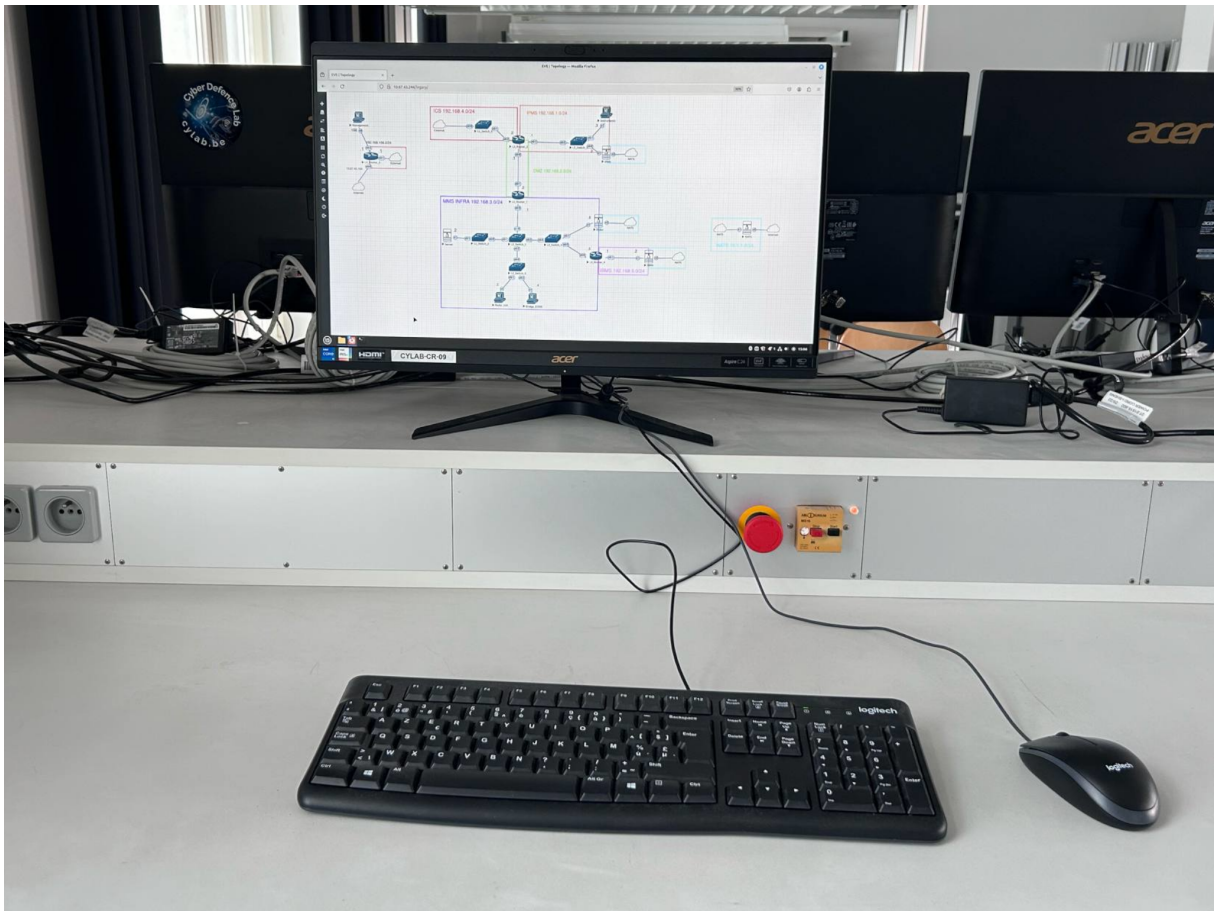


Figure 6.4. Setup with one machine for the manager

### 6.3.2. Execution of the Cyber Awareness Scenario with Volunteer Trainees

In the scenario developed for the cyber awareness training with volunteer participants, trainees were tasked with navigating from the Nervi anchorage to the western breakwater of the Genoa port. The mission briefing stated that the Genoa port was under control of an armed separatist faction, requiring the crew to follow a predefined route circumventing the port. The enemy situation included fast-patrol boats and cyber threats such as potential WECDIS chart corruption and radar interference.

The session lasted approximately 1.5 hours, during which the steps shown in the timeline in Figure 6.5 were executed. Each scenario phase is detailed in the following section.

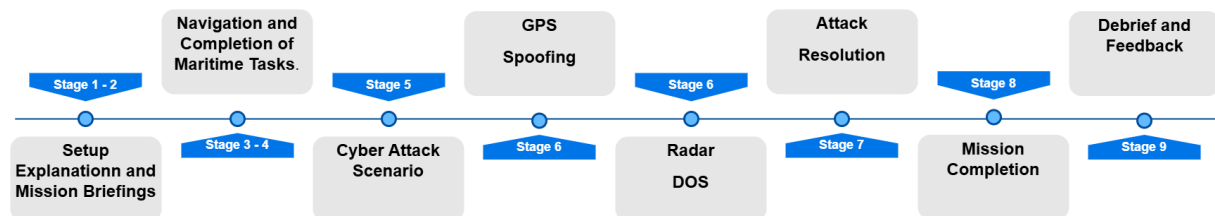


Figure 6.5. Timeline of the cyber awareness scenario execution

1. **Setup Explanation Briefing:** Trainees were introduced to the training setup, services available within their virtual machines, and the various GUI interfaces. A PowerPoint presentation used during this briefing is available in Appendix E.3.
2. **Mission Briefing:** A contextual briefing was given outlining the mission objectives, map overview, critical locations, potential threats, and crew role assignments. A picture of the session is shown in Figure 6.6. A PowerPoint presentation used during this briefing is included in Appendix E.4.
3. **Mission Start:** Trainees began the navigation route and familiarized themselves with their respective GUI interfaces based on assigned roles.
4. **Completion of Maritime Tasks:** During navigation, trainees received tasking mails from the cyber range manager (acting as crew manager). These emails required them to complete various navigation-related operations and respond with confirmation and data. Figures 6.7 and 6.8 illustrate this activity. The full mail library is provided in Appendix E.2.
5. **Cyber Attack Scenario:** Midway through the mission, the cyber range manager sent the phishing email described in Section 5.7, embedded among other routine emails. Clicking the link triggered the malware installer and launched the multi-stage cyber attack described in Section 5.7.
6. **GPS Spoofing and Radar DOS:** Upon infection of the designated machines, the manager launched the GPS spoofing attack from the attack GUI in the management VM (Figure 6.9). Trainees observed the GPS spoofing on the WECDIS and initiated response procedures (Figure 6.10). Navigation continued using radar data only. After several minutes, the manager launched the ASTERIX radar DOS attack, forcing the trainees to rely solely on the Navico radar (Figure 6.11).
7. **Attack Resolution:** A system restoration mail was sent to all trainees, prompting them to identify and remove the malware using the steps in Section 5.7.3. They were also asked to submit a report summarizing the attack. Hints were provided by the manager orally or by mail if needed. Figure 6.12 shows trainees in the process of identifying the malicious process.
8. **Post-Attack Navigation Tasks and Mission Completion:** Following malware eradication and attack report redaction, the trainees received new tasking mails from the crew manager and continued operations until the ship reached the designated endpoint, putting an end to the mission.
9. **Debriefing:** After completion of the mission, a debriefing was held during which the cyber range manager discussed performance highlights and areas for improvement.
10. **Participant Feedback:** Trainees were provided with a feedback form link via mail, accessible from within their VM. The results of this feedback, regarding the naval cyber range in general and the cyber awareness scenario, are analysed in the next section.



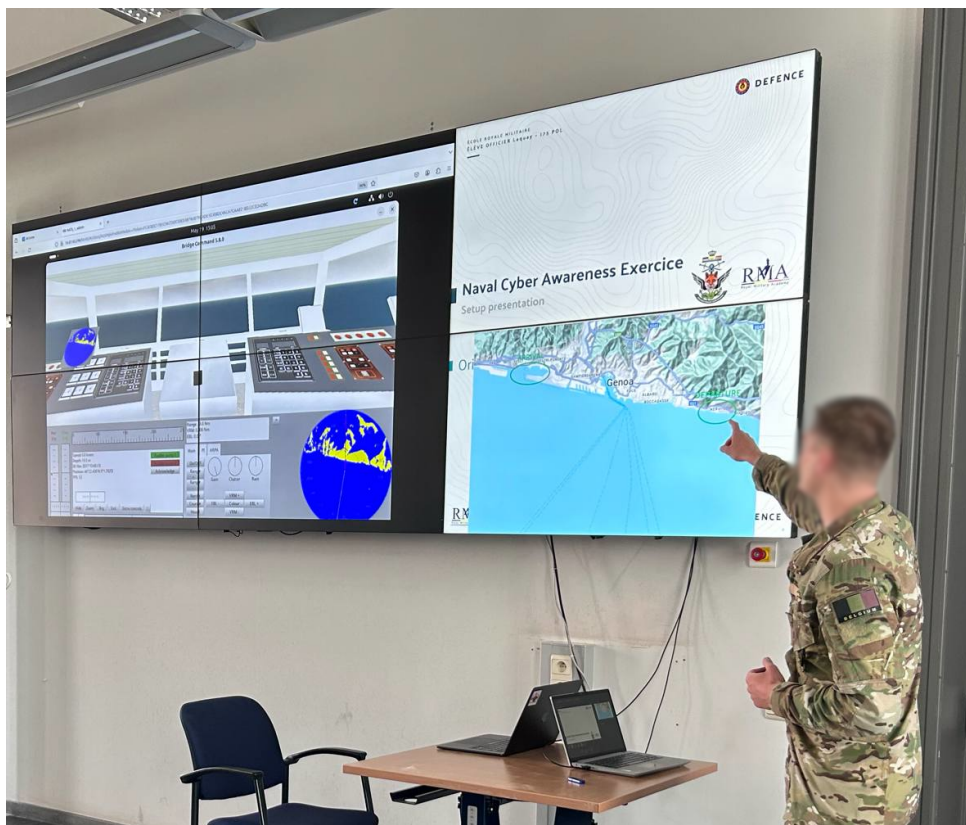


Figure 6.6. Setup explanation and mission briefing before the scenario

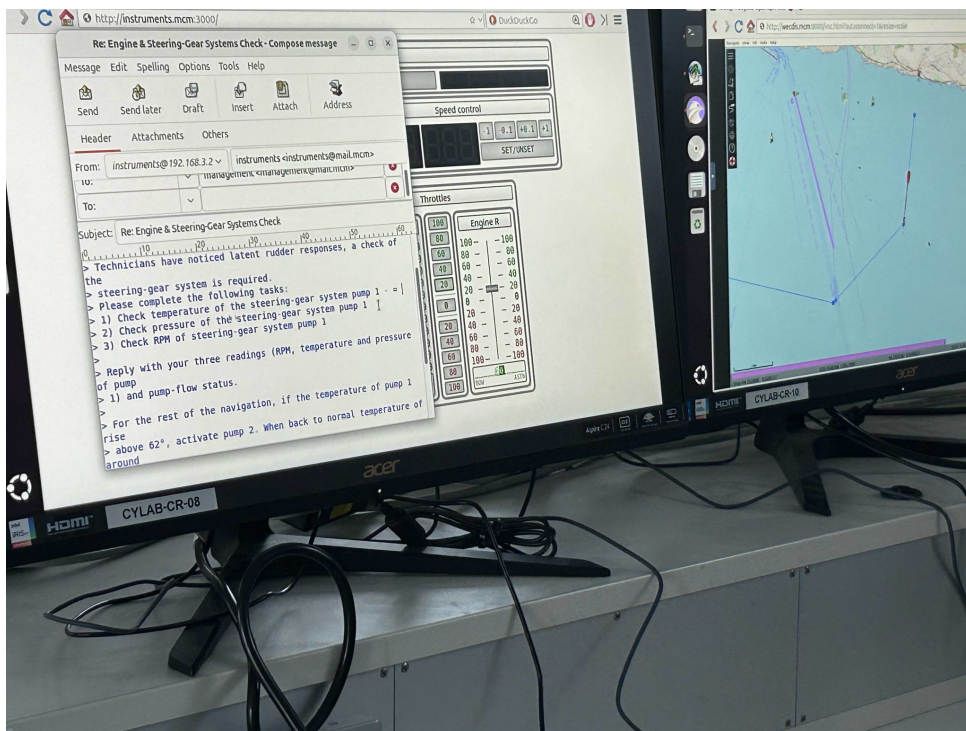
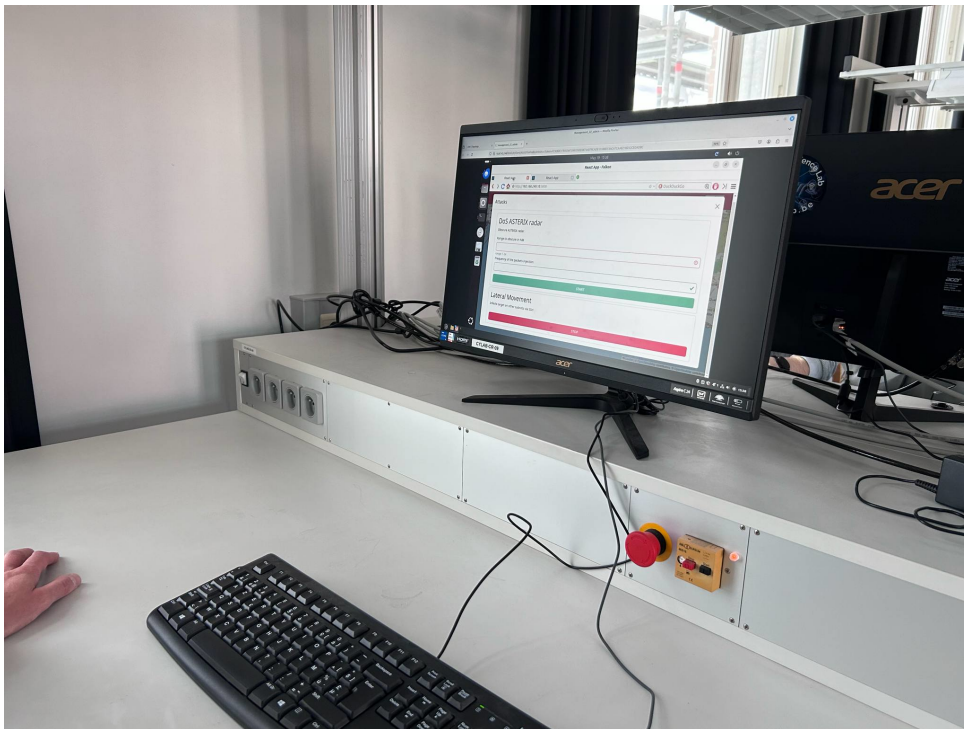


Figure 6.7. Mail received by a trainee with tasks related to his function



**Figure 6.8.** Completion of their respective tasks by the trainees



**Figure 6.9.** Launch of the cyber attacks on the attack GUI by the cyber range manager

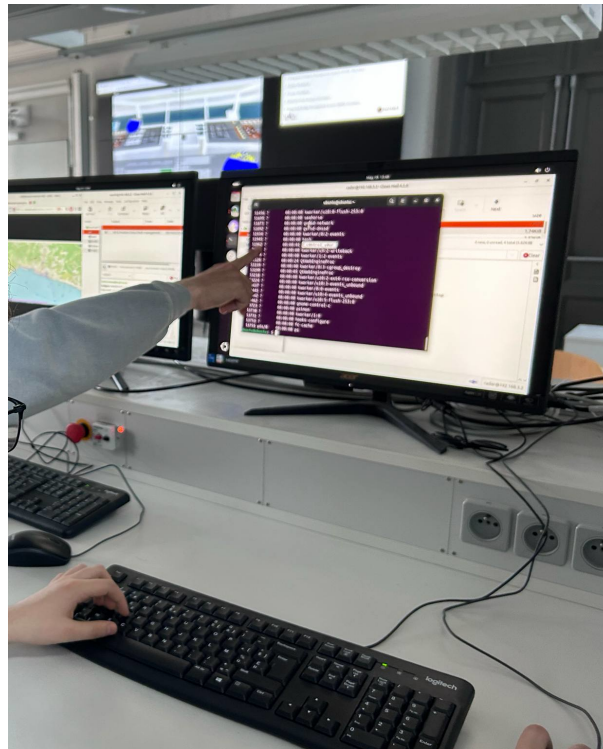




**Figure 6.10.** Trainee reacting against a GPS spoofing attack on the WECDIS



**Figure 6.11.** Trainee facing a DOS of his ASTERIX radar



**Figure 6.12.** Removal of the malicious processes by the trainees

### **6.3.3. Session Outcome and Observations**

The scenario unfolded smoothly and convincingly, offering a high level of realism well adapted to the maritime operational context. The integration of mission-oriented maritime tasks throughout the session proved highly effective in maintaining participant engagement and simulating crew dynamics. These tasks not only anchored the session in operational reality but also encouraged continuous communication and coordination among the trainees.

The introduction of the cyber-attack midway through the mission created a controlled stress environment, offering a close approximation of real-world operational conditions. Trainee reactions to this disruption demonstrated both situational awareness and adaptability. The interaction model between the trainees and the organiser (acting as the crew manager) was particularly effective, ensuring realism through consistent communication, timely hints, and scenario-based feedback loops.

Even though it was not originally planned, the presence of an additional supervisor acting as the ship's captain brought significant added value to the session. Through effective animation and active involvement, this role enhanced trainee engagement and played a key part in maintaining pressure during the attack phase. For future iterations, assigning such a role by default is strongly recommended to reinforce immersion and operational tension when the cyber range manager is too busy managing the scenario.

The resolution of the attacks was carried out competently by the trainees, including a well-handled post-incident analysis phase. This reflective process allowed them to correctly identify and understand the root causes of the disruptions, particularly the radar DOS and erroneous map coordinates resulting from malware pivoting to a server host. Throughout the scenario, the trainees maintained focus on the mission objectives, displaying a strong sense of team collaboration and resilience in responding to both technical and operational challenges.

Overall, the session demonstrated the viability of the naval cyber range as a training and awareness platform and confirmed the relevance of the implemented scenario in fostering both technical understanding and teamwork under cyber pressure.

### 6.3.4. Feedback from the Trainees Regarding the Cyber Awareness Scenario and Usability of the Naval Cyber Range

As mentioned in Section 6.3.2, following the naval cyber awareness training session with volunteer participants, feedback was collected through an online form. The purpose of this feedback was to evaluate the naval cyber range and the execution of the training scenario from the perspective of the end users.

Participants were asked to rate a series of statements on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree), based solely on their experience using the simulation. This approach ensured that the collected responses reflected the usability, clarity, and realism of the scenario as perceived during the session.

A summary of the feedback form, including the list of questions and the corresponding average scores, is provided in Appendix E.5.

**Positive Feedback** The feedback from the trainees highlights several strengths of the naval cyber range and confirms its relevance as a cybersecurity awareness training tool. The overall usability of the environment was positively received, with trainees finding the access procedure intuitive and the user interfaces accessible. The mission flow and scenario design kept participants engaged, and the use of mail for communication proved to be both realistic and effective. The cyber attack sequence was well understood, and the difficulty level was deemed appropriate, striking a good balance between challenge and achievability.

**Areas for Improvement** However, some areas were identified as needing improvement. System performance, particularly the responsiveness of the virtual machines, was reported as suboptimal. This can be addressed by further optimizing resource allocation or reducing the graphical load on desktop VMs. This problem of limiting CPU resources has already been discussed in Section 6.2. Additionally, the usefulness of the network topology presentation was rated poorly, suggesting that it was not necessary to go into more technical details at the setup presentation briefing. Certain malware remediation steps, such as file tracing and process identification, were seen as more difficult, which may warrant additional hints or in-scenario guidance for future sessions, especially if trainees are expected to carry out basic forensic analyses in real time.

**Conclusion** In summary, the cyber range demonstrated strong potential in terms of immersion, learning outcomes, and scenario coherence, with targeted adjustments recommended to enhance technical fluidity and instructional clarity.

## 6.4. Exportability and Future Reusability of the Project

As highlighted throughout the previous sections, exportability, reusability, scalability, modularity, and the potential for future improvements have been essential guiding principles during the development of the naval cyber range. These criteria significantly influenced architectural choices and the overall project design.

The objective of ensuring exportability and reusability appears to be successfully met. The entire project can be reproduced in a matter of hours on a fresh machine or in a cloud environment using only the configuration files and source code made available on the project's GitHub repository<sup>2</sup>, provided that the installation and implementation instructions detailed in this document are followed accurately.

To further enhance this exportability in the future, it would be beneficial to include a dedicated step-by-step installation guide directly within the repository. Such documentation would simplify deployment for external users and support broader adoption and contribution to the platform.

---

<sup>2</sup><https://github.com/LaquayL/RMA-Naval-Cyber-Range>



## 7. Discussion

### 7.1. Assessment of Objectives Fulfilled

As formulated in Chapter 1, the main objective of this thesis was to address the lack of controlled environments for training, testing, and simulating cyber threats in the maritime and naval domain. To meet this need, the goal was to develop a realistic and extensible warship simulation environment in the form of a naval cyber range, specifically tailored to the network architecture of the new Belgian Mine Countermeasure (MCM) warships. A central challenge throughout the project was to strike a balance between fidelity and abstraction, ensuring the preservation of critical operational characteristics while allowing for practical implementation within limited simulation resources.

By evaluating the final implementation against the sub-objectives and contributions outlined in Section 1.3, the following conclusions can be drawn:

- The project successfully delivered a fully operational naval cyber range prototype.
- The implemented architecture fulfils core requirements by modelling a realistic yet simplified version of onboard systems, inspired by the network architecture of the Belgian MCM vessels. The network produces credible maritime traffic and uses real-world protocols, supporting practical training and research applications.
- The platform demonstrates strong modularity and exportability. Its open structure and GitHub-based deployment facilitate reuse, adaptation, and future integration of advanced functionalities such as AI-driven cyber defence or live scenario adaptation.
- While the initial objective was to provide a threat injection framework and a scenario library, the project exceeded expectations by integrating and validating a complete cyber awareness scenario during a real-world training session. This demonstration with volunteer trainees confirmed both the functional and pedagogical value of the cyber range.

This work lays a solid foundation for future research, operational preparation, and technological innovation in the field of naval cybersecurity training.

### 7.2. Strengths and Limitations of the Current Work

As demonstrated in the previous section, the developed solution effectively meets the core objective of this thesis. However, despite its demonstrated value, the current implementation of the naval cyber range also presents several limitations. This section offers a balanced discussion of both the strengths and constraints of the project in its current state.

One of the most notable strengths lies in the platform's modularity and scalability, as discussed in Section 7.1 and further detailed in Section 6.4. The architecture has been designed to facilitate straightforward extension, allowing for additional systems, roles, and scenarios to be integrated with minimal restructuring. Moreover, the choice of the EVE-NG framework has proven highly appropriate, supporting both structured cyber awareness training and future experimental research in the maritime cybersecurity domain.

On the other hand, the current implementation is primarily intended as a proof of concept rather than a production-ready training platform. As such, the level of system complexity is deliberately simplified. While the simulated network is inspired by the real architecture of the new Belgian MCM warships, only a limited number of representative systems have been implemented. Furthermore, the environment

currently does not incorporate cybersecurity mechanisms such as firewalls, VLANs, intrusion detection systems, secure authentication, or access control policies. Similarly, some systems critical to the specific operational context of MCM warships, such as Mine Avoidance Sonar, Multi Mission Drone System (SMMD), or military-specific components like weapon systems and encrypted communications, are not yet included.

Another significant limitation concerns the scale and operational logistics of the current setup. At present, the naval cyber range can support only a single training session at a time, accommodating up to three trainees. While this is sufficient for demonstration and evaluation purposes, it presents a major constraint for broader training deployments. Moreover, as highlighted in Section 6.3.3, each session requires the involvement of at least two qualified personnel—a cyber range manager and an additional supervisor to guide and animate the scenario. The session's duration, which spans approximately 90 minutes, further compounds the issue. If the platform were to be scaled for comprehensive crew-wide training, new strategies would need to be developed to optimize participant throughput, reduce staffing demands, and streamline execution without compromising the quality or fidelity of the training experience.

Despite these current limitations, the naval cyber range developed in this project establishes a robust and extensible foundation. Its modular design and flexible architecture enable future enhancements, whether to support additional crew roles, integrate complex systems, or expand session capacity. With relatively minimal structural changes, missing cybersecurity mechanisms and operational features can be progressively introduced to bring the platform closer to real-world deployment standards. As such, this proof-of-concept does not mark the end point, but rather the beginning of a scalable and adaptable tool for both maritime cyber training and research, capable of evolving in line with emerging threats, technologies, and training demands.

### **7.3. Practical Relevance for Cyber Awareness Training**

One of the key goals of the proof-of-concept naval cyber range developed in this thesis was to assess its relevance for executing cyber awareness training specifically within the maritime domain. This objective has been directly addressed through the execution of a real-life training session, in which the platform was used in a practical setting with live participants.

As summarized in Sections 6.3.3 and 6.3.4, the exercise demonstrated the effectiveness of the cyber range as a training tool. The platform successfully engaged the participants, provided realistic interaction with operational systems, and supported the detection and resolution of a simulated cyber attack, thereby validating its educational and operational value. The results clearly confirm that such a cyber range constitutes a strong and adaptable solution for enhancing training capabilities in maritime environments where cyber threats are increasingly relevant.

In addition, the high degree of modularity and flexibility in the implementation of the cyber awareness components opens the door to a wide variety of training scenarios. The architecture allows for quick adaptation or extension of functionalities, enabling the design of exercises at varying levels of complexity.

While the scenario implemented in this thesis was intended to demonstrate a medium level of cyber difficulty, targeting participants with a solid IT background and operational understanding but without being cybersecurity specialists (such as an IT officer aboard a naval vessel), the cyber range is equally capable of supporting more advanced and intricate scenarios. Conversely, it can also accommodate more simplified awareness exercises where cyber incidents are handled externally, and participants are only exposed to the effects and consequences of attacks, with no expectation of technical remediation.

Consequently, the naval cyber range can be tailored to meet the needs of diverse target audiences, ranging from non-specialist crew members with limited cybersecurity knowledge to technically advanced trainees or professional cybersecurity teams. This flexibility significantly enhances its long-term value as both an instructional tool and a research platform, supporting evolving training requirements and advancing the field of maritime cybersecurity.



## 7.4. Potential for Research in Maritime Cybersecurity

A second major objective of the thesis project was to establish a coherent and relevant foundation for conducting research in the field of maritime cybersecurity. To enable such studies, the simulation environment must ensure a high level of fidelity and similarity with actual shipboard IT and OT architectures. This includes generating realistic network traffic and reproducing system behaviours that closely mirror those of real naval platforms.

As discussed in Section 7.2, the current implementation remains somewhat simplified when compared to the full complexity of the Belgian MCM warships' onboard systems. Additionally, penetration testing and other advanced cybersecurity evaluations are not yet feasible due to the absence of security enforcement components in the current version.

Nevertheless, the naval cyber range as implemented already offers a solid foundation for cybersecurity research, particularly as a proof of concept for the integration of AI-driven methods. Despite its abstraction, the simulated systems and containers exhibit behaviour with a high degree of realism. Importantly, the network traffic generated within the environment uses real-world maritime protocols, such as NMEA for the IBMS, Asterix and Navico for radar data, and Modbus for IPMS components, enhancing the credibility and applicability of the simulation.

Moreover, the container-based implementation ensures that each functional component is assigned a unique IP address, even when hosted on the same virtual machine. From the perspective of other systems or users within the simulated environment, each container thus behaves as an independent networked device. This level of segmentation is particularly valuable for testing detection and monitoring solutions under realistic conditions.

As a result, the current naval cyber range is already capable of supporting meaningful research applications. These include the development and evaluation of AI-powered anomaly and intrusion detection systems specific to maritime networks, as well as the generation of high-quality, protocol-specific datasets for training machine learning models. With further refinement and expansion, the platform has strong potential to become a central tool for experimental research in the naval cybersecurity domain.

These capabilities position the naval cyber range as a valuable tool not only for education but also for advancing applied research in maritime cybersecurity.



## 8. Future Work and Improvements

Following the discussions and evaluations presented in Chapter 7, several limitations and areas for enhancement have been identified within the current implementation of the naval cyber range. At the same time, these observations also highlight promising directions for further development.

The objective of this chapter is to propose concrete improvements that could address the current weaknesses, and to outline future work that may be carried out in direct continuation of the research and development initiated in this thesis. These reflections are divided into two main perspectives: the first considers the naval cyber range as a platform for cyber awareness training, while the second addresses its potential for more advanced cybersecurity research in the maritime domain.

### 8.1. Enhancing Cyber Awareness Training

Taking into account the training outcomes presented in Section 6.3.3, the participant feedback discussed in Section 6.3.4, and the broader reflections on the relevance for training of the naval cyber range outlined in Section 7.3, three primary areas of improvement have emerged for enhancing the cyber range's effectiveness in cyber awareness training: (1) increasing available CPU resources per virtual machine to improve user experience and system responsiveness; (2) strengthening instructional clarity and scenario management to support smoother training execution; and (3) addressing the current lack of scalability, as the platform presently supports only a limited number of trainees per session, limiting its capacity to efficiently train larger crews. Conversely, strong opportunities were also identified, particularly in terms of the platform's modularity and the ease of implementing new cyber threat scenarios.

#### 8.1.1. Use of More Powerful Hardware or Cloud Solutions

One straightforward yet impactful improvement would be to deploy the naval cyber range on more powerful hardware. Increasing the number of CPUs available to virtual machines, especially the desktop VMs used by trainees, would greatly enhance interface responsiveness and overall user experience. Furthermore, higher CPU availability would enable the implementation of a greater number of systems within the simulation, thereby expanding the range of crew roles represented during training sessions. This would significantly increase the training capacity of the cyber range, making it possible to involve larger or more functionally diverse crews in a single scenario.

Alternatively, the cyber range could be deployed in the cloud, as discussed in Section 4.1.2. While cloud-based deployments offer scalability and remote accessibility, the financial cost associated with commercial cloud providers often remains significantly higher than that of local hardware solutions.

#### 8.1.2. Extending the Library of Available Maritime Cyber Threats

Thanks to the modular structure of the project, it is technically straightforward to expand the library of available cyber awareness scenarios. New training exercises could incorporate a variety of threat types, target systems, attack vectors, and remediation strategies.

Such extensions would broaden the scope of the naval cyber range, allowing it to address the needs of different audiences, from novice maritime personnel to trainees with more advanced cybersecurity knowledge. Furthermore, a diverse scenario library would enable comparative studies on the effectiveness of different training methodologies.

### **8.1.3. Advanced Scenario Management Tools**

Another major area for enhancement involves improving the management tools available to the cyber range manager during training sessions. In the current version, many tasks, such as sending instruction emails, launching attacks, and tracking trainee progress, are handled manually.

Automating these aspects would not only streamline session management but also improve consistency across repeated scenario runs. Inspired by the Cyber-MAR project (see Section 2.3.3), the integration of structured scenario timelines and automated scoring mechanisms would offer clear advantages. Such mechanisms would allow managers to track trainee performance objectively and facilitate evaluations or certifications.

Beyond improving the quality of each session, automation could also significantly increase the training capacity of the cyber range. A first step would be to reduce the need for two qualified personnel per session by developing fully automated, event-driven cyber awareness scenarios that no longer require a cyber range manager to operate in real-time. In this setup, only one supervisor would be needed to oversee the trainees.

Looking further ahead, this automation potential opens the door to a larger-scale vision: a centralized naval cyber awareness training centre where multiple training sessions are run in parallel, each triggered and executed autonomously. A single cyber range manager could monitor the status and progress of all ongoing sessions from a central command interface, ensuring efficient and scalable delivery of training across a broad user base.

### **8.1.4. AI Integration in Cyber Training**

Building upon the scenario management improvements, artificial intelligence could be integrated into the platform for real-time monitoring and feedback during training sessions. For instance, AI models could be trained to detect specific user actions, such as stopping a packet injection or removing a malware process, by analysing system logs or network traffic.

This would not only support the cyber range manager in assessing performance but also enable the development of adaptive training environments that respond dynamically to trainee behaviour. In the continuity of Section 8.1.3, AI could also play a central role in automating key aspects of scenario execution, such as generating real-time adapted attack paths based on user responses, automatically scoring trainee performance, and providing personalised feedback or post-session lessons.

Looking toward more innovative and immersive applications, an original vision for AI use in this context would be the development of an intelligent virtual ship captain, displayed life-sized on a screen and capable of fully animating a training session. This AI-driven figure would serve as both guide and supervisor, engaging trainees, simulating operational pressure, offering hints when necessary, and dynamically managing many aspects of the scenario flow. Such a system would eliminate the need for a human supervisor-animator, vastly increasing training session scalability while preserving, or even enhancing, the realism and pedagogical value of the exercise.

Altogether, these AI-driven developments represent a natural extension of the project's automation objectives, pushing the naval cyber range towards unprecedented levels of autonomy, adaptability, and training throughput.

## **8.2. Enabling Maritime Cybersecurity Research**

Building on the conclusions drawn in Section 7.4, the naval cyber range developed in this thesis presents strong potential for enabling research in the field of maritime cybersecurity. While the current implementation reveals some limitations, particularly in terms of network complexity and the number of integrated systems, it also demonstrates several promising opportunities. These include the realistic behaviour of implemented components, proper use of maritime communication protocols, and a modular architecture that supports scalable experimentation.

### **8.2.1. Enhanced Realism and Complexity**

A key improvement to elevate the research capability of the cyber range lies in expanding the scope of implemented systems, devices, and security mechanisms. Increasing the architectural complexity to more closely resemble the real-world network of Belgian MCM warships would enable more nuanced and credible research.

This enhancement would open avenues for investigating specific protocols, mine warfare systems, and military-specific technologies under various conditions. It would also allow researchers to study cross-system interactions and evaluate the cascading effects of cyber incidents or defensive countermeasures. Ultimately, a more sophisticated architecture would lead to more insightful findings and higher-quality contributions to the maritime cybersecurity research domain.

### **8.2.2. Integration of Machine Learning**

As previously highlighted in Section 7.4, the current version of the naval cyber range already provides a suitable foundation for the integration of machine learning (ML) components.

The platform's modular design enables flexible deployment of AI agents. These can be implemented as individual containers, embedded in existing virtual machines, or deployed on dedicated hosts within the simulated network. This flexibility supports experimentation with a range of AI architectures and deployment models.

Given the unique nature of shipboard systems, the naval domain offers opportunities for highly specialised AI applications. For example, a trained model could detect anomalies in autopilot behaviour, such as heading drift or unexpected route deviation, caused by potential attacks or internal malfunctions. Similarly, the system could be trained to recognise timing-based anomalies in deterministic maritime protocols, enabling early detection of communication disruptions or injection attacks.

### **8.2.3. Traffic dataset creation**

The naval cyber range also provides an ideal environment for the generation of high-fidelity network traffic datasets tailored to maritime contexts. The traffic produced by onboard systems, based on real protocols like NMEA, Modbus, Asterix, and Navico, offers an authentic basis for such data collection.

Furthermore, capturing traffic during simulated missions executed by human trainees allows for the generation of rich datasets combining operational activity with contextual events. These datasets can be used for analysis or to train AI and ML models. Additionally, scenarios involving active cyber attacks can be executed to collect labelled anomalous traffic, facilitating the development of supervised learning solutions.

## **8.3. Long-Term Vision for a Full-Scale Maritime Cyber Range**

The naval cyber range developed in this thesis is currently positioned as a proof of concept. However, from the outset, it has been deliberately designed with scalability and future expansion in mind. A natural question thus arises: could this prototype evolve into a full-scale, production-grade naval cyber range, comparable to those described in Section 2.2?

The answer is not straightforward, as it largely depends on the intended scope and level of realism required from such a platform. An analysis of existing operational-grade maritime cyber ranges reveals two recurring characteristics. First, many of them are hybrid in nature, combining simulated systems with real hardware components. Second, these projects are often the result of collaborative efforts involving multiple institutions or industry partners. The integration of hardware is often necessary to overcome the limitations of pure simulation, especially when attempting to replicate the intricate behaviour of complex onboard systems that are difficult to model or emulate with high fidelity.

Moreover, developing a maritime cyber range of this level of sophistication typically requires extensive expertise across multiple domains. Individual development becomes increasingly challenging as the range grows in complexity. In this context, collaborative contributions, each offering a specialised subsystem or simulation module, often lead to the creation of state-of-the-art platforms.

Nonetheless, the current cyber range demonstrates considerable potential for further development without yet encountering those critical bottlenecks. Its modularity, fidelity, and protocol accuracy form a strong technical foundation for increased realism and broader system coverage. If additional support were to be secured, for example, through technical insights or validation from stakeholders such as Naval Group, the platform could evolve into a substantially more advanced and operationally relevant training and research environment.

In summary, while evolving this prototype into a full production-grade cyber range would be a complex endeavour, the foundational work carried out in this thesis lays the groundwork for such a transformation, particularly if bolstered by institutional collaboration and incremental development.

## 9. Conclusion

### 9.1. Summary of Work

This thesis addressed a critical gap in maritime cybersecurity: the lack of realistic, structured environments tailored to naval contexts for training, simulation, and research. As naval platforms increasingly rely on interconnected IT and OT systems, their vulnerability to cyber threats has grown. Yet, awareness and preparedness remain limited, particularly regarding attacks targeting operational technology, deterministic protocols, and mission-critical maritime systems.

To tackle this challenge, the thesis designed, implemented, and validated a proof-of-concept naval cyber range that simulates the digital landscape of a modern Mine Countermeasure (MCM) warship in a resource-efficient yet realistic way. The architecture uses EVE-NG for virtual machine orchestration and Podman containers for lightweight, modular deployment. Systems communicate via maritime-relevant protocols like NMEA, Modbus TCP, ASTERIX, and proprietary radar formats. A central ship simulator, powered by Bridge Command, generates coherent navigation data shared through a clustered NATS message queue.

The range integrates core operational components, DNS, mail services, navigation, radar interfaces, steering gear simulations, and autopilot control, all accessible via web-based GUIs. Threat injection and monitoring are supported through an attacker interface to ensure scenario realism.

A major contribution of this work is the simplification of the complex Belgian MCM warship architecture into a representative simulation. This involved distilling essential functions without compromising interaction fidelity. The result is a modular platform that supports integration of new scenarios and components.

The range was validated through a live cyber awareness session at the Royal Military Academy. Volunteers completed a scenario involving phishing, malware deployment, lateral movement, and GPS/radar attacks. The session demonstrated the platform's capacity for structured training, with positive feedback confirming its usability and effectiveness.

### 9.2. Final Reflections

This thesis delivers not only a functional prototype but also a foundation for future naval cyber ranges supporting both training and research. The modular, scalable architecture accommodates future developments, including AI-based detection, increased complexity, and real-time performance analysis.

Though currently a proof of concept, the range already supports diverse scenarios and research. Simplified coverage and absence of integrated security mechanisms reflect deliberate design choices favoring accessibility and extensibility.

Feedback from live testing highlighted engagement, educational impact, and operational realism. Trainees interacted with shipboard systems, experienced cyber disruptions, and executed remediation within a mission context, affirming the range's value to the Belgian Defence and beyond.

Ultimately, this project underscores the need for domain-specific cyber ranges. Maritime systems are too unique and critical for generic simulation tools. By bridging this gap, this work opens the door to future training, certification, and research into cyber resilience at sea.





## A. MCM Warship Network Architecture Additional Content

### A.1. MCM Warship IBMS Sub-Networks and Systems Overview

Table A.1 gives a non-exhaustive summary of the systems hosted by the different IBMS sub-networks.

Sub-Network	System	Function / Description
Inertial Navigation System (INS)	Inertial Navigation Unit (INU)	Provides navigation data based on motion sensors and gyroscopes without reliance on external references.
	Navigation Data Distribution System (NDDS)	Distributes navigation data to relevant on-board systems.
	Control Computing Unit (CCU)	Central processor for managing and integrating navigation information.
	Attitude and Heading Reference System (AHRS)	Provides attitude (pitch, roll) and heading data based on inertial sensors.
	Secure Sync	Ensures precise and secure time synchronization by authenticating and encrypting time signals, and protecting against spoofing or jamming, including GPS/GNSS sources.
Dynamic Positioning System (DPS)	Operator Stations	User interfaces to monitor and control dynamic positioning.
	Control System Electronic Cabinets	Host DPS control logic and interfaces with propulsion.
	Thruster Cabinets	House power and control units for ship thrusters.
	Portable Remote Unit	Allows remote and portable control of dynamic positioning.
Navigation Civil System (NCS)	Multifunction Consoles	Display navigation, radar, and ship data.
	Warship Electronic Chart Display and Information System (WECDIS)	Displays digital nautical charts and routes.
	Radar/Automatic Radar Plotting Aid (Radar/ARPA)	Detects, tracks, and predicts movement of nearby vessels.
	Conning Display	Centralized navigation and control interface on bridge.
	X-band and S-band Radars	Surface search radars for short and long-range detection.
	Warship Automatic Identification System (WAIS)	Identifies and tracks nearby ships.
	DGNSS and Military GPS (MIL GPS)	Provide precise global positioning data.

Continued on next page

Sub-Network	System	Function / Description
	Echo Sounder and Multi-Beam Sounder	Measure water depth below hull using sonar.
	Electromagnetic Log (EM Log)	Measures ship's speed through the water.
	Doppler Velocity Log (DVL)	Measures speed over ground using Doppler shift.
	Bridge Overhead Display (BOD)	Displays main navigation and weather info above bridge consoles.
	Automatic Weather Station	Provides wind and meteorological data to ship systems.
	Magnetic Compass	Offers a mechanical backup to electronic navigation systems.
	Ship Proximity Management System (SPMS)	Assists in collision avoidance by evaluating nearby obstacles.
	Voyage Data Recorder (VDR)	Records ship's navigation, communication, and control data.
Masterclock System (MSK)	Masterclock	Provides and synchronizes time references for all systems via NTP.

**Table A.1.** MCM Warship IBMS Sub-Networks and Systems Overview

## B. Framework Selection Additional Information

### B.1. Comparison Between Cloud Services and Owned Hardware Cyber Range Solutions

Aspect	Cloud Services	Owned Hardware
<b>Development Phase</b>		
Initial Cost	Low cost (pay-as-you-go, no capital investment)	High upfront investment for hardware
Scalability	Instantly scalable based on demand	Limited to physical hardware available
Setup Time	Minutes to deploy environments	Days or weeks to acquire and set up hardware
Flexibility	Easily switch configurations, OSES, architectures	Requires manual reconfiguration or new hardware
Collaboration	Easy for distributed teams to access shared environments	Requires VPN or network configuration for remote access
Snapshot	Built-in snapshot and rollback features	Requires manual backup and restore mechanisms
<b>Production Phase</b>		
Availability	High availability and redundancy (99.99%+ SLAs)	Requires investment in redundant infrastructure
Scaling	Automatically scales with load	Needs manual scaling and potential downtime
Security	Managed by provider with compliance support	Full control, but full responsibility for security
Disaster Recovery	Built-in backups and geo-replication available	Must implement backup and DR solutions manually
Global Reach	Deploy in multiple regions easily	Deployment restricted to physical site(s)
Maintenance	Handled by cloud provider	Requires dedicated personnel and downtime planning
Long-term Cost	Can be high over extended periods	More cost-effective if hardware is used over many years

**Table B.1.** Comparison Between Cloud Services and Owned Hardware During Development and Production

As seen in Table B.1, during development phase, the main disadvantage of owned hardware is the initial investment being high, especially for substantial resource needs. However, this criterion is not relevant in the context of this project as the hardware is already available for research. Besides, the other disadvantages of owned hardware solutions, regarding scalability, flexibility, collaboration and snapshot, are not critical as they can easily be overcome by devoting a certain amount of extra time to the project. As for the setup time criterion, time is not an issue during project implementation.

Considering the production phase, most criterion are quite critical for a proper deployment for active training of personnel. Indeed, should the naval cyber range be integrated in training programs and used on a daily basis, it is of the utmost importance to provide at the same time a high availability,

security, disaster recovery, maintenance, etc. These important considerations can become difficult to handle without assigning permanently personnel to the corresponding infrastructures. In this context, even with the presence of higher long term costs, it could be convenient to move to a cloud based solution, way easier to implement in production and maintain.

## B.2. Evaluation of Available Tools and Frameworks for Cyber Range Platform Implementation

On the basis of the required features for the framework and the simulations needs, several frameworks can be considered for the development of the maritime cyber range. This section evaluate the possible usage of theses frameworks.

- **Cisco Packet Tracer<sup>1</sup>**: is educationally focused and lacks the flexibility for custom VM deployments or advanced simulations, making it unsuitable for realistic cyber attack-defense scenarios.
- **Mininet<sup>2</sup>**: focuses on SDN and lightweight emulation, but it is primarily CLI-driven and not suitable for broader system-level or multi-OS simulations.
- **VirtualBox<sup>3</sup> and VMware Workstation<sup>4</sup>**: offer full OS virtualization but do not natively support complex network topologies or multi-user management, and lack integrated network device simulation.
- **Proxmox VE<sup>5</sup>**: is a powerful virtualization platform with clustering and container support but is less intuitive for building network topologies visually, which is crucial for cyber range design.
- **Open Cyber Range<sup>6</sup>**: can provide a very complete and robust solution for developing a cyber range, but the configuration is very complex and the solution quickly becomes very cumbersome and time-consuming to implement.
- **Kypo<sup>7</sup>**: as for Open Cyber Range, can provide a very complete and robust solution for developing a cyber range, but the configuration is very complex and the solution quickly becomes very cumbersome and time-consuming to implement. [49]
- **GNS3<sup>8</sup>**: offers strong network emulation and GUI-based topology building but lacks built-in virtual machine support and full-featured OS simulation, limiting realism in cyber range scenarios.
- **EVE-NG<sup>9</sup>**: offers similar capabilities to GNS3, as well as the ability to simulate custom full operating systems and greater scalability with larger network topologies.

---

<sup>1</sup><https://www.netacad.com/cisco-packet-tracer>

<sup>2</sup><https://mininet.org/>

<sup>3</sup><https://www.virtualbox.org/>

<sup>4</sup><https://www.vmware.com/products/desktop-hypervisor/workstation-and-fusion>

<sup>5</sup><https://www.proxmox.com/en/products/proxmox-virtual-environment/overview>

<sup>6</sup><https://github.com/Open-Cyber-Range> & <https://documentation.opencyberrange.ee/docs>

<sup>7</sup><https://docs.crp.kypo.muni.cz/>

<sup>8</sup><https://docs.gns3.com/docs/>

<sup>9</sup><https://www.eve-ng.net/>

## C. Cyber Range Implementation and Network Configuration Details

### C.1. Device Images List and Installation Procedure

The images used later to build the Naval Cyber Range are the following:

1. Cisco IOL Switches: L2-ADVENTERPRISE-M-15.1-20140814.bin
2. Cisco IOL Routers: L3-adventerprisek9-15.5.2T.bin
3. Linux desktops: linux-ubuntu-desktop-24.04.1
4. Linux servers: linux-ubuntu-24.04.2-live-server-amd64

These images have to be stored on the EVE-NG server in /opt/unetlab/addons/iol/bin/ (1 and 2) and /opt/unetlab/addons/qemu (3 and 4). Instructions to properly setup the IOL images are available in the EVE-NG documentation<sup>1</sup> along with the upload instructions of Linux images<sup>2</sup>.

### C.2. Mail Infrastructure Installation and Configuration

#### C.2.1. Mail Server Installation and Configuration

The following instructions outline the installation and configuration steps required to set up a local mail server using **Postfix** and **Dovecot** on the Server virtual machine.

##### Step 1: Install Postfix

```
sudo apt update
sudo apt install -y postfix
```

##### Step 2: Configure Trusted Networks

Edit /etc/postfix/main.cf and add the private subnets of the simulated network to the mynetworks directive.

```
mynetworks = 127.0.0.0/8, 192.168.1.0/24, 192.168.2.0/24, 192.168.3.0/24
```

Restart Postfix to apply the changes:

```
sudo systemctl restart postfix
```

##### Step 3: Create Mail Users

Create user accounts that will be able to send and receive mail:

```
sudo useradd -m <username>
sudo passwd <password>
```

<sup>1</sup><https://www.eve-ng.net/index.php/documentation/howtos/howto-add-cisco-iol-ios-on-linux/>

<sup>2</sup><https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-linux-host-image/>

The used user accounts and password in the project implementation are the following:

- instruments instruments
- radar radar
- wecdis wecdis
- management management

#### Step 4: Enable IMAP via Dovecot

```
sudo apt install -y dovecot-imapd
```

#### Step 5: Configure Postfix for Maildir Delivery

Edit `/etc/postfix/main.cf` and add the following line:

```
home_mailbox = Maildir/
```

Then reload Postfix:

```
sudo systemctl restart postfix
```

#### Step 6: Configure Dovecot

Edit the file `/etc/dovecot/conf.d/10-mail.conf` and set:

```
mail_location = maildir:~/Maildir
```

Then edit `/etc/dovecot/conf.d/10-auth.conf` and set:

```
disable_plaintext_auth = no
```

Finally, restart the Dovecot service:

```
sudo systemctl restart dovecot
```

This configuration enables the local mail server to send and receive messages using IMAP, allowing access via mail clients within the simulated network.

### C.2.2. Mail Client Installation and Configuration

This section details the steps for installing and configuring mail clients on the trainee virtual machines. Due to resource constraints, **Claws Mail** is preferred for trainee systems. However, **Thunderbird** may be used when HTML email composition is required (e.g., on the Manager VM).

For each VM, installation is performed using the corresponding credentials listed in Appendix C.2.1.

#### Step 1: Install Claws Mail or Thunderbird

Update package sources and install the desired mail client:

```
sudo apt update
sudo apt install -y claws-mail
```

Alternatively, for Thunderbird:

```
sudo apt install -y thunderbird
```

## Step 2: Launch the Mail Client

After installation, locate and launch **Claws Mail** from the application menu. On first launch, the *New Mail Account* wizard will appear.

## Step 3: Account Configuration

Fill in the following details during the setup wizard:

- **User name:** <username>
- **Email address:** <username>@mail.mcm
- **Incoming protocol:** IMAP
- **IMAP server:** 192.168.3.2
- **Port:** 143, without SSL/TLS (lab environment)
- **Login:** <username>
- **Outgoing SMTP server:** Use the Postfix server at port 25

Complete the wizard and fetch a test message to validate the setup.

## Step 4: Enable HTML Rendering (Claws Mail Only)

To allow Claws Mail to render HTML content (e.g., links), install the lightweight HTML viewer plugin:

```
sudo apt install claws-mail-lite-html-viewer
```

Then open Claws Mail and navigate to:

Configuration → Plugins → Enable Web Browser View or HTML Viewer

Once activated, HTML content will be properly displayed within Claws Mail.

## Note

Thunderbird does not require additional plugins for HTML rendering and is used exclusively on the Manager VM for composing formatted emails.





## D. Naval Cyber Range Management Useful Information

### D.1. Naval Cyber Range Sub-network and Virtual Machine List

Table D.1 provides a list of all virtual machines deployed within the simulation environment, along with their relevant configuration information and resource allocation. The sub-network in which each VM is located is also indicated.

Sub-network	Name	Image	IP Address	CPU	RAM (MB)	Storage (GB)
MMS INFRA 192.168.3.0/24	Radar_GUI	linux-ubuntu-desktop-24.04.1	192.168.3.3	2	4096MB	35GB
	Radar	linux-ubuntu-24.04.2-live-server-amd64	192.168.3.6	2	4096MB	33GB
	Bridge_ECDIS	linux-ubuntu-desktop-24.04.1	192.168.1.4	2	4096MB	35GB
	Server	linux-ubuntu-24.04.2-live-server-amd64	192.168.3.2	2	4096MB	52GB
IPMS 192.168.1.0/24	Instruments	linux-ubuntu-desktop-24.04.1	192.168.1.3	2	4096MB	35GB
	IPMS	linux-ubuntu-24.04.2-live-server-amd64	192.168.1.2	2	4096MB	33GB
IBMS 192.168.5.0/24	IBMS	linux-ubuntu-24.04.2-live-server-amd64	192.168.5.2	2	4096MB	33GB
External 192.168.166.0/24	Management	linux-ubuntu-desktop-24.04.1	192.168.166.166	2	4096MB	35GB
NATS 10.1.1.0/24	NATS	linux-ubuntu-desktop-24.04.1	10.1.1.100	4	4096MB	35GB

Table D.1. Summary of the Virtual Machines in the Simulated Network

### D.2. Container Management Useful Commands

The following make commands are the most relevant for managing containers during development and execution:

**Build the container images defined in the scenario of a given virtual machine:**

```
sudo make build-containers SCENARIO_NAME=<VM_name>
```

**Build the Bridge Command ship simulator Flatpak on the NATS virtual machine:**

```
sudo make build-flatpaks SCENARIO_NAME=core_simulation
```

**Start the containers and create the Podman networks for the specified virtual machine scenario:**

```
sudo make up SCENARIO_NAME=<VM_name>
```

**Stop the containers and remove the Podman networks for the specified virtual machine scenario:**

```
sudo make down SCENARIO_NAME=<VM_name>
```

## D.3. Links to Graphical User Interfaces

### D.3.1. IP Addresses URLs

- Radar ASTERIX: 192.168.3.103:3000
- Radar Navico: 192.168.3.104:8080
- SGS HMI: 192.168.1.109:1881
- SGS master: 192.168.1.110:8080
- Instruments: 192.168.1.106:3000
- WECDIS: 192.168.5.102:8080
- Radar Attack: 192.168.249.10:3000
- WECDIS Attack: 192.168.249.11:3000

### D.3.2. Name Resolution URLs

- Radar ASTERIX: radar\_asterix.mcm:3000
- Radar Navico: radar\_navico.mcm:8080/vnc.html?autoconnect=1&resize=scale
- SGS HMI: sgs.mcm:1881
- SGS master: sgs\_master.mcm:8080
- Instruments: instruments.mcm:3000
- WECDIS: wecdis.mcm:8080/vnc.html?autoconnect=1&resize=scale

## E. Scenario Additional Material

### E.1. Example Solution for Eradicating Malware and Performing Initial Forensics Analysis

To meet the objectives of malware detection, removal, and initial forensic analysis, the following sequence of commands demonstrates a practical approach.

#### E.1.1. Malware Removal

##### Step 1: Identify the malicious process.

Look for a suspicious process named I\_control1\_your\_5hip:

```
ps aux  
# or alternatively  
ps -e
```

##### Step 2: Terminate the malicious process.

Forcefully stop the process using:

```
pkill -f I_control1_your_5hip
```

##### Step 3: Locate the malware files.

Search your home directory for any files related to the process:

```
find "$HOME" -name '*I_control1_your_5hip*'
```

##### Step 4: Remove the malware files.

Delete the files found in suspicious hidden locations (e.g., /.tmp/):

```
sudo rm -rf /.tmp/.I_control1_your_5hip
```

#### Forensic Investigation (Advanced)

##### Step 5: Identify the download origin.

If the malware was downloaded via curl, you can trace its origin with system logs:

```
sudo journalctl _COMM=curl
```

##### Step 6: Trace the malware installation and activity.

A filtered search through system logs can reveal the full sequence of execution and system interactions involving the malware:

```
sudo journalctl -b | grep -iE '(malware|I_control1_your_5hip)'
```

## **E.2. Scenario Tasking Mails**

### **Task 1 radar**

SUBJECT: Radar Calibration & Range Setting

Radar operator,

Outbound corridor is narrow. Perform the following immediately after being at least 3NM from the coast : 1) Check Radar Navico and raise range to 12 NM, then lower back to 6 NM. 2) Check Radar ASTERIX once Navico has cycled, adapt ASTERIX range to 6NM. 3) Adapt gain on ASTERIX radar to avoid excessive clutter.

Reply with screenshots of both radars' PPI displays correctly configured.

Crew manager

### **Task 1 wecdis**

SUBJECT: AIS & Position Cross-Check

WECDIS operator,

With heavy traffic south of our track, maintain collision avoidance vigil. Please complete the following tasks: 1) Check position of nearby ships. 2) Send me your current coordinates. 3) Send me the coordinates and AIS code of the nearest vessel.

Crew manager

### **Task 1 instruments**

SUBJECT: Engine & Steering-Gear Systems Check

Engine operator,

Technicians have noticed latent rudder responses, a check of the steering-gear system is required. Please complete the following tasks: 1) Check temperature of the steering-gear system pump 1 2) Check pressure of the steering-gear system pump 1 3) Check RPM of steering-gear system pump 1

Reply with your three readings (RPM, temperature and pressure of pump 1) and pump-flow status.

For the rest of the navigation, if the temperature of pump 1 rise above 62°, activate pump 2. When back to normal temperature of around 50° for both pumps, deactivate pump 2 to go back to normal operation mode.

Crew manager

### **Phishing radar**

SUBJECT: URGENT: Updated Tide Predictions for Genoa Passage

Radar operator,

Harbour Operations have just posted a revised tide forecast for today's run past the Western Breakwater. To maintain optimum steerage and engine thrust scheduling, please: 1) Consult this website <https://www.tide-forecast.com/locations/Genova/tides/latest> to view the latest high-tide and low-tide times at Genoa's Western Breakwater. 2) Report back the next high-water time and its predicted height.

Respond within 10 minutes so we can issue updated engine orders before we enter the narrow corridor.

Crew manager

## **Cyber report radar, wecdis, instruments**

SUBJECT: IMMEDIATE ACTION: SYSTEM RESTORATION & MALWARE ERADICATION

All stations,

The recent DOS on both radars and the spoofed WECDIS contacts have been confirmed as hostile cyber intrusions. We must regain full sensor and navigation fidelity before the flood tide slackens (in 45 minutes). Failure to restore systems promptly risks navigational error in the narrow corridor and jeopardizes the entire convoy schedule.

You have 30 minutes to: 1) Identify the root cause of the disruptions on your systems. 2) Disable the cause of the disruption to get back clear radar signal and correct WECDIS positioning. 3) Locate and delete permanently all unauthorized executables, scripts, or registry entries installed during the attack. 4) Confirm systems sanity by testing the proper functioning of the radar and WECDIS features. 5) Identify the different steps of the attack and the entry point for the malware installation on the different machines.

Immediately upon task closure, report completion of each step and any unresolved anomalies on the systems. Give also your conclusions conclusions on the course of the attack

Crew manager

### **Task 2 radar**

SUBJECT: Radar Sector Scan & Range Setting

Radar operator,

Prior to anchoring, perform the following tasks: 1) Set Navico radar range to 3 NM; Then ASTERIX to 3 NM. 2) Adjust ASTERIX gain to 1.1 for close-in contacts.

Send PPI screenshot and “Radar clear” once complete.

Crew manager

### **Task 2 instruments**

SUBJECT: Approach & Anchoring Preparations

Engine operator,

You are now at the entry to Genoa’s western anchorage.

Do not set engine power above 50% and reduce speed below 5 knots.

Reply with “Engine ready” for acknowledgement.

Crew manager

### **Task 2 wecdis**

SUBJECT: Final Position & AIS Report

WECDIS operator,

Upon arrival, send your exact current coordinates and confirm “WECDIS ready for anchoring.”

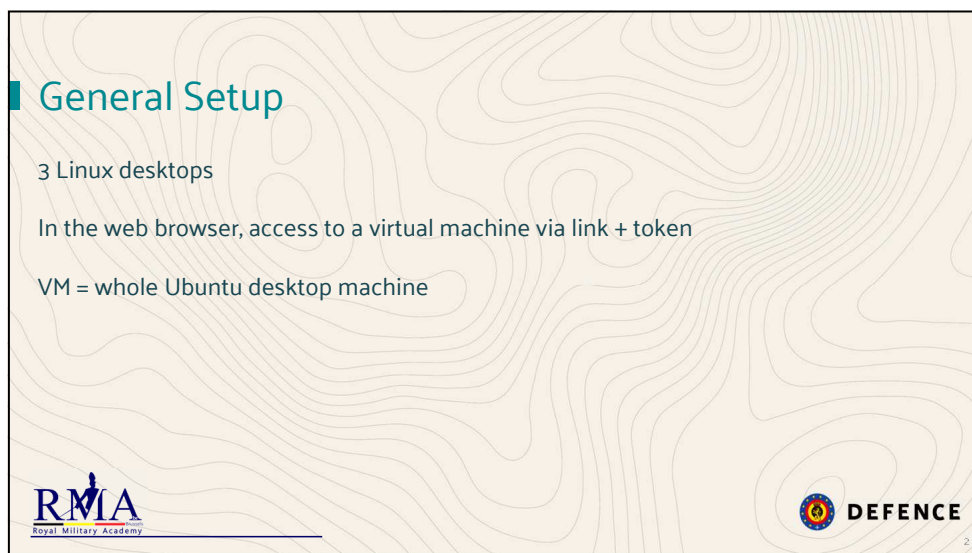
Crew manager

## E.3. Setup Explanation Briefing

21-05-25



1





2

## Useful Services

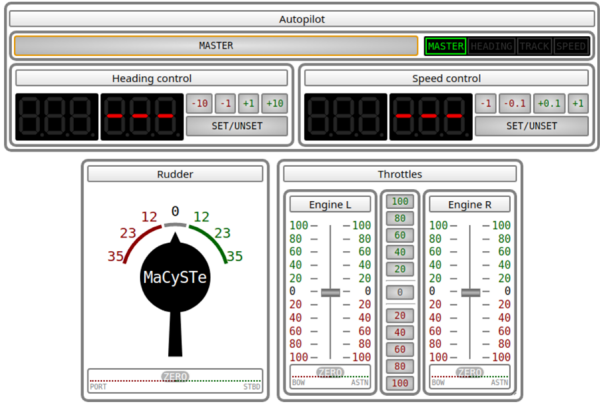


- Mail client “Claws”
- Web browser “Falkon” (Firefox not advised due to high resource consumption)
- Terminal

→ Communication of instructions by mail during the exercise

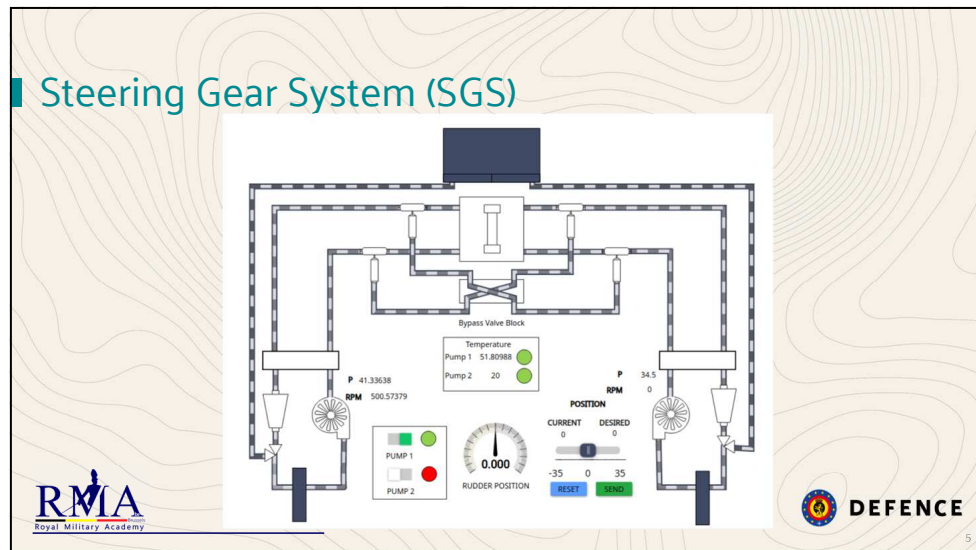



3

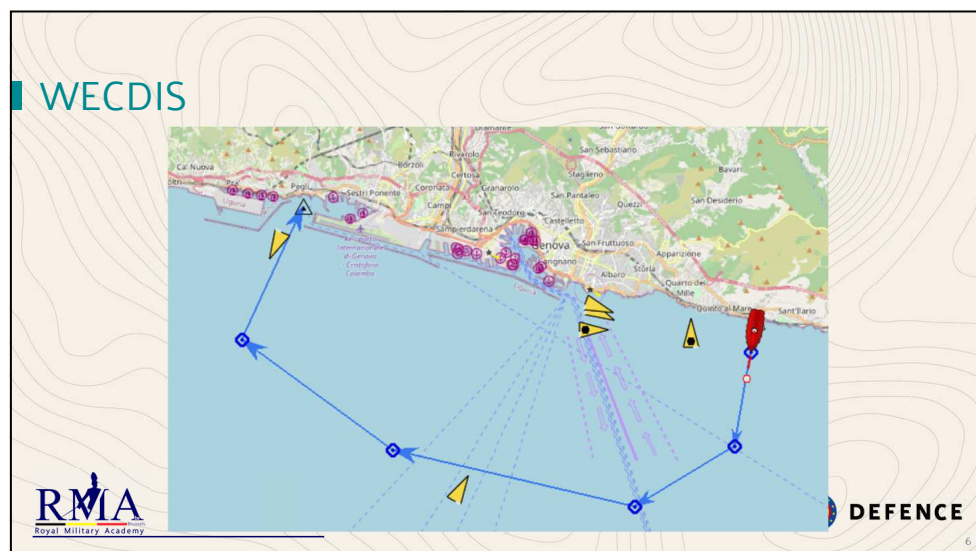
## Instruments

4

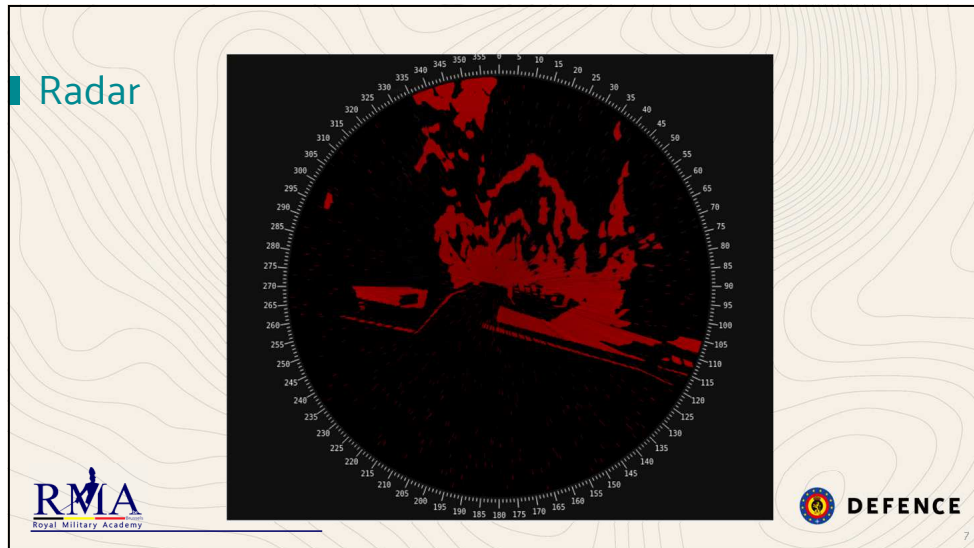


5

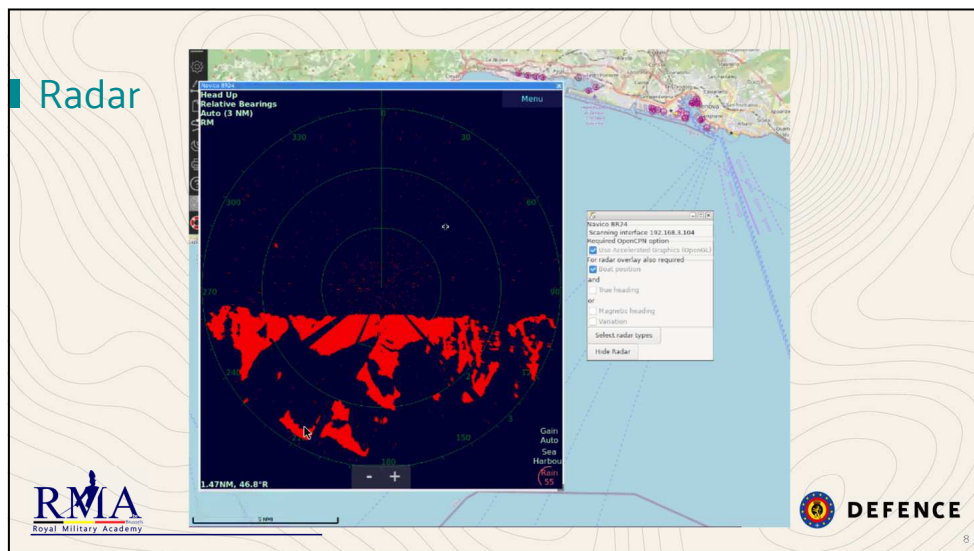


6

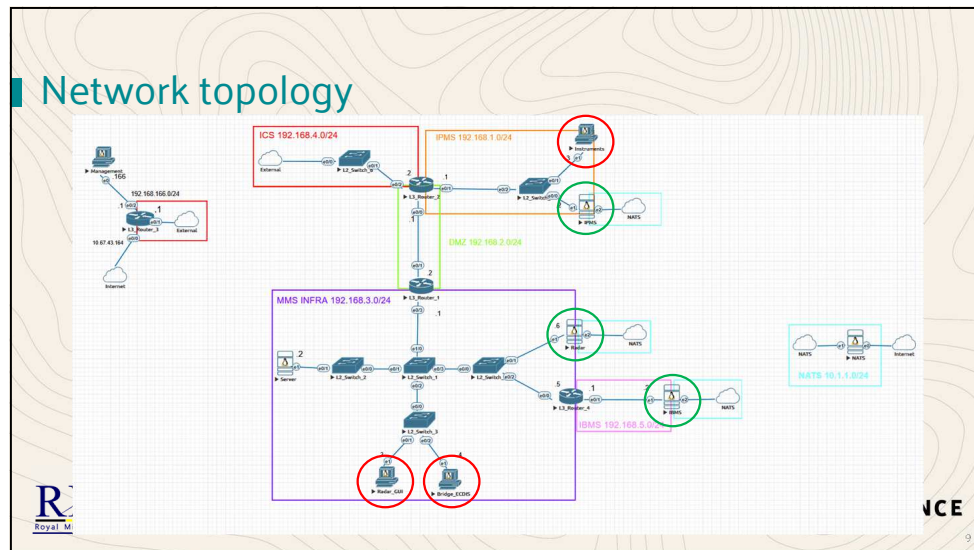




7



8



9

## Virtual Machines list

For all machines  
**Username: ubuntu**  
**Password: ubuntu**

- Instruments : 192.168.1.3
- Integrated Platform Management System (IPMS) : 192.168.1.2
- Radar: 192.168.3.6
- Server: 192.168.3.2
- WECDIS (chart display): 192.168.3.4
- Integrated Bridge Management System (IBMS): 192.168.5.2



**RMA**  
Royal Military Academy

**DEFENCE**

10

## Training agreements



1. Do not reboot or shutdown any machine
2. Do not modify or interact with Podman containers
3. Do not modify or interact with machine "Server"
4. Do not touch to directory "RMA-Naval-Cyber-Range"
5. Do not change VM network configuration
6. What you should find has distinct names



11

11

Question ? → Shoot

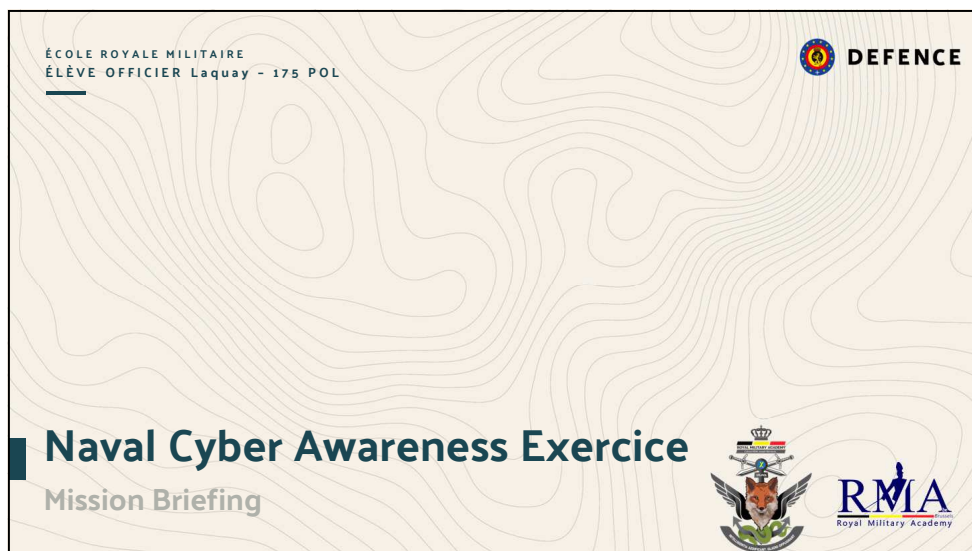


12

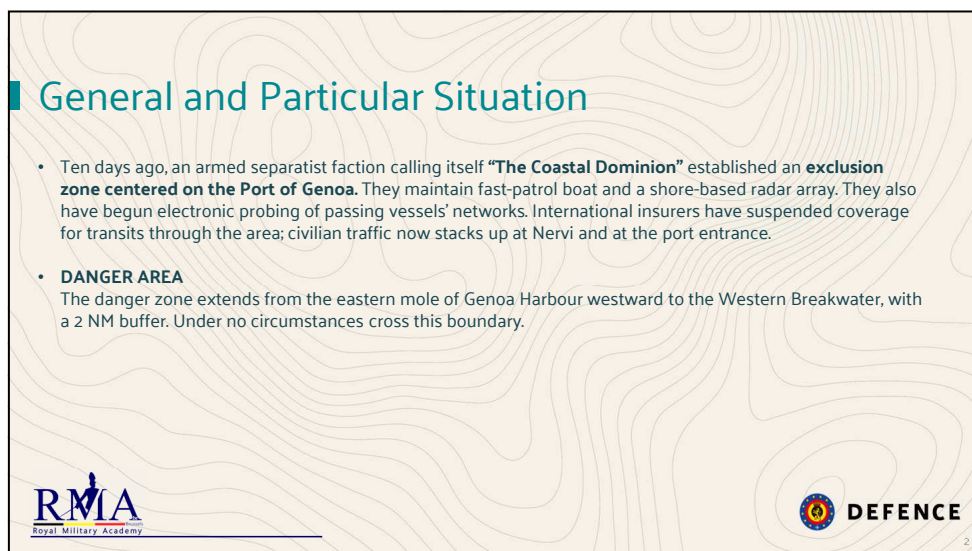
12

## E.4. Mission Briefing

21-05-25



1



2

1

## Orientation

**AREA OF OPERATIONS**

- Start Point:** Nervi Anchorage (44°28.0' N, 9°07.5' E)
- End Point:** Western Breakwater, Genoa Harbour (44°23.5' N, 8°57.0' E)

Genova port : One of Europe's busiest commercial ports—expect dense tanker and container traffic transiting inbound lanes south of your track.

**Exclusion Zone Boundary**

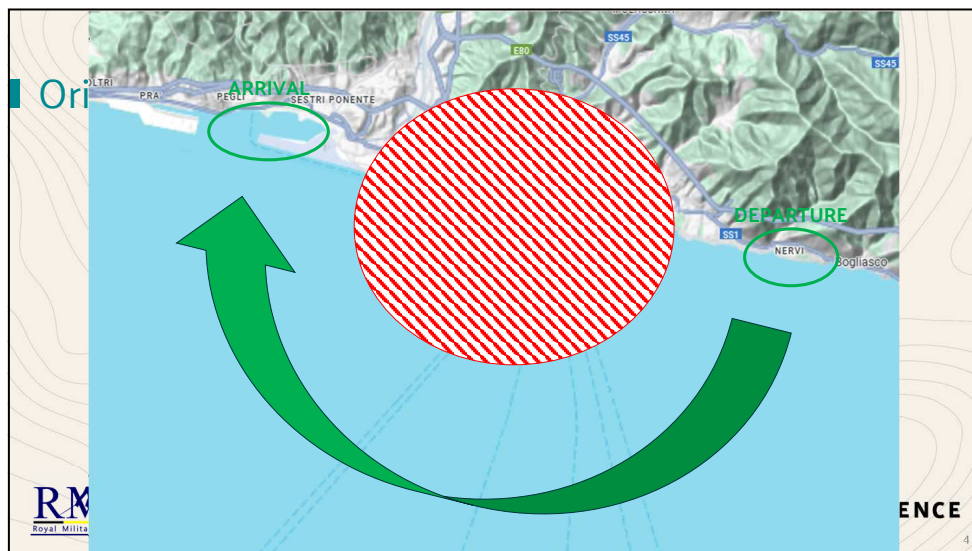
- Around main part of Genova port (cf. map)
- Crossing risks both kinetic interdiction and loss of commercial insurance.

**RMA**  
Royal Military Academy

**DEFENCE**

3

3





4



## Situation

Intelligence indicates the Dominion has **at least two fast-patrol boats** on station and a **shore-based radar array**. We also have credible reports that their technical arm has begun probing shipboard networks in past transits, attempting to **blind radars or corrupt ECDIS charts**.






5

5

## Mission

At **1130** local, **MCM warship** will depart Nervi, transit the designated coastal corridor, and arrive at the Western part of the Genova port by **1230**, ready to rendezvous with pilot boat. Avoid the exclusion boundary entirely.



6

6

## Execution

3 functions on the warship:



- Engine Control
- Bridge
- Radar



7

7

# Good luck !!!




















8

8





## E.5. Feedback Form and Results

Table E.1 summarizes the responses gathered from the feedback form completed by trainees after the cyber awareness training session. Responses are shown on a scale from 1 (Strongly Disagree) to 5 (Strongly Agree).

Feedback Question	Score (1-5)
<b>Access and Usability</b>	
The login and initial access to the cyber range environment was straightforward.	
The web-based GUI to access the virtual machine was responsive and intuitive.	
Launching and interacting with the Ubuntu workstation was user-friendly.	
The provided instructions (on-screen or in documentation) were clear.	
The presentation of the network topology was necessary for the scenario execution.	
The layout of VM consoles and network diagrams was convenient, well-organized and easy to understand.	
The network connectivity (ping, SSH, HTTP) behaved consistently.	
The performance (responsiveness, load times) of VMs met my expectations.	
Receiving feedback (logs, status messages) helped me understand what was happening.	
<b>Cyber Scenario and Technical Tasks</b>	
I correctly understood how the cyber attack was carried out (phishing mail, malware installation listening for C&C commands, lateral movement to IBMS server, launch of the attacks).	
Performing the phishing exercise (reading and clicking the simulated email) was seamless.	
Finding the malicious process running on the infected VM was challenging.	
Terminating the malware process required significant effort.	
Adding malware persistence across reboots and user logins would have been a relevant improvement to the scenario.	
Locating the malware's installation files and scripts on disk was difficult.	
The overall difficulty level of the cyber challenges was appropriate.	
The scenario felt realistic compared to actual maritime cyber operations.	

*Continued on next page*



Feedback Question	Score (1-5)
<b>Training Flow and Global Evaluation</b>	
Mail was a convenient communication channel to receive instructions during the training.	
The balance between scenario complexity and available time was appropriate.	
The overall flow of the scenario kept me engaged.	
I would feel confident using this environment for future training exercises.	

**Table E.1.** Summary of Participant Feedback Responses



## Bibliography

- [1] Muna Al-Hawawreh, Zubair Baig, and Sherali Zeadally. Ai for critical infrastructure security: Concepts, challenges, and future directions. *IEEE Internet of Things Magazine*, 7(4):136–142, 2024.
- [2] Thiago Rodrigues Alves, Mario Buratto, Flavio Mauricio de Souza, and Thelma Virginia Rodrigues. Openplc: An open source alternative to automation. In *IEEE Global Humanitarian Technology Conference (GHTC 2014)*, pages 585–589, 2014.
- [3] Belgium Naval & Robotics and Naval Group. Mcm be-nl program: Combat domain ssrs cdrl dc.3. Technical report, Belgium Naval & Robotics, April 2024. Version B, 8 Apr. 2024.
- [4] Belgium Naval & Robotics and Naval Group. Mcm be-nl program: Platform & navigation domain ssrs cdrl dc.3. Technical report, Belgium Naval & Robotics, April 2024. Version B, 8 Apr. 2024.
- [5] Belgium Naval & Robotics and Naval Group. Mcm be-nl program: Whole warship & container digital domain ssrs cdrl dc.3. Technical report, Belgium Naval & Robotics, April 2024. Version B, 8 Apr. 2024.
- [6] Belgium Naval & Robotics and Naval Group. Mcm-benl program: System/subsystem design description mcmplf. Technical report, Belgium Naval & Robotics, April 2024. Version F, 30 Apr. 2024.
- [7] Belgium Naval & Robotics and Naval Group. Ssdd cs: Combat system system/subsystem design description. Technical report, Belgium Naval & Robotics, April 2024. Version H, 30 Apr. 2024.
- [8] Aymeric Chincolla. Cyber-mar platform and the vessel pilot. <https://www.cyber-mar.eu/wp-content/uploads/2022/05/3.-Cyber-MAR-Vessel-pilot-Cyber-MAR-platform..pdf>, 2020. [Accessed 22-04-2025].
- [9] Aymeric Chincolla. Cybermar-architecture and technical modules: Valencia pilot. [https://www.cyber-mar.eu/wp-content/uploads/2020/12/Cyber-MAR\\_Architecture-and-technical-modules\\_1st-Pilot.pdf](https://www.cyber-mar.eu/wp-content/uploads/2020/12/Cyber-MAR_Architecture-and-technical-modules_1st-Pilot.pdf), 2020. [Accessed 22-04-2025].
- [10] Joseph Chukwunweike, Uchechukwu Mba, and Caleb Kadiri. Enhancing maritime security through emerging technologies: The role of machine learning in cyber threat detection and mitigation. pages 4121–4136, 08 2024.
- [11] Bridge Command. Bridge Command - an interactive 3d ship radar simulator. <https://www.bridgecommand.co.uk/>. [Accessed 26-04-2025].
- [12] Naval Sea Systems Command. Uss secure. <https://www.navsea.navy.mil/Media/Images/igphoto/2001343390/>. [Accessed 22-04-2025].
- [13] Crack-MCR. Macyste reference manual. <https://crack-mcr.github.io/MaCySTe/introduction.html>. [Accessed 20-05-2025].
- [14] Crack-MCR. Prerequisites - MaCySTe reference manual. <https://crack-mcr.github.io/MaCySTe/running/prerequisites.html>. [Accessed 23-04-2025].
- [15] Crack-MCR. Simulator - MaCySTe reference manual. <https://crack-mcr.github.io/MaCySTe/reference/bridgecommand.html>. [Accessed 26-04-2025].
- [16] CyberMAR. CyberMAR: The project. <https://www.cyber-mar.eu/about/>. [Accessed 21-04-2025].
- [17] Adrian Dabrowski, Sebastian Busch, and Roland Stelzer. A digital interface for imagery and control of a navico/lowrance broadband radar. In *Robotic Sailing*, pages 169–181. Springer, 2011.
- [18] Uldis Dzerkals, Michael Doe, and Christopher Lim. *EVE-NG Professional Cookbook*. EVE-NG Limited, July 2024. [Accessed: 2025-05-08].

- [19] EUROCONTROL. EUROCONTROL Specification for Surveillance Data Exchange – Part 1: All Purpose Structured EUROCONTROL Surveillance Information Exchange (ASTERIX). <https://www.eurocontrol.int/publication/eurocontrol-specification-surveillance-data-exchange-part-i>, 2021. Edition 3.1, Published on 23 November 2021. Accessed on 22 May 2025.
- [20] Frangoteam. Fuxa wiki – scada visualization tool. <https://github.com/frangoteam/FUXA/wiki>, 2024. Accessed: 2025-05-19.
- [21] Naveen Goud. Cyber Attack on COSCO. <https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/>. [Accessed 28-04-2025].
- [22] Andy Greenberg. The untold story of notpetya, the most devastating cyberattack in history. *Wired*, August 2018. [Accessed: 2025-04-26].
- [23] Omar Hasan, Derek Crane, and Gregory Dukstein. Incorporating simulated cyberspace effects on navy shipboard systems during training. In *Proceedings of the 2024 Spring Simulation Innovation Workshop (SIW)*. Simulation Interoperability Standards Organization (SISO), 2024. [Accessed: 2025-04-26].
- [24] International Maritime Organization. Resolution msc.428(98): Maritime cyber risk management in safety management systems. [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428\(98\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf), 2017. [Adopted on 16 June 2017.] [Accessed: 2025-05-17].
- [25] International Maritime Organization. Msc-fal.1/circ.3/rev.2: Guidelines on maritime cyber risk management. [https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20\(Secretariat\).pdf](https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf), 2022. [Issued on 7 June 2022.] [Accessed: 2025-05-17].
- [26] Giacomo Longo, Alessandro Orlich, Stefano Musante, Alessio Merlo, and Enrico Russo. MaCySTe: A virtual testbed for maritime cybersecurity. *SoftwareX*, 23:101426, July 2023.
- [27] Cyber MAR. CyberMAR - Pilot Scenarios. <https://www.cyber-mar.eu/pilot-scenarios/>. [Accessed 21-04-2025].
- [28] Eric Priante Martin. Msc container ship aground for three days in red sea amid questions over gps jamming. *TradeWinds*, May 2025. [Accessed: 2025-05-17].
- [29] National Marine Electronics Association. NMEA 0183 Standard. <https://www.nmea.org/nmea-0183.html>, 2025. Accessed: 2025-05-22.
- [30] NATS.io. About nats. <https://nats.io/about/>, 2024. [Accessed: 2025-05-19].
- [31] NATS.io. Jetstream clustering – nats documentation. [https://docs.nats.io/running-a-nats-service/configuration/clustering/jetstream\\_clustering](https://docs.nats.io/running-a-nats-service/configuration/clustering/jetstream_clustering), 2024. [Accessed: 2025-05-18].
- [32] NATS.io. Jetstream concepts – nats documentation. <https://docs.nats.io/nats-concepts/jetstream>, 2024. [Accessed: 2025-05-18].
- [33] OpenCPN. Opencpn chart plotter navigation. <https://opencpn.org/>, 2024. [Accessed: 2025-05-19].
- [34] pynmea2. The NMEA 0183 Protocol. <https://github.com/Knio/pynmea2/blob/master/NMEA0183.pdf>, 2010. Accessed: 2025-05-22.
- [35] Ørnulf Rødseth. Onboard maritime ict architecture and standards intelligent ship transport system. *ISTS*, 09 2023.
- [36] SAFETY4SEA. Norsk Hydro lost about \$35-40 million after cyber attack – safety4sea.com. <https://safety4sea.com/norsk-hydro-lost-about-35-40-million-after-cyber-attack/>, 2019. [Accessed 28-04-2025].
- [37] SAFETY4SEA Editorial Team. Windward: Gps jamming is a rising cyber threat in the red sea. *SAFETY4SEA*, May 2025. [Accessed: 2025-05-17].

- [38] Zandi Shabalala and Tanisha Heiberg. Cyber attack disrupts major south african port operations. *Reuters*, July 2021. [Accessed: 2025-05-17].
- [39] MPA Singapore. Mpa commissions mariot training facility. <https://www.mpa.gov.sg/media-centre/details/mpa-commissions-mariot-training-facility>, 2025. [Accessed 22-04-2025].
- [40] Singapore University of Technology and Design (SUTD). MPA Commissions MariOT Training Facility. <https://www.sutd.edu.sg/media-releases-listing/mpa-commissions-mariot-training-facility>, 2025. [Accessed 22-04-2025].
- [41] Samuel Souvannason. Navy Utilizes Realistic Cyber Simulations to Mature Cyber Mission Forces Beyond Qualifications. <https://www.navy.mil/Press-Office/News-Stories/Article/2249824/navy-utilizes-realistic-cyber-simulations-to-mature-cyber-mission-forces-beyond/>, 2018. [Accessed 26-04-2025].
- [42] Control Engineering Staff. Throwback Attack: How NotPetya Ransomware Took Down Maersk. <https://www.controleng.com/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/>, 2021. [Accessed 17-05-2025].
- [43] Kimberly Tam, Kemedi Moara-Nkwe, and Kevin D Jones. The use of cyber ranges in the maritime context: Assessing maritime cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, 3(1):16–30, 2021. [Accessed: 2025-04-26].
- [44] Naval Technology. US Navy’s FCC/C10F develops new cyber simulation training methods. <https://www.naval-technology.com/news/us-navys-fcc-c10f-develops-new-cyber-simulation-training-methods/?cf-view>, 2018. [Accessed 26-04-2025].
- [45] Daisy Thornton. Navy using virtual test bed to secure shipboard systems. <https://federalnewsnetwork.com/all-news/2016/03/uss-secure-ready-launch/>, 2016. [Accessed 22-04-2025].
- [46] Naval Today. US Navy developing cyber-safe ship. <https://www.navaltoday.com/2016/02/17/us-navy-developing-cyber-safe-ship/>, 2016. [Accessed 22-04-2025].
- [47] University of Plymouth. Cyber-ship lab. <https://www.plymouth.ac.uk/research/cyber-ship-lab>, 2024. [Accessed: 2025-04-10].
- [48] Gabor Visky, Arturs Lavrenovs, Erwin Orye, Dan Heering, and Kimberly Tam. Multi-purpose cyber environment for maritime sector. *International Conference on Cyber Warfare and Security*, 17:349–357, 03 2022.
- [49] Jan Vykopal, Pavel Čěleda, Pavel Šeda, Valdemar Švábenský, and Daniel Tovarnák. Scalable learning environments for teaching cybersecurity hands-on. In *2021 IEEE Frontiers in Education Conference (FIE)*, pages 1–9, New York, NY, USA, 2021. IEEE.
- [50] Alan Williams. €7 million project aims to enhance global maritime cyber security. <https://www.plymouth.ac.uk/news/eu7million-project-aims-to-enhance-global-maritime-cyber-security>, 2019. [Accessed 22-04-2025].