

Doctoral thesis

Doctoral theses at NTNU, 2024:109

Erlend Erstad

Operational training for enhanced maritime cyber resilience

Bridging safety and security through maritime education and training

NTNU
Norwegian University of Science and Technology
Thesis for the Degree of
Philosophiae Doctor
Faculty of Engineering
Department of Ocean Operations and Civil
Engineering



Norwegian University of
Science and Technology

Erlend Erstad

Operational training for enhanced maritime cyber resilience

Bridging safety and security through maritime
education and training

Thesis for the Degree of Philosophiae Doctor

Trondheim, March 2024

Norwegian University of Science and Technology
Faculty of Engineering
Department of Ocean Operations and Civil Engineering

NTNU

Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering

Department of Ocean Operations and Civil Engineering

© Erlend Erstad

ISBN 978-82-326-7812-9 (printed ver.)

ISBN 978-82-326-7811-2 (electronic ver.)

ISSN 1503-8181 (printed ver.)

ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2024:109

Printed by NTNU Grafisk senter

UiT The Arctic University of Norway

Faculty of Science and Technology

Department of Technology and Safety

Norwegian University of Science and Technology

Faculty of Engineering

Department of Ocean Operations and Civil Engineering

University of South-Eastern Norway

Faculty of Technology, Natural Sciences and Maritime Studies

Department of Maritime Operations

Western Norway University of Applied Sciences

Faculty of Business Administration and Social Sciences

Department of Maritime Studies

Declaration

The work presented within this thesis is my own. All work which is not my own is properly and clearly acknowledge to the respectful author of knowledge.

Abstract

Modern maritime navigation and operations heavily rely on technology. While this has brought many benefits, it has also introduced new risks, especially in cyber security. This thesis investigates how the maritime industry and maritime education and training institutions can be better prepared against cyber threats. By taking a human-centred design approach, the thesis investigates how qualitative research can be utilized to enhance maritime cyber resilience. This thesis explores how the traditional maritime ship safety transition into an industry which not just need to consider normal accidents, like fire onboard or ship collision avoidance, but also needs to address cyber security aspects. Central to this research is the exploration of the International Maritime Organization's (IMO) Resolution for Maritime Cyber Risk Management in Safety Management Systems (MSC.428(98)), which positioned cyber risk on the global maritime safety agenda. By underscoring the need for heightened awareness and urging the maritime sector to evolve and learn continuously, this Resolution has become a cornerstone in discussions about maritime cyber resilience. As a strategic focus for the IMO, MET's potential to fortify human capacity on ships stands out as a pivotal element in the quest to make humans the strongest link in maritime cyber security. Through a rigorous examination of current research trends, industry initiatives, and the pivotal intersection of automation and human interaction, this thesis underscores the importance of integrating maritime cyber security into MET curricula. To provide a comprehensive perspective, the research methodology encompasses a review of existing literature, an evaluation of the development of maritime cyber security, and a deep dive into how the maritime industry responds to regulations and frameworks. The thesis also assesses the relevance and applicability of concepts like maritime cyber resilience in the context of MET. The research approach includes a look at existing studies, an examination of how maritime cyber security has evolved, and a review of how the maritime sector deals with rules and guidelines. The thesis looks at how resilience applies to cyber issues in the maritime context. Key findings come from four major papers and a workshop. These insights stress the importance of teaching maritime cyber resilience widely. The first two papers address how a navigator's workday now is affected by cyber risks and how the navigator experience those risks. The final papers present human-centred design approach to developing and conducting maritime cyber resilience training, as well as a novel procedural framework. The final discussions in the thesis link these findings with existing knowledge to suggest how MET can really make a difference in improving cyber security at sea. In conclusion, this thesis offers insights both for researchers and for maritime professionals. As technology keeps advancing, the findings here offer a roadmap for future research and training efforts.

Acknowledgement

This PhD journey, with all its challenges and rewards, would have been unimaginable without the steadfast support of family, friends, and colleagues.

A profound thanks you to my supervisors, Dr. Runar Ostnes, Dr. Mass Soldal Lund and Dr. Kimberly Tam. Their expertise and guidance have been pivotal. Additionally, gratitude is owed to our MarCy project partners: NTNU, Norwegian Defence University College, DNV, Norwegian Hull Club, and Kongsberg Defence & Aerospace.

A special thanks to my good colleague and dear friend Marie Haugli-Sandvik. Without your support, reaching the finish line of this project would have been far more challenging, maybe even out of reach.

I want to thank other good colleagues and friends at NTNU in Ålesund. Special mention goes to Knut Remøy, Andreas Madsen, Dr. Marte Fanneløb Giskeødegård, Terje Slinning, and Arnt Håkon Barmen, among the many others who've enriched this journey. In addition, I also wish to acknowledge the importance of industry interest, collaboration and contribution, especially mentioning Dr. Odd Sveinung Hareide at the Norwegian Coastal Administration, as well as Lars Benjamin Vold at NORMA Cyber.

My research stay at the University of Plymouth's Cyber-SHIP lab was both enlightening and rewarding. I'd like to express my thanks to the dedicated team there, with a particular nod to Dr. Rory Hopcraft, Juan Misas, and Avanthika Vineetha Harish.

Finally, to my family for believing in me and supporting me, thank you. Above all, my deepest gratitude and thanks is reserved for my dear Sara and Ellie. Your unwavering and caring support during the tandem challenges of a PhD project and a global pandemic, has been my guiding light and safe harbour.

Published works

Paper I

Erstad, E., Ostnes, R., Lund, M. S. (2021). An operational approach to maritime cyber resilience. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 15.

<http://dx.doi.org/10.12716/1001.15.01.01>

Paper II

Erstad, E., Lund, M., Ostnes, R. (2022). Navigating through Cyber Threats, A Maritime Navigator's Experience. In: Tareq Ahram and Waldemar Karwowski (eds) *Human Factors in Cybersecurity*. AHFE (2022) International Conference. AHFE Open Access, vol 53. AHFE International, USA.

<http://doi.org/10.54941/ahfe1002205>

Paper III

Erstad, E., Hopcraft, R., Vineetha Harish, A. et al. A human-centred design approach for the development and conducting of maritime cyber resilience training. *WMU J Marit Affairs* 22, 241–266 (2023).

<https://doi.org/10.1007/s13437-023-00304-7>

Paper IV

Erstad, E., Hopcraft, R., Dorje J.M., Tam, K. (2023). CERP: A Maritime Cyber Risk Decision Support Tool. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 17.

<https://doi.org/10.12716/1001.17.02.02>

Workshop report

Erstad, E., Larsen, M. H., Lund, M. S., & Ostnes, R. (2022). Maritime Cyber Simulator Scenario Workshop report.

<https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3037765>

List of figures

Figure 1 Maritime Cyber Attack Database (MCAD) (NHL Stenden, 2023)	2
Figure 2 Structure of thesis	6
Figure 3 The bridge of Le Commandant Charcot, a highly complex and technological Polar Class 2 ice breaker vessel, delivered 2021. Picture used with courtesy of Ponant.....	8
Figure 4 'Incidents per year' (Meland et al., 2021).....	9
Figure 5 Saunders 'Research onion' as presented by Melnikovas (2018).	14
Figure 6 DRM Framework (Blessing & Chakrabarti, 2009, page 15)	18
Figure 7 Human-Centred design activities, adopted from (ISO, 2019a, page 12)	19
Figure 8 Research methods	21
Figure 9 'Strategies for Validation in Qualitative Research', adopted from Creswell et al. (2018, page 260).....	25
Figure 10 'Analysis of historical trends' (Bolbot et al., 2022, page 8)	28
Figure 11 'General form of resilience curve for resilience defined as rebound.' (Madni et al., 2020, page 4).....	33
Figure 12 'Google search trends about cyber resilience since 2004' (Sepúlveda Estay et al., 2020, page 2).....	35
Figure 13 'Cyber Resilience Engineering Framework' (Bodeau et al., 2015, page 10).....	36
Figure 14 - Research results and how they relate to research questions.	43
Figure 15 "Origins of Maritime Cyber Resilience" (Erstad et al., 2021)	44
Figure 16 - Categories and sub-categories (Erstad, Lund, et al., 2022)	45
Figure 17 - Flowchart for the Cyber Emergency Response Procedure (CERP) (Erstad, Hopcraft, Misas, et al., 2023).....	47
Figure 18 'Human-centred quality' (ISO, 2019b, page 78).....	58

List of tables

Table 1 Overlapping themes for DRM and HCD.....	19
Table 2 'Basic difference between Safety-I and Safety-II' (Hollnagel, 2013, page 8)	33
Table 3 'Balancing Safety-I and Safety-II in DPO training' (Wahl et al., 2020, page 3)	42
Table 5 Cyber resiliency goals compared to categories of navigators cyber experience	55
Table 6 - Interview guide - translated from Norwegian to English.....	I

Glossaries and acronyms

ALARP	As Low As Reasonably Possible
AIS	Automatic Identification System
BIMCO	Baltic and International Maritime Council
BRM	Bridge Resource Management
BWS	Ballast water management system
COLREG	Convention on the International Regulations for Preventing Collisions at Sea
ENISA	The European Union Agency for Cybersecurity
FAL	Facilitation Committee
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
HCD	Human-Centered Design
ICT	Information and Communications Technology
IMO	International Maritime Organization
ISM	The International Safety Management (ISM) Code
IT	Information Technology
MARPOL	International Convention for the Prevention of Pollution from Ships
MET	Maritime Education and Training
MSC	Maritime Safety Committee
NATO	The North Atlantic Treaty Organization
NIS	Network and Information Security (NIS) Directive (EU Directive 2016/1148)
NIS2	Network and Information Security (NIS) Directive (EU Directive 2022/2555)
NIST	The National Institute for Standards and Technology
OT	Operation Technology
SLR	Structured Literature Review
SMS	Safety Management System
SOLAS	International Convention for the Safety of Life at Sea

Contents

Declaration	I
Abstract	I
Acknowledgement.....	II
Published works	III
List of figures	IV
List of tables.....	IV
Glossaries and acronyms	V
Contents.....	VI
1 Introduction	1
1.1 Thesis objective.....	3
1.1.1 Research questions	4
1.1.2 Limitations.....	5
1.2 Structure of thesis.....	5
2 Research background and motivation for the thesis	7
2.1 Maritime ship safety.....	7
2.2 Evolution of navigation	8
2.3 The industry challenge	10
2.4 The industrial opportunity	11
2.5 The academic challenge and opportunity	12
3 Research approach.....	14
3.1 Ontology and the view of reality.....	15
3.2 Epistemology and the creation of knowledge	15
3.3 Axiology and the role of values	16
3.4 Research methodology	17
3.4.1 Human-Centred Design.....	19
3.5 Research methods.....	20
3.5.1 Literature review research	21
3.5.2 Qualitative interviews.....	22
3.5.3 Workshops with focus group interviews	23
3.5.4 Simulator exercise and training	23
3.6 Validity and reliability.....	24
	VI

4	Theoretical foundation.....	27
4.1	Maritime cyber security.....	27
4.1.1	The development of maritime cyber security in research.....	27
4.1.2	Industry and governance frameworks for maritime cyber security	30
4.2	Resilience and safety	32
4.3	Cyber resilience.....	34
4.4	Maritime cyber resilience.....	36
4.4.1	Results from maritime cyber resilience literature review.....	37
4.5	Maritime training and education	40
5	Research results and contributions	43
5.1	Paper I – An operational approach to maritime cyber resilience	43
5.2	Paper II – Navigating through cyber threats, a maritime navigator’s experience	44
5.3	Paper III – A human-centred design approach for the development and conducting of maritime cyber resilience training.....	46
5.4	Paper IV – CERP: A maritime cyber risk decision making tool.....	46
5.5	Workshop, focus groups and simulator experiment	48
5.6	Reflection of papers.....	49
5.6.1	Reflections - Paper I.....	49
5.6.2	Reflections – Paper II.....	49
5.6.3	Reflections – Paper III.....	50
5.6.4	Reflections – Paper IV	50
5.6.5	Reflections - Workshops	50
6	Discussion.....	52
6.1	Integrating of resilience into maritime cyber security and maritime training and education	52
6.2	Relevance and usability of Human-Centered Design.....	57
7	Conclusions	59
7.1	Academic impact and contributions	59
7.2	Industrial impact and contributions	60
7.3	Future research	60
8	References	62
	Annex I – Published scientific papers and workshop report	
	Annex II – Additional SLR information	
	Annex III – Interview guide	
	Annex IV – Course feedback scheme	

Annex VI – NSD forms.....

1 Introduction

As maritime operations increasingly rely on technology, understanding cyber threats and building maritime cyber resilience becomes essential to maintaining safe and effective operations. In 2011, ENISA (2011) analysed the cyber security aspects in the maritime sector, emphasising that the maritime is a critical infrastructure which is also vulnerable to cyber-attacks, such as the well-known, well documented STUXNET incident. The STUXNET incident altered and damaged nuclear centrifuges in a top-secret Iranian enrichment nuclear plant, which was supposed to be completely air-gapped, meaning no connection to the internet at all (Farwell & Rohozinski, 2011). However, it became clear that digital threats affected more critical infrastructure than nuclear. ENISA emphasised that digital incidents could happen to the maritime industry. There has not yet been a reported cyber-attack that scale as STUXNET, creating physical damage on board ships. However, the maritime industry has also been affected by the largest cyber-attack in the history, the NotPetya attack (Crosignani et al., 2023), causing over 300 million US dollars in loss for AP Moeller-Maersk in 2017 (Ashford, 2019). Due to the increasing reliance on technology and digital systems in the maritime industry, in 2017, the International Maritime Organization (IMO) provided a Resolution for Maritime Cyber Risk Management in Safety Management Systems (MSC.428(98)) (International Maritime Organization, 2017b). The Resolution put cyber risk on the global, maritime safety agenda, describing there is an urgent need to raise awareness on cyber threats in the maritime industry. The Resolution emphasize that the maritime industry must become operationally resilient to cyber risks, and learning and evolving is a cornerstone in cyber resilience (Bodeau et al., 2011). Maritime Education and Training (MET) is a vital strategy focus for IMO, considering there is formalized and standardized training in the International Convention on Standards of Training, Certification and Watchkeeping for Ships (STCW) (International Maritime Organization, 2016). Hareide et al. (2018) noted that the human capacity onboard a ship must become the strongest link in the protection of maritime cyber security issues and that maritime cyber security must be a part of MET to enhance navigator competence. This thesis focuses on enhancing operational training for maritime cyber resilience, by bridging the gap between safety and security through Maritime Education and Training (MET).

In research, the topic of maritime cyber security began to receive increased and proper attention in 2017 and onwards, as it was less than five research papers a year in the previous years (Bolbot et al., 2022). However, in 2021, the Resolution for maritime cyber risk management went into force (International Maritime Organization, 2017b) and the maritime industry and shipowners were required to consider maritime cyber risk as required per the International Safety Management code (ISM). Several reports put cyber security concerns on a top ten list of global trends, for instance, World Economic Forum (2023) rates it as a number 8 risk out of 10 in the “The Global risk Report 2023”. World Maritime University (WMU) in the report “Transport 2040: Impact of Technology on Seafarers”, cyber security is noted as a growing concern and as a number eight trend to influence commercial shipping in the years to come (Ölçer et al., 2023). Maritime cyber-attacks are an increasing problem and occurs all around the globe, as shown in Figure 1. Fortunately, the maritime industry is now actively engaged in cyber security projects. In 2023, cyber security is starting to become a well-known subject to most people in the industry, ranging from onboard crew and shipowners to shipbuilders and suppliers. here are several different research initiatives, such as MarCy in Norway, Cyber SHIP-lab in United Kingdom, the Maritime Cyber Attack Database (MCAD) in Netherlands, MariCyBERA in Estonia, amongst several

others. As shown in Figure 1, the MCAD displays numerous reported cyber incidents in the maritime industry, displaying both facts about where it happened, but also what happened (NHL Stenden, 2023).

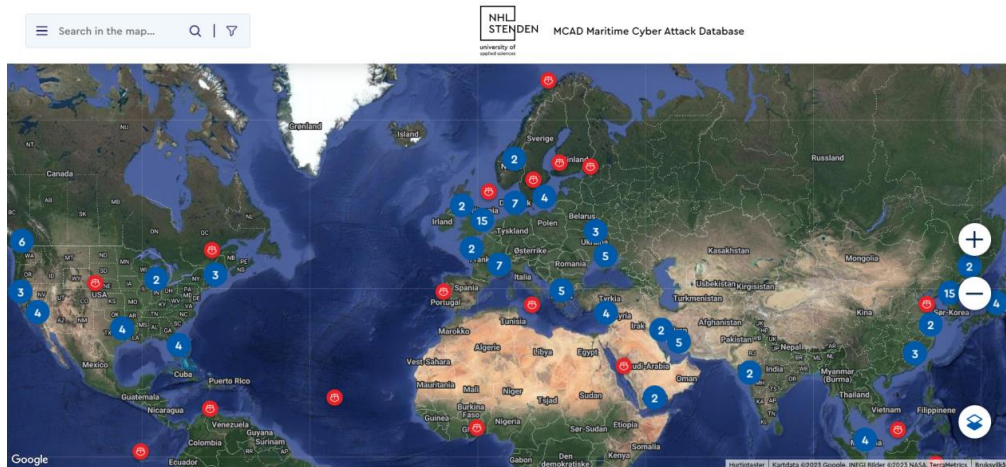


Figure 1 Maritime Cyber Attack Database (MCAD) (NHL Stenden, 2023)

In 2020, there was a gap between academia and the industry in terms of discussing and collaborating on cyber security related topics (Erstad, Lund, et al., 2022) and a contributing factor might be that companies were afraid of negative reputation if it were to be revealed that their company was not cyber secure (Bolbot et al., 2022). Yet there isn't any formal education concerning maritime cyber security (Erstad, Lund, et al., 2022; Heering et al., 2021; Hopcraft, 2021), but today the industry and academia are collaborating side by side in terms of maritime cyber resilience research and training programs, which benefits both sides.

While advancements in maritime cyber security research have been instrumental in understanding and mitigating technical vulnerabilities, it is equally paramount to recognize the symbiotic relationship between technology and its human operators. As highlighted by Lützhöft and Dekker (2002), increased automation creates new human weaknesses and amplifies existing ones. This indicates that technology race faster than the society adapts to new technology, leaving the human left behind. Forty years ago, Bainbridge (1983) published the paper "Ironies of automation", which explains why there is a need for human focus when designing and operating technology. Bainbridge's is related to automation, however, as automation and computer today is two sides of the same coin, one can relate the ironies of designing computers systems, and hence maritime cyber security issues is a problem which can occur. Thus, there is a need for human focus when considering maritime cyber resilience.

Bainbridge (1983) presented two key ironies:

1. Designer errors can be a major source of operating problems.
2. The person who tries to eliminate the operator still leaves him to do the tasks which he cannot think how to automate.

Since the 1960s, numerous research papers have cited Bainbridge and said that the “Ironies of automation” still is valid today as it was forty years ago (Strauch, 2018). Considering a nautical context, ships today are designed highly automated and Integrated Bridge Systems (IBS) onboard ships control ship movements and systems and are designed to be monitored by a navigator to ensure that the systems are working correctly. The ironies can imply that a navigator (i.e., the operator) must manually take the wheel when the navigation technology onboard the ship fail (Lützhöft & Dekker, 2002). Fortunately, a problem only occurs now and then, which means that the navigator can simply monitor that the navigation and ship handling systems is working correctly. Research also indicates that the human operator is not good at long-term monitoring (Lützhöft & Dekker, 2002). Unfortunately, this again means that navigators practical skills considering navigation and manual ship handling may slowly deteriorate, as which is pinpointed by Bainbridge (1983). Making things simpler in daily operations, may make things harder in an emergency. How will a problem escalate in a cyber threat situation, where an adverse actor wants to exploit or compromise the navigation systems? If all systems onboard are inter-connected and/or connected to the internet, one single, well-engineered cyber-attack may affect the whole ship, such as presented by Longo et al. (2022); Lund, Gulland, et al. (2018); Tam et al. (2021). In a cyber risk situation this mean that an experienced navigator may be degraded to a novice (Erstad et al., 2021), as a cyber-attack in not as known and tangible as a normal technical problem (Erstad, Lund, et al., 2022).

1.1 Thesis objective

This PhD thesis is part of a Norwegian Research Council funded project called MarCy (Maritime Cyber Resilience) which is a Knowledge Building project for Industry. MarCy is a collaboration between the academic partners Norwegian University of Science and Technology (NTNU), the Norwegian Defence university College (NDUC) and the industry partners DNV, Kongsberg Defence and Aerospace, and Norwegian Hull Club. MarCy project goal is to develop validated means for improving cyber resilience of maritime digital control systems and maritime operations. MarCy will address both human and technological aspects of maritime cyber resilience, and the objectives are formulated as:

- Mapping the current state of maritime cyber security and resilience with respect to risks, regulations, and mitigating activities.
- Develop demonstrators of maritime cyber resilience based on operational scenarios incorporating cyber risk.

The MarCy project is focused on the several aspects of cyber risks related to IBS onboard maritime vessels, more specifically Integrated Navigation Systems (INS). Because of this, the navigator who is at the sharp end of the operation and operates/monitors the INS will be the main focus of this thesis, but the thesis will also address other stakeholders, such as shipowners, other on-board crew members, Cyber Emergency Response Teams (CERT), insurance providers, and class societies.

The main objective of the PhD thesis is as follows:

- Research how Maritime Education and Training strategies can be utilized to enhance maritime cyber resilience.

‘Strategies’ are here understood as methods, demonstrators, and recommendations, which can be utilized in maritime operations and training.

Even though STCW does not explicitly mention any kind of maritime cyber training, it does not indicate that it should not be considered (International Maritime Organization, 2016). As the ISM code is part of STCW scope, maritime cyber risk is implicitly a learning requirement. As put forward by Scanlan et al. (2022), there is a need for new approaches when considering maritime cyber awareness training and a special focus on the human element. When considering onboard computer and navigation systems which encompass e-Navigation, IMO has recognized and suggested Human Centred-Design in a guideline regarding software quality assurance for navigation system software trustworthiness (International Maritime Organization, 2015), which acknowledges and indicates the shift from a technology focus to a more human factor focus

The thesis will contribute to the development of new concept for enhanced operational maritime cyber resilience and providing knowledge of how to bridge maritime cyber security and safety for maritime training and education. The thesis will present a research project with the aim of giving a better understanding of the challenges and opportunities associated with maritime cyber resilience. The research project has been conducted in close collaboration with the industry and the project partners, as well as with partners within academia, and has been achieved by exploring the following research questions:

1.1.1 Research questions

Research question 1: How can maritime cyber resilience be defined, and what is the state-of-the-art research within the concept of maritime cyber resilience?

RQ1 investigates the vulnerabilities, threats, and protection measures in a nautical operation where a navigator is interacting with INS, and what the potential operational consequences are which can occur if the navigator fails to detect a cyber threat. RQ1 contributes to the main objective by providing a foundation for the research to be conducted. RQ1 will be supported by a literature review of the relevant research.

Research question 2: What is required to enhance maritime cyber resilience in maritime operations?

RQ2 investigates how operational experience can be used to enhance maritime cyber resilience, by undertaking semi-structured interviews. It provides information regarding what training is provided in maritime organizations with complex socio-technological systems concerning cyber resilience, to create input to what training should be provided for enhanced maritime cyber resilience. Further, RQ2 provides insight into MET methods, such as simulator and real-life scenarios, can be used to enhance maritime cyber resilience.

Research question 3: What strategies can be used to make operations on maritime vessels more resilient to cyber risks, and how can the strategies be tested and evaluated?

RQ3 utilizes the findings from RQ1 and RQ2, to further develop strategies which can be implemented in MET for enhanced maritime cyber resilience. Maritime simulator scenarios are

developed for maritime cyber resilience training, where the emphasis are on bridging security and safety. Workshop and focus group methods were used to validate the maritime cyber simulator scenarios.

1.1.2 Limitations

The thesis will focus on discussing human aspects of maritime cyber resilience and maritime education and training. Even though the findings in the paper may be relevant for military vessels and organizations, ports or port organizations, and autonomous or remotely operated vessels, the main scope of the thesis is to investigate civilian conventional merchant vessels and the civilian organizations supporting them.

The technological aspect of maritime cyber resilience is acknowledged, but out of scope of the thesis. Technical aspects, such as network architecture, algorithms, tools for surveillance and handling of malware, among other things, are a separate research focus of the MarCy project. A cyber-attack could take many forms and what is interesting for the research is the cyber risk and how to operationally mitigate the consequences. The knowledge of the technical aspects of maritime cyber resilience will be used for understanding of how to enhance the operational handling of such, but the thesis will not contribute to the knowledge of technical measures for enhancing maritime cyber resilience.

1.2 Structure of thesis

An illustration of thesis structure is shown in Figure 2. The introduction presents the research project as a whole and the research questions. Section 2 investigates how maritime safety have been treated historically and how modern technology have provided the maritime industry with great benefits, but also by introducing cyber risks. Further, the section presents the industry and academic challenge and opportunities. Section 3 describes the research's philosophical underpinnings, methodology, and specific methods, offering a comprehensive view of the research strategy. Section 4 investigates the state-of-the-art theoretical background for the thesis and the research objective. The section starts by presenting the development of maritime cyber security and provides insight into how the industry cope with regulations and frameworks. Further, the section presents resilience and safety, which further will be extended to cyber resilience and maritime cyber resilience, before the section close by explaining maritime training and education. Section 5 presents the research results of the PhD project, presenting the essence of the four published papers and the workshop conducted, before offering critical reflections on each. Section 6 engages the findings in light of relevant theory, focusing on the enhancement of maritime cyber resilience through training and education. The thesis is concluded in section 7, where also the academic and industry contributions and impacts are highlighted, before the thesis finish by suggesting some potential areas for future exploration.

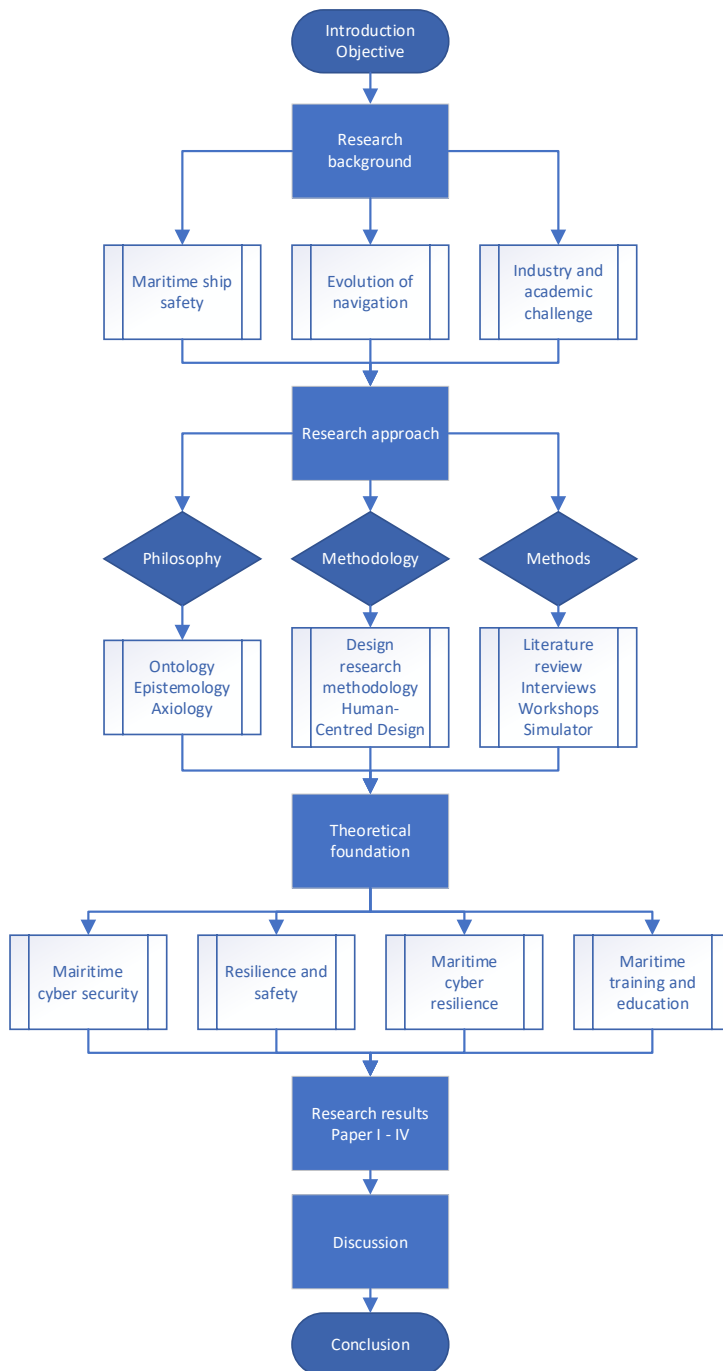


Figure 2 Structure of thesis

2 Research background and motivation for the thesis

The maritime industry is complex and affected by many factors. To provide the reader with a grasp of the complexity, this section is dedicated to the industry and academic background for the thesis. In addition, the section will provide context and the motivation for investigating maritime cyber resilience and maritime training and education, by looking into industrial and academic challenges and opportunities. Maritime regulations and standards are historically slow processes, and it is important to understand how the maritime industry has traditionally been a reactive industry, to provide recommendations for the industry to become more proactive and resilient in the face of technological challenges. First, the section will take a step back in history and highlight maritime accidents which have shaped modern maritime safety aspects. Further, the section will describe navigation and modern maritime operations and the organizations and regulatory aspects which govern the industry today. In addition, the section will describe the technological development of ships as well as how modern operations are being managed.

2.1 Maritime ship safety

Safety is an cornerstone in the modern maritime industry (International Maritime Organization, 2020). Providing the full history of safety impacts in the maritime industry is out of scope for the thesis, however, it have previously been thoroughly covered in previous research (Lutzhof & Oltedal, 2018). However, it is important to look back at historical events to understand how reactive the maritime industry treats safety concerns to set the stage for the thesis, as the thesis scope is to research how MET strategies can be utilized to enhance maritime cyber resilience.

Historically, maritime safety events that have resulted in massive loss of lives have led to significant changes in safety regulations (Lutzhof & Oltedal, 2018). One of the earliest and most known pivotal changes in modern maritime history was the sinking of the *Titanic* in 1912, where over 1500 people perished (Parsons & Allen, 2018). The disaster led to the first International Convention for the Safety of Life at Sea (SOLAS) in 1914, establishing the first comprehensive safety standards, including ship design, equipment, and emergency procedures (International Maritime Organization, 2020). Another example is the *Herald of Free Enterprise* incident in 1987, a British ferry that capsized, leaving 193 dead. The incident was attributed to the failure to close the bow doors, and the subsequent inquiry called for improvements in the ships Safety Management System (SMS) (Parsons & Allen, 2018). This incident was instrumental in the creation of the ISM Code, aimed at providing an international standard for the safe management and operation of ships (International Maritime Organization, 2023). These incidents show a pattern of reactive regulation, where new safety measures are often only introduced following a disaster. However, they have undeniably contributed to higher safety standards and practices in the maritime industry. Below is a list of a selection of safety incidents which have impacted the maritime industry and regulatory frameworks (Lutzhof & Oltedal, 2018):

- 1967: The grounding of the super tanker *Torrey Canyon* led to one of the earliest and most significant oil spills, which then precipitated the International Convention for the Prevention of Pollution from Ships (MARPOL) in 1973.
- 1978: The grounding of the *Amoco Cadiz* off the coast of France resulted in one of the largest oil spills in history. This incident also led to modifications to International Convention for the

Prevention of Pollution from Ships (MARPOL), specifically focusing on double-hull designs for oil tankers.

- 1989: A catastrophic oil spill from the *Exxon Valdez* led to increased scrutiny on single-hulled tankers and contributed to changes in international regulations on tanker design.
- 1994: The *Estonia* disaster where the ship sank in the Baltic Sea resulted in 852 deaths, leading to new international regulations concerning the stability and survivability of passenger ships.
- 2002: The oil tanker *Prestige* broke apart and sank, resulting in a significant oil spill. This further expedited the transition to double-hulled tanker designs.

Each of these incidents and numerous others have contributed to a better understanding of maritime risks and resulted in specific regulatory changes aimed at improving global safety in maritime navigation. The accidents have augmented the maritime industry's understanding of safety from not just a technological standpoint but also to include operational, environmental, and human factors perspectives, transitioning to the age of resilience (Lutzhof & Oltedal, 2018). There has not yet been any cyber incident equivalent to the Titanic incident, but as the following sections will outline, the industry is now taking a resilient and proactive approach towards cyber risks, by implementing new resolutions and guidelines. The following sections will focus on the evolution of maritime navigation and the opportunities and technical challenges that follow with it.

2.2 Evolution of navigation

The art of maritime navigation and the nautical science of determining a ship's position and plotting its course, has witnessed changes over time, especially with the introduction of digital navigation systems (Hareide, 2020). Historically, sailors relied on celestial bodies for navigation, using instruments like astrolabes and sextants to measure angles between stars and the horizon (Bowditch, 2002). Celestial navigation, while reliable under clear skies, was often considered impractical during overcast conditions. In addition, celestial navigation was far less precise than today's navigation (Bowditch, 2002).



Figure 3 The bridge of *Le Commandant Charcot*, a highly complex and technological Polar Class 2 ice breaker vessel, delivered 2021. Picture used with courtesy of Ponant.

Technological developments brought instruments like the gyrocompass, which worked independently of external references, offering consistent accuracy. Moreover, the introduction of radio-based navigation systems such as LORAN (Long Range Navigation) and later, the Global Positioning System (GPS), revolutionized maritime navigation. These systems diminished the dependency on celestial bodies, ensuring that vessels could navigate accurately under any condition (Bowditch, 2002). Despite some ships still use charts, modern navigation is increasingly reliant on several computer systems for the safety of navigation, such as maritime radars and maritime Electronic Chart Display and Information System (ECDIS). This has undoubtedly yielded efficiency and safety for navigation of ships, but it has also introduced new issues to consider. For instance, in 2008 the Marine Accident Investigation Branch (MAIB) introduced the term “ECDIS-assisted groundings”, describing that a main reason for such accidents to occur is the improper use of ECDIS and/or lack of training and awareness (Hareide, 2020). DiRenzo et al. (2015) notes that massive ships, such as 400-metre-long containership can be operated by just 13 crew onboard, thanks to ECDIS and other automated computer systems. Further, DiRenzo et al. (2015) emphasize that an cyber-attack could affect ECIDS, and hence impact the safety of the ship, resulting in an environmental and financial disaster.

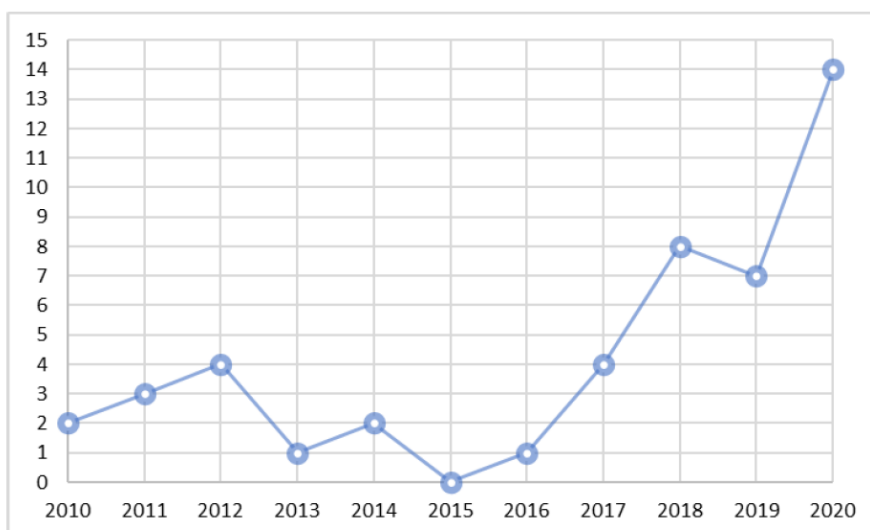


Figure 4 ‘Incidents per year’ (Meland et al., 2021)

The increasing reliance on digital tools and computers exposes vessels to cyber risks (DiRenzo et al., 2015) and there are several reported incidents in recent decades (Meland et al., 2021), which underscores the importance of enhancing maritime cyber resilience. A number of reported maritime cyber security incidents covering both offshore and onshore systems are listed in Figure 4, even though there are probably large number of unreported cyber incidents due to the fear of negative publicity (Bolbot et al., 2022). Cyber-attacks in the maritime industry may also be classified and unavailable to the public (Farah et al., 2022). The following sections will describe the industry and academic challenges and opportunities which the maritime industry faces considering maritime cyber risks.

2.3 The industry challenge

World Economic Forum identifies widespread cybercrime and cyber insecurity as number eight on a top ten list of global risks ranked by severity, both in a short and long term perspective (World Economic Forum, 2023). There is also a rise in cybercrime which specifically targets the maritime sector. The Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) for increased maritime cyber resilience was established on 1 January 2021 as an initiative by the Norwegian Shipowner Association and The Norwegian Shipowners' Mutual War Risks Insurance Association (DNK). NORMA Cyber publishes an annual cyber threat assessment, which reports that there is an increasing cyber threat level. For instance, there was 49 publicised ransomware attacks on the maritime sector in 2022 compared to 20 in 2021, which is a 145% increase. The changing security situation in the world, such as the Ukraine War, has its impact on the maritime sector and has made the threat landscape even more insecure (NORMA Cyber, 2022, 2023). Ransomware is a cyber-attack which can harm a company both economically and practically, hindering access to critical systems used by ship navigators or operators of other technical systems onboard and ashore. According to Meland et al. (2021), ransomware is the most common attack vector in maritime cyber incidents from 2010 to 2020, and Potamos et al. (2023) specifies that 41% of all the attacks mentioned in Meland's paper are related to ransomware.

In recent times, there have been multiple instances of cyber related incidents. As of today, the best known cyber-attack which also affected the maritime industry was in 2017 when AP Moller–Maersk was attacked by a destructive ransomware, NotPetya, which showed how an aggressive cyber-attack could destroy over 55,000 computers and 7000 servers of the shipowners infrastructure for business operation (Ashford, 2019). Meland et al. (2021) analysed 46 maritime cyber security incidents between 2010 and 2020, ranging from attacks on shipping companies IT infrastructure to exposed OT systems onboard ships and offshore installations. For instance, control systems onboard a commercial ship bound for New York were harmed by a cyber incident in 2019 and the dynamic positioning systems and thus thruster control onboard a drilling rig in New Mexico in 2013 were infected by a virus, resulting in an operational halt (Meland et al., 2021). Tam et al. (2021) have physically demonstrated cyber vulnerabilities in a ships rudder system and described how a ship grounding caused by a cyber-attack can impact a port. Even though the 2021 Suez Canal obstruction caused by the container vessel *Ever Given* was not caused by a cyber-attack, the cost associated with the obstruction was approximately 12% of world trade, which indicates that a cyber-attack could have the same effects (Afenyo & Caesar, 2023). Even radar systems onboard ships has been demonstrated as vulnerable to cyber-attacks (Longo et al., 2022).

Safety and security regulations in the maritime industry are internationally governed by the IMO. Often the chosen solution to safety and security hazards more regulations, standardisation, implementation of risk management systems and/or standardized training. This is primarily done by classification of ships by class societies and implementation of STCW modules. This has undoubtedly yielded a positive impact on safety onboard ships considering traditional risks, accidents, or incidents. However, the IMO is slow when considering the implementation of new technological challenges (Heering et al., 2021). The difference between a traditional risk (i.e., fire, grounding, flooding, etc.) and a cyber risk, is that the latter is somehow always tailored by a human being who has the intent that something happens with a system to generate a consequence (Erstad et al., 2021). This means that when it comes to cyber security,

standardization and “one-size-fits-all” solutions can have a negative impact on the cyber risk profile. It is important to emphasize that it is not an exclusively negative impact, but rather the contrary, as cyber security frameworks and regulations have yielded increased the industry knowledge and provided a foundation for further work. However, if all computer and cyber protection systems (including support systems and sub-systems) are designed the same, all can have similar or identical vulnerabilities, which means it is a matter of time, effort, capability, and profitability for a malicious actor to expose the vulnerability. Some insurance companies will not cover cyber security incidents if the system is not as specified in the contract for the ship, as the classification and documentation for the ship form the basis for the insurance. This is a paradox observed in the maritime industry. In terms of security patching for systems, the operator may sometimes not be allowed to alter the software by installing critical updates. Computer systems need regular patching to be cyber secure and many ships today have several onboard systems which still operate on outdated Windows operating systems, which in itself poses a cyber risk (Hopcraft et al., 2023; Jones et al., 2016). Shipowners also need to consider cost when installing and updating onboard systems. Ships are often contracted several years in advance prior to the actual shipbuilding process. In the specification for the shipbuilding contract, it is also specified the intended hardware and software for the ship, and it is widely known that computer systems often have a life span of three to eight years (HP Online Store, 2022). A ship is normally designed to operate for 30 years (Dinu & Ilie, 2015), which means the ship will most likely outlive its own onboard digital components.

Sophisticated malicious actors, such as nation state actors and APT actors (Advanced Persistent Threat), often search for, and exploit, new and previously unknown vulnerabilities, which are known as zero-day exploits. Therefore, when considering maritime cyber resilience, the maritime industry needs to consider all the known vulnerabilities relevant for its own operation as well as unknown vulnerabilities. It is exceptionally difficult to know and prepare for the unknown cyber threats. The human operator (regardless of whether it is a navigator or engineer, onboard or ashore) needs to have in-depth knowledge of the system they are operating as well as be flexible enough to tackle unknown threats, vulnerabilities, and risks in their own systems. As of 2023, there are no formal specific measures for training on cyber security problems for onboard crew. The next sub section will argue why cyber risk also could be an industry opportunity.

2.4 The industrial opportunity

“No risk, no reward” is an old saying. Increased digitalization of ship systems will introduce new rewards, such as opportunities for enhanced efficiency, profit, and safety for both the ship and the crew (International Maritime Organization, 2015). Increased digitalization will also increase the complexity of the vessel and implementation of more technology in a maritime system does not necessarily cohere with the reduction of human error (Relling et al., 2018). There is potential for the maritime industry to view cyber risk as an opportunity. In a business context, risks and opportunities are often two sides of the same coin, and technology can pose both to organizations. Treating and handling emerging risks can stimulate for innovation, learning, adaption, cost reduction, and give stakeholders a competitive advantage. Addressing risks can lead to the development of innovative solutions or improvements in existing processes, products, or services (Tongur & Engwall, 2014).

Embracing risks can encourage problem-solving within an organization. The following paragraphs in this sub-section will address Tongur and Engwall (2014) perspective on risks connected with technology shifts and discuss them in a maritime cyber perspective. Businesses and organisations that confront risks

often gain knowledge and experience, enabling them to make better informed decisions and adapt more effectively to future challenges, which can improve a company's resilience. Successfully managing risks can result in a competitive edge by enhancing a company's reputation for reliability, responsiveness, and resilience. This can lead to increased customer loyalty, better supplier relationships, and improved investor confidence, which will be argued to be important throughout this thesis. By identifying and addressing potential risks, a business can minimize or avoid negative consequences, such as financial losses or reputational damage. This risk management process can ultimately result in cost savings and improved operational efficiency.

In a specific cyber resilience context, cyber risks highlight the importance of employee training and awareness. Organizations can use known cyber incidents, or research of such, as an opportunity to educate their workforce on cybersecurity best practices, ultimately reducing the likelihood of future breaches due to human error. By effectively responding to and recovering from a cyber incident, an organization can demonstrate its resilience and commitment to security. This can result in a competitive advantage. The key is to proactively learn from the incident and implement measures to prevent similar occurrences in the future, which in other terms is basic cyber resilience. From a management point of view, maritime cyber risk assessments will yield better control of own vessels. Ships today range from newbuilds to retrofits, and not two sister-ships are identically the same. The requirement to documentation of the ship have also undergone a development the last decades, as new rules and regulations have been implemented. Maritime cyber risk assessment will provide shipowners with technological overview even of ships with less documentation than vessels which is built today (International Maritime Organization, 2017b), as knowledge of asset inventory is key (BIMCO, 2020).

One way to overcome an unknown problem is to do business as usual and manually understand and handle the system an operator is working with each day (Bainbridge, 1983). Therefore, by enhancing maritime cyber resilience in the industry and the operator's (i.e., navigator) general knowledge about the system, the maritime industry will become more robust and resilient than before.

2.5 The academic challenge and opportunity

Based on the industrial challenges and opportunities, there are also academic challenges and opportunities. According to Heering et al. (2021) and Hopcraft and Martin (2018), cyber aspects of maritime education should be implemented as part of STCW-training. To aid the maritime industry with its emerging cyber challenges, academia needs to prepare for maritime cyber resilience training. Universities and educational institutions need to understand how to tackle a problem, which is not only a technical problem, but also could be an attack (Erstad, Lund, et al., 2022). There is a need to think differently when educating (Scanlan et al., 2022), and that there is not a single answer for all cyber problems. This also mean that there is a solid need for more and extensive research in the domain (Bolbot et al., 2022).

In addition to the Resolution MSC.428(98), there are also new requirements to be implemented in the industry and enforced from 01.01.2024, namely The International Association of Classification Societies (IACS) Unified Requirement (UR) E26/27, considering cyber resilience of ships (IACS, 2022b, 2022c). These unified requirements be further described in Section 4.1.2, but the essence is that they will urge academia to be able to train and educate seafarers and workers in the maritime industry to plan for and handle cyber-attacks, for instance using cyber exercises. Incorporating maritime cyber

resilience into navigator training is now imperative. Academia needs to contribute to the industry challenges, and therefore to understand how to educate and train for cyber risks by increasing maritime cyber resilience will be of academic interest. Recognizing the present maritime cyber risk landscape is essential for both academic and professional progression. On the bright side, maritime universities and educational institutions today are well equipped with modern maritime simulator facilities (Hontvedt & Arnseth, 2013; Sellberg, 2017), and should be well equipped to handle the transition towards maritime cyber training.

In addition to be a hub for new knowledge, academia also needs to train tomorrows operators for both present, past, and future problems. It is therefore a need for innovation when considering maritime cyber resilience and according to Gassmann et al. (2013) approximately 90% of new innovations are combinations and reusing of already existing concepts. An approach of combination of theories, such as safety and security, as well as adaption of learning theories and using well known tools, such as maritime simulators, could therefore be reasonable when looking into emerging concepts of maritime cyber resilience. It will be important to build on the existing maritime traditions for education of seafarers, whilst incorporate new knowledge and methods. This section has described some of the technological challenges and opportunities the maritime industry face today, and the next section will describe this thesis research approach for enhanced maritime cyber resilience.

3 Research approach

This section will present the research approach for the thesis, including the philosophical assumptions for the PhD project, the methodology, the methods used and the validity and reliability. There are always different philosophical assumptions in research and to provide a foundation for the research at hand, the philosophical assumptions must be clarified to pave way and the direction of the thesis (Creswell et al., 2018). Figure 5 shows the “Research Onion” by Saunders et al. (2016) as presented by Melnikovas (2018). Despite just a small portion of the available existing philosophies, methodologies, methods and procedures for conducting research, the research onion visually presents the different layers in a research project and illustrate how choices in a project syntehsise from overarching philosophy and down to data collection methods (Melnikovas, 2018).

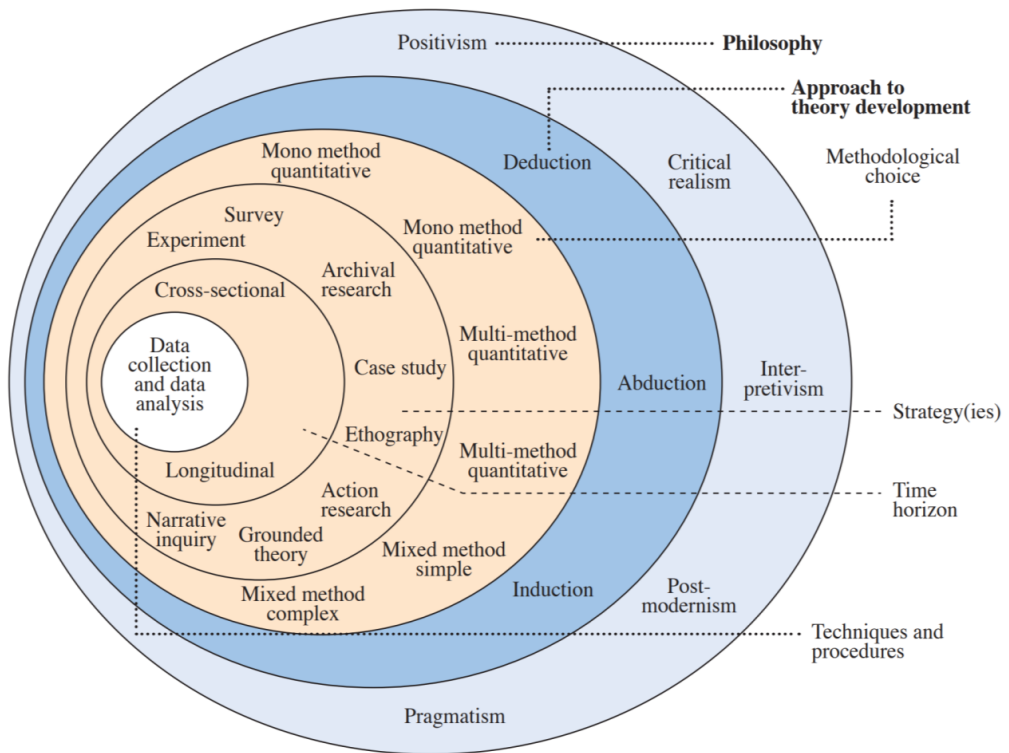


Figure 5 Saunders ‘Research onion’ as presented by Melnikovas (2018).

Creswell et al. (2018) mention four cornerstones of philosophical assumptions to be described when commencing a research project: ontology, epistemology, axiology, and methodology. Ontology considers how the researcher views reality, epistemology describes how the researcher knows this reality and how the researcher believes knowledge is obtained, while axiology describes how the researcher views values, and methodology describes the procedures and boundaries for the study. Considering these aspects, there are several different approaches and philosophical assumptions, such as interpretivism, postpositivism, pragmatism, critical theories, and social constructivism, among others

(Creswell et al., 2018). This thesis falls under the tradition of social sciences and is conducted as a qualitative research project. Further, the philosophical foundation concerning ontology, epistemology and axiology for the thesis will be explained, as well as the specific methodology and methods used for data gathering.

3.1 Ontology and the view of reality

This section present the stance of ontology, focusing on social reality and centring around Searle (2006)'s perspectives. Considering the ontological question, the differences between subjectivity and objectivity are crucial in understanding research, especially considering risk. Objectivity exists independently of observers, while subjectivity depends on them (Searle, 2006). The challenge arises when scientists, viewing risk objectively, communicate with the public who might perceive risk subjectively (Slovic, 1987). Modern maritime operations aim for safety, where the risk is as low as reasonably possible (ALARP). What does an "acceptable level" of cyber risk mean for a navigator? Alexandrova (2012) emphasizes that well-being varies by perception and maritime cyber risk also depends on the point of view for the person experiencing it, as pointed out by Larsen et al. (2022). Hence, using appropriate language in maritime cyber risk research is crucial. The wrong phrasing can negatively skew the research impact. Safety, intrinsically linked with risk, is a paradox. Hollnagel (2014a) suggests safety is about the absence of incidents. A navigator might feel safe, regardless of cyber risk awareness. In studying maritime cyber risk, one can use Searle's social reality concept, equating the absence of cyber risks to safety. This can be seen as a form of collective intentionality.

For navigators, the social phenomenon of operation of navigation and the cyber risk associated with it is important. The operation of navigation can be considered a social phenomenon, in line with Searle's claim regarding social reality. Maritime cyber risk can affect the social phenomenon of navigation. Searle highlights the difference between observer relative and observer independent phenomena. By applying Searle (2006) view on social reality, one can have a starting point of investigating how the maritime cyber risk affects operation of navigation. An ontological subjective phenomenon can both have an epistemic objective and subjective claim (Searle, 2006). Searle argues that social science would not be possible if epistemic objectivity required ontological objectivity. Social phenomena are ontologically subjective but claims about them may be epistemically objective. Claims about ontological subjective phenomenon can both be epistemic objective and subjective. Navigation and maritime cyber risk will in this example be placed under the ontological subjectivity and considered as an observer relative phenomenon, as navigation and cyber threats is invented and created by humans and will not exist independently of human experienced.

3.2 Epistemology and the creation of knowledge

Enhancing maritime cyber resilience requires a nuanced understanding of operational maritime cyber risk, as risk and resilience are similar terms, while similar, are not the same thing (Linkov & Kott, 2019). Ship engineering relies heavily on natural science principles, like physics and mechanics. While quantifiable risks, such as component failures, are assessed using these principles, understanding of maritime cyber risks might demand a more nuanced approach. Unlike traditional risks, such as fire or grounding, cyber risks are intangible and dependent on human threats creating and deploying digital threats. The cyber risks may have physical consequences for navigators, who each uniquely perceive and respond to such risks. Hence, integrating insights from social sciences research projects becomes

vital. While navigators are traditionally trained in natural science, understanding the implications of social sciences can provide a deeper grasp of non-routine challenges. Delving into maritime cyber risk through a social science lens not only offers a comprehensive understanding but also aids in formulating tailored strategies and policies. Research in maritime cyber resilience serves dual purposes: guiding stakeholders and policymakers while also refining educational training. By incorporating social sciences, the industry can gain richer insights, enabling data-informed decisions and strengthening maritime safety.

Risk is difficult to define and it is even argued that it may be best to not have a common definition of risk, but rather let each author define it in their own light (Rausand, 2013). Cyber risk, especially, necessitates a clear conceptual framework, especially when communicating with navigators and seafarers. Cyber risk can be seen as something that exist just because we think it exist (Searle, 2006). A 'cyber risk' is in this thesis defined as a risk that is caused by a malicious or non-malicious threat that exploits cyber space (Refsdal et al., 2015). Herein, 'cyber risk' exploits threats in cyberspace (Refsdal et al., 2015), focused around ship navigation. Different concepts of risk means different things to different people and there is a difference in how scientists research risk and how ordinary people perceive risk (Slovic, 1987). This may create a gap where the scientists to communicate the findings to the public. There is an ongoing discussion in how to measure risk, much because of the different perceptions of risk (Roeser, 2012; Slovic, 1987). This discussion relates to how one should measure and communicate risk, as an objective phenomenon or a subjective phenomenon. It is common in the maritime industry to address risk as something objective, however, in this thesis risk is considered subjective, as cyber risks is dynamic in nature and the individual experiences of navigators. It is important to note that the aim of this thesis is not to address, or judge, whether subjective is superior or subordinate than objective. There are no "one-size-fits-all" solution regarding risk (Rausand, 2013).

Social constructivism describes how the researcher seeks to understand the world which they live in (Creswell et al., 2018). Individuals develop subjective meanings from experience and directed towards things. The goal of such research is to rely as much as possible on participants views of the situation, deriving meanings through interaction with others (Creswell et al., 2018). In constructivism, researchers acknowledge their background and recognize that it biases the interpretation (Creswell et al., 2018).

3.3 Axiology and the role of values

Values play an important role in the social sciences, and their presence is cited as one of the main reasons why the social science did not experience the same success as the natural sciences (Douglas, 2014). Douglas emphasizes that the social science is criticized for being value-laden, making their result seem less reliable. Values play a role in the researchers choosing of direction of research and is a product of the researcher's personal background, such as interests and training, as well as external factors, such as funding. Douglas divides values into legitimate and illegitimate roles. Aesthetic, moral and personal epistemic values are viewed as legitimate roles of value, highlighting the idea that researchers should submerge in their topics of interest because of what they would like to do, that they find the topic morally significant, or are intrigued by them. Conversely, values can affect the direction of research in a negative way, which Douglas calls illegitimate roles of values. It is important for scientists to avoid being tempted to aim to suit their methodology to best fit their wanted result. What results one might find when practicing science should not be altered because one personally has another opinion than the found

evidence. It is important to not ignore or neglect evidence because one prefers it to be otherwise (Douglas, 2014).

Therefore, it is important to highlight the Science-Value coordination, as emphasized by Alexandrova (2012) and Cartwright and Montuschi (2014), to understand what these aspects truly represent. Researchers must engage with the public on the public's terms if they hope to resonate with them. Otherwise, their results might not reach or resonate with their intended audience. Alexandrova poses a pivotal question regarding well-being: "How do we know if these scientists really study well-being, as it matters to us, and not something else?". This query is also pertinent to maritime cyber risk. Alexandrova also discusses the science-philosophy gap. One might argue that this gap directly pertains to maritime cyber risk, given the ongoing dialogue between the scientific theorization of risk and the philosophical understanding of it, as previously mentioned by Slovic (1987). This will be acknowledged, but not delved into deeply within the thesis.

Creswell et al. (2018) notes the importance of positioning oneself and shedding light on bias and background as a researcher, especially when considering what values are brought to a study. As a researcher, I am a former maritime deck officer navigator with in-depth experience in technical maritime risk analysis. Additionally, I have acted as a teacher in maritime simulator courses. It's essential to recognize how these biases may steer the research, forming a foundational philosophical concern of this thesis. This is also why the clarification of the philosophical assumptions, as well as the choice and description of methodology and methods, is important. As I can be considered part of the population which is to be approached and interviewed in this thesis, transparency in the process is key to upholding consistency, integrity, validity, and reliability.

3.4 Research methodology

This section will describe the research methodology for the thesis, which provides a roadmap and present milestones to be achieved (Creswell et al., 2018). As the qualitative research project at hand is explorative and inductive, the research questions, and the project itself can change during the research process (Creswell et al., 2018). According to Melnikovas (2018), deductive approaches are being used when there is existing theory available, whilst inductive is normally used in fields with a lack of research on the topic. It is therefore a need for a flexible and iterative approach, where focus on evaluating the project as it goes is paramount.

The research methodology is based on the philosophical assumption of the research project (Creswell et al., 2018), and in combination with the research objective, it was found that Design Research Methodology (DRM) (Blessing & Chakrabarti, 2009) and the ISO standard 9241-210:2019 'Human-Centred design for interactive systems' (HCD) (ISO, 2019a) fits such an research approach. DRM is a methodological framework for design research and the framework is illustrated in Figure 6. Blessing and Chakrabarti proposed the DRM to systematically approach design research, ensuring it's rigorous and exhaustive. HCD can be seen in contrast to approaches where design is primarily driven by technical or business needs. Instead, HCD prioritizes the user's perspective, ensuring that the end-product or solution is usable, accessible, and beneficial to the target audience. Both methodologies emphasize systematic approaches to design research and development, with an emphasis on understanding the problem space and validating solutions in context. Both methodologies promote an iterative approach.

After testing and validation, insights are looped back into the design process, leading to refinements and better solutions.

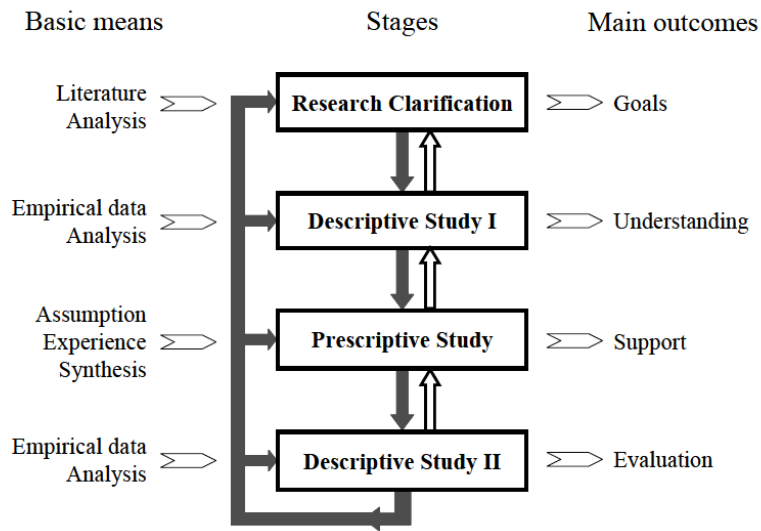


Figure 6 DRM Framework (Blessing & Chakrabarti, 2009, page 15)

Where the methodologies differ might be in their origin and emphasis. While HCD is more explicit about its user-centered approach, DRM provides a broader methodological framework for design research, which can be applied to a wider range of problems, not limited to those directly related to end-users. In practice, elements of both methodologies can be combined for a comprehensive design research approach that is both systematic (as per DRM) and deeply user-centered (as per HCD).

	DRM	HCD
Phase 0	Planning phase	Planning phase
Phase 1	Research Clarification: This involves understanding the problem and establishing the need for a solution.	Understanding and specifying the context of use: Understand the users, their needs, challenges, and contexts.
Phase 2	Descriptive Study I: Observing the current situation and gathering data.	Specifying the user requirements: Clearly articulate the user's needs and problems. Brainstorm potential solutions.

Phase 3	Prescriptive Study: Proposing a potential solution based on observations and tests from the previous phase.	Producing design solutions: Create tangible representations or early versions of solutions.
Phase 4	Descriptive Study II: Validating the proposed solution in real-world scenarios.	Evaluate the design: Validate the solutions with users to get feedback.

Table 1 Overlapping themes for DRM and HCD

DRM and HCD have many similarities and overlapping interest. It was therefore decided to take an approach of a combination of the two, where the DRM acted as the overarching methodology and HCD guides the thesis work. Hence, as the HCD steered the normal, everyday work as a researcher, it will be described more in detail in the following section.

3.4.1 Human-Centred Design

HCD have been utilized in the maritime industry previously (Erstad, Hopcraft, Vineetha Harish, et al., 2023). Before being developed to an ISO standard, HCD was a concept emerging from different fields and were developed from the 1950s and became increasingly popular in the 1980s (Vu & Lützhöft, 2020). HCD is a design standard which ‘provides requirements and recommendations for human-centred design principles and activities throughout the lifecycle of computer-based interactive systems’ (ISO, 2019a). Even if the standard is tailored to aid the design process of computer-based interactive systems, it can also be used as a design philosophy in various projects (Norman, 2013), and can therefore be adapted to research projects. Norman (2013, page 9) emphasize that “designers need to focus their attention on the cases where things go wrong, not just on when things work as planned”, which is relevant for designing resilience strategies against maritime cyber risks.

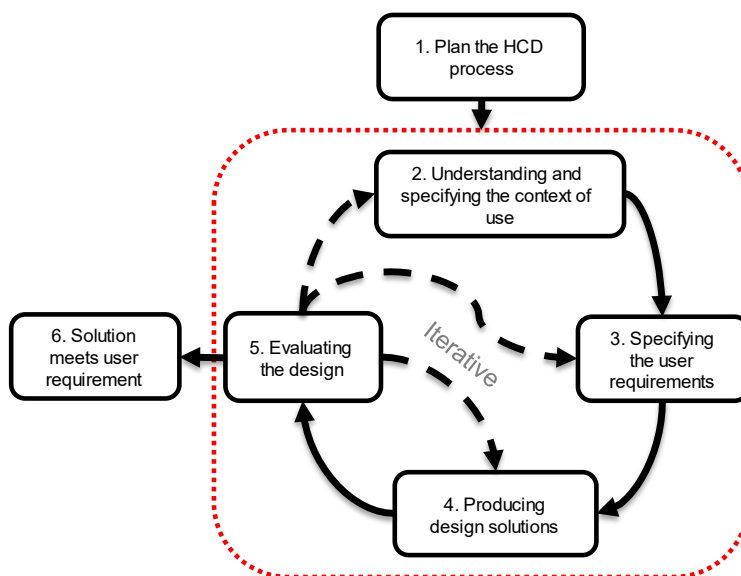


Figure 7 Human-Centred design activities, adopted from (ISO, 2019a, page 12)

Norman (2013) notes that the HCD activities is described in the following order:

1. Observation
2. Idea generation
3. Prototyping
4. Testing

The activities for the ISO standard are the same, but more specified with clearly defined goals and milestones. Figure 7 outlines the overall process and main activities for the HCD process. The HCD process will make the user (in this case the navigator) the centre of the research and focus on the navigator when investigating how one can develop strategies to enhance operational maritime cyber resilience. There is also an emphasis on that the process is iterative. This means that each step of the process is meant to be continuously evaluated to provide feedback to the process and if there is room for improvement or adjustment of the way forward.

Norman (2013) mention that one shall strive to solve the ‘actual’ problem, and not just the anticipated problem. Lützhöft and Vu (2018) notes that design (when done right) enhance safety, but still there are some potential challenges to be aware of. Although users must be involved, they must not be considered co-designers, as users may not be aware of their needs and can make false assumptions of their actual needs. If not considered, the solution may result in overly complex designs (Lützhöft & Vu, 2018).

In this project, the focus is on the navigator and how to help them understanding maritime cyber risks and eventually overcome cyber incidents. The HCD process also emphasize to include a range of stakeholders as well as testing prototype design, to give feedback to the iterative process. It is found throughout the thesis work that it is as important to aid the stakeholders in how they can learn to prepare themselves and aid the navigators for cyber risks.

3.5 Research methods

This section will present the specific research methods which have been utilized in the thesis. The methods are based on qualitative research approach will heavily rely on the inclusion of people external to the project. When doing qualitative research with, for, and about people, there is strict regulations for research ethics (Ringdal, 2018). All process for handling information which can consider privacy as well as how to gather and store data, were pre-approved by the Norwegian Centre for Research Data (NSD) (Notification Form 364232 and 422483) and handled according to relevant regulations. There have also been signed NDAs with maritime organizations throughout the project. These are crucial steps of the research project, as the integrity of the researcher is particularly important. The NSD forms can be found in Annex VI – NSD forms.

The selection of people to participate in the research project was from several segments in the maritime industry. The participants were from academia, sailing crew, ship owner personnel, naval academies, maritime insurance, maritime classification companies and maritime technology companies. Some people attended everything, from single interviews to focus groups and simulator experiments, and others participated on single events. There were planned not to be dependent on single persons, due to the progress and time limitation of the project.

In addition to be based on the research methodology, the research methods was also founded on the research questions. Figure 8 indicates how each method relates to each research question and each research paper presented in the thesis.

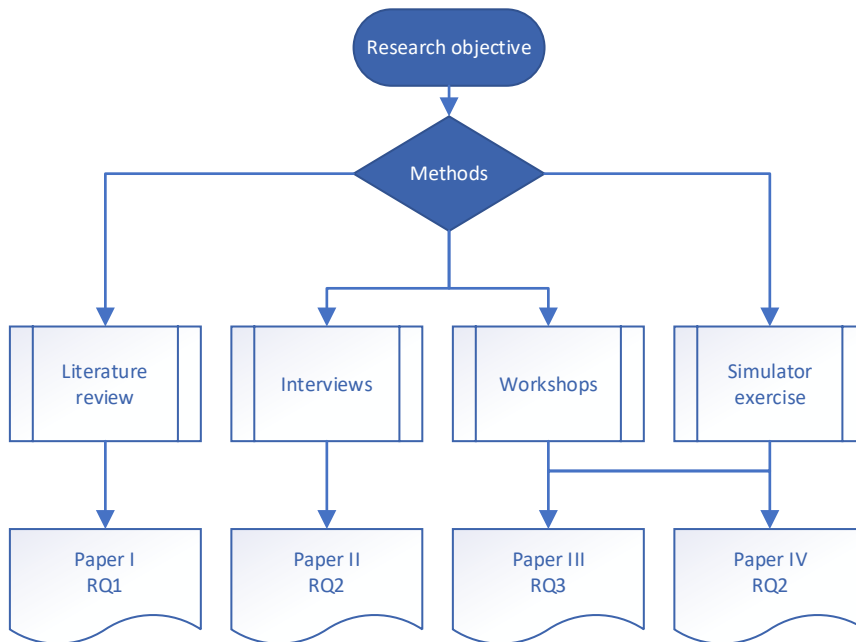


Figure 8 Research methods

3.5.1 Literature review research

An important aspect of any study is the literature review (Blessing & Chakrabarti, 2009), as the literature review contains information about the theoretical background, learning from the breadth of research which exists, as well as it synthesise the writers understanding of the topic at hand (Okoli & Schabram, 2010). The literature studies provide the foundation for the RQ1, which is answered through Paper I and Section 4 in this thesis.

As the research field of maritime cyber security and resilience is expanding rapidly, both conventional (semi-structured) literature review and a systematic literature review (Okoli & Schabram, 2010) have been conducted. Since the start of the PhD project, there have been undertaken a conventional literature review, constantly searching for new literature considering cyber research in the maritime domain. Databases available both for the specific university and for the public have been regularly searched, covering such as Oria (NTNU University Database covering many other databases as well) and Google Scholar. In addition, to be certain to cover the essence of maritime cyber resilience research, there have been performed a standalone structured literature review (SLR), which forms the basis for the maritime cyber resilience section in the theoretical foundation section.

It is important to uphold consistency, transparency, and integrity in a literature review. There are several different SLR methods to choose from, but Okoli and Schabram (2010) guide to a SLR was chosen as a method, as the guide is suited for information system research, which Okoli and Schabram (2010) claim is a combination of social science, business, and computing science. This means that this guide should fit the research area of maritime cyber resilience well, as it can be considered a combination between computer science and social science, in this thesis. The basis for the search strings were founded on the research question and the sub-research question for the review. The original search string was: (maritime and cyber AND (resili* OR safe*)). This means it should catch all papers relevant for maritime cyber resilience and all papers concerned with maritime cyber and safety, meaning it should cover maritime cyber security research which have some form of direct interest for safety. The aim of this thesis is to enhance maritime cyber resilience, and the reviewed paper should have some form of relevance to the aspect. This means that the papers for review must:

1. Must have relevance for conventional navigational operation of vessels (. i.e., excludes autonomous vessels)
2. Must consider aspects of maritime cyber resilience, including but not limited to:
 - Operational handling of cyber situations (anticipate, withstand and recover)
 - Training/educating to overcome cyber situations (evolve)

Extensive information for the SLR can be found in Annex II – Additional SLR, and the results is presented in Section 4.

3.5.2 Qualitative interviews

A key element in HCD is to include the specific users in the development process, so inviting navigators to a one-to-one interview. RQ2 focuses on “Specifying the user requirements” and intends to find out what is required to enhance maritime cyber resilience in maritime operations, which forms the foundation for Paper II. Using qualitative semi-structured interview described by Creswell et al. (2018) was chosen as a method to get the individual perspective from the users.

Paper II focused on interviews with navigators and as an interviewer it is important to follow good interview practice (Creswell et al., 2018). The participants were chosen as all had experience and knowledge of cyber threats, and all participants are navigators holding a deck certificate, actively sailing or not, still working in the maritime industry. Nine interviews with ten navigators were undertaken. One of the interviews was also an interview of two people at the same time, as they had experienced the same cyber incident onboard the same vessel. The interviews were conducted both in-person and digitally. The interviews were designed as qualitative semi-structured interviews conducted in Norwegian, as the navigators is from Norway. The interview was recorded on a separate recording device, and the data were stored safe according to the NSD approved plan. The interviews were analysed using Systematic Text Condensation method (STC) (Malterud, 2012), described further in Erstad, Lund, et al. (2022). This correlate well with HCD, as it emphasizes that the designer or researcher should figure out what the user needs, not necessarily how to achieve the need. The interview guide can be found in Annex III – Interview guide.

3.5.3 Workshops with focus group interviews

To vary the input to the project, focus group interviews was an additional data gathering method that was used. Focus groups is interviews (i.e., conversations) with several persons simultaneously, and is advantageous to use when time is limited (Creswell et al., 2018). It was arranged two workshops with focus group interviews throughout the PhD project; the first was intended to gather data for the foundation for training is necessary for maritime cyber resilience exercises and the second was for validating and discussing the results. This part of the project served multiple phases of the HCD project. First, it was added as extra data, to be evaluated against the interviews. Second, it is a difference between what a user want and what a user need, and it is valuable input to the process to get stakeholders perspectives (ISO, 2019a). Finally, evaluating the process is important in HCD (ISO, 2019a), and both workshops was aimed to be a evaluator for the project, to map out if there was a need for any adjustments. In addition, the workshop also served the opportunity to gather people from the industry, with the intent to give something back, as the research project is dependent on industry input and perspectives. In contrary to the one-to-one interviews described in the previous section, it was easier to recruit people from the maritime industry to the focus group workshops. More people seem more willingly to show up and talk about maritime cyber issues when other people from the industry also was invited, compared to of single interviews. Creswell et al. (2018) notes that focus groups interviews may be advantageous if individuals hesitate to answer on one-to-one interviews, not implying that it was the case for this thesis.

The focus groups interviews were audio recorded. The workshop participants were split into three separate groups and all groups were supposed to discuss aspects of the workshop scope. Two out of three groups in both workshops were speaking Norwegian and the last group were speaking English. The facilitators for the three groups were instructed to not actively participate in answering questions, but rather asking questions which fits with the workshop scope. The workshop day was divided into three parts, beginning with a lecture, before conducting two 10–15-minute simulator scenarios, before an audio recorded discussion workshop. The transcription was not a detailed, in-depth transcript of what all the participants said, as the participants discussed many aspects not relevant for the workshop scope. Instead, what was found to be of importance to the scope was noted and later synthesised into one document.

To make industry actors participation worth-while, it was found best to give them something in return, for showing up and providing valuable input. Therefore, it was decided to hold a short lecture about potential cyber security risks in the maritime industry before the participants in the workshop were introduced to some inspirational simulator scenarios, in advance of the actual workshop. The simulator scenarios are described in the workshop report associated with this thesis (Erstad, Larsen, et al., 2022). There is always a risk of biasing when holding a lecture and simulator exercises before the workshop, so the lectures and the exercises was designed to be as general as possible but still embracing the overarching challenges of maritime cyber resilience.

3.5.4 Simulator exercise and training

A crucial step in ISO (2019a) is considering the producing design solutions. Design decision have a major impact on user experience (ISO, 2019a) and it will form how the user and the stakeholders value the designers integrity after the end result. It was therefore decided to hold simulator demonstrators and

implement the simulator exercises which was developed into a M.Sc. level course. The simulator exercises were presented at one internal shipowner conference (approximately 90 people involved), one open conference for shipowners (approximately 200 persons) and through a M.Sc. level life-long-learning course at NTNU (approximately 20 persons). The M.Sc. level course were developed together with a fellow PhD student at NTNU, and consisted of a six-day course, where two full days was dedicated to simulator exercises. The last day was combined with the workshop focus groups, as described in the previous section.

Simulator training and exercise is a well-known and well proven method of learning in the maritime sector (Hontvedt & Arnseth, 2013; Sellberg, 2017; Sellberg et al., 2018). The briefing and the debriefing is the most critical and important phases of a simulator exercise (Sellberg et al., 2018), which is to be emphasized in the simulator exercises. The foundation for the simulator exercise is described in detail throughout Paper III.

3.6 Validity and reliability

A crucial part of any research project is to understand if the results are valid and reliable. Validation considers the accuracy of the chosen method and puts forward if the results present what they are supposed to present. Reliability refers to the consistency of a method and considers if the results of a study can be reproduced and yield the same results. This section will describe how these aspects is ensured and transparent throughout the project (Creswell et al., 2018). Creswell et al. (2018) emphasize that it might even be possible to not find a “right/correct” answer in a qualitative study, hence it is even more important with transparency.

Considering reliability, the consistency of the results is important and so is the question of whether the researcher have special knowledge about the subject or not (Tjora & Tjora, 2021). This is stated in Section 3.3 Axiology and the role of values, where the authors background is described. Transparency and the question of whether the results can be reproduced or not is also important (Creswell et al., 2018).

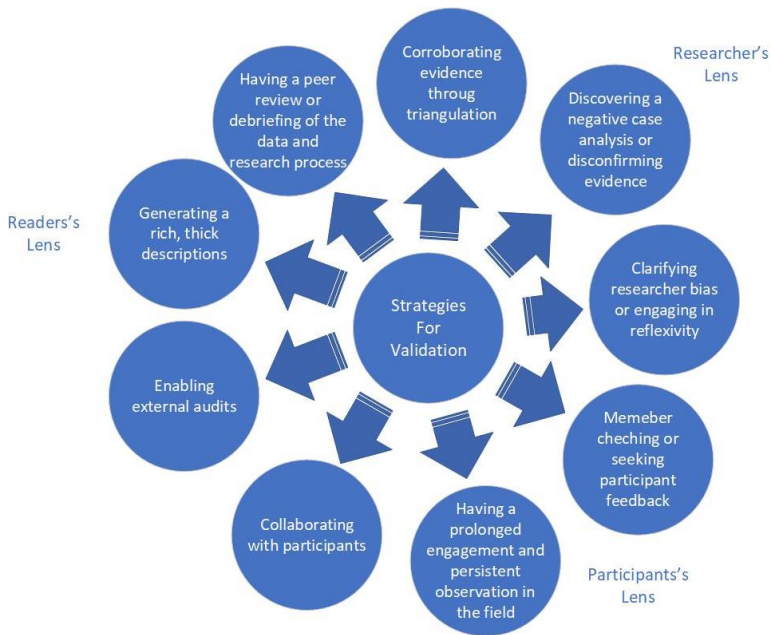


Figure 9 'Strategies for Validation in Qualitative Research', adopted from Creswell et al. (2018, page 260)

Creswell et al. (2018) emphasise triangulation when validating data to establish credibility. Figure 9 shows different strategies for validation in qualitative research and the HCD evaluation process, covering both including of industry participants, interviews, workshops, and simulator scenarios, will be important when considering verification and validation. This thesis aims to uphold the validity through the following:

- Researcher's lens
 - "Clarifying researcher bias or engaging in reflexivity":
 - This have been stated in the previous section considering the axiology.
 - "Corroborating evidence through triangulation"
 - Triangulation is ensured by undertaking literature review, interviews, focus group workshops and simulator experiments.
- Participant's lens
 - "Collaborating with participants"
 - By using the HCD method, the projects ensure active engagement of participants.
 - "Member checking or seeking participant feedback".
 - Feedback is provided by utilizing interviews, focus group, workshop and simulator exercises.
- Reader's lens
 - "Generating a rich, thick descriptions".
 - The thesis aims to provide thick (i.e., thorough) descriptions for the reader.
 - "Having a peer review or debriefing of the data and research process".
 - Papers in this thesis is peer reviewed.

Specific validation for each of the scientific peer-reviewed papers:

- Validation for Paper I:
 - There is conducted an up-to-date literature review for validation of the results. In addition, the qualitative interviews and focus group workshops validates the importance of the topic of maritime cyber resilience.
- Validation for Paper II:
 - Understanding the users' perspectives is a vital part of the HCD process. However, it is a difference between what the user wants and what the user needs. Therefore, as a parallel activity to this paper it was planned a workshop with maritime industry actors and stakeholders. The workshop reports itself serves as a validation of Paper II, and the paper serves as a foundation for Paper III as well as it has given input to the M.Sc. course.
- Validation for Paper III
 - Validation for Paper III is conducted by simulator scenarios in the M.Sc. course and Workshop II. After the course there where held a poll amongst the students, which says that they are positive to simulator training, and that the students experience a learning outcome, even if they are not educated as navigators. Results of the poll is presented in Annex IV – .
- Validation for Paper IV:
 - In contrary to Paper I, II and III, there is no practical validation for Paper IV. Paper IV is validated on a theoretical level by input from nautical lecturers at maritime universities. In addition, Paper IV is developed in close collaboration with industry experts and Norwegian maritime authority representatives.

4 Theoretical foundation

This section will present the theoretical foundation which is relevant for the thesis. Maritime cyber resilience is founded on safety, cyber resilience, and maritime cyber security. This section will first describe how cyber security is treated in the maritime industry and in research today, before describing relevant industry frameworks. Further, resilience will be described and how the concept relates to safety, then describe how it develops to cyber resilience. Further, the results from a literature review of maritime cyber resilience will be presented, before the theoretical foundation closes by investigating maritime training and education.

4.1 Maritime cyber security

The Resolution MSC.428(98) (International Maritime Organization, 2017b) could be considered as a paradigm shift in the maritime industry considering maritime cyber security. According to Cambridge Dictionary a paradigm shift is ‘a time when the usual and accepted way of doing or thinking about something changes completely’. MSC.428(98) was adopted as an Annex to the ISM code in 2017, adding the aspect of maritime cyber risk into a vessels SMS. In short, MSC.428(98) states that maritime cyber risk must be addressed appropriately in SMS no later than 1 January 2021. Ironically, the shipping industry were shocked by a major cyber-attack in 2017 as described previously. Moeller-Maersk is a global company with offices all around the world and ships sailing inter-continental. Even though it did not cause safety related problems for Maersk ships, the incident made an impression on the maritime industry. This section will investigate how maritime cyber security develops in research and how the concept is treated by the industry on a regulatory level.

4.1.1 The development of maritime cyber security in research

Maritime cyber security has gained increasing interest in the maritime industry and research the last decade. As maritime cyber security is a tactical field of interest when considering botch attack and defence, it would be reasonable to believe that militaries and coast guards around the world have investigated maritime cyber security issues years before the merchant fleet caught interest. For instance, United States Coast Guard released a proceedings report in 2015 which considers many aspects of maritime cyber security, such as cyber risks, social engineering, zero-day-vulnerabilities and solutions for enhanced maritime cyber security and resilience (COAST GUARD WASHINGTON DC, 2015). This is important to bear in mind, even though military aspects are out of scope of the thesis. For merchant vessels and civilian research institutions, Bolbot et al. (2022) notes that maritime cyber security research has gained increased attention from 2012 and the number of publications considering maritime cyber security really began to increase in 2017, with a wide range of research topics, as shown in Figure 10.

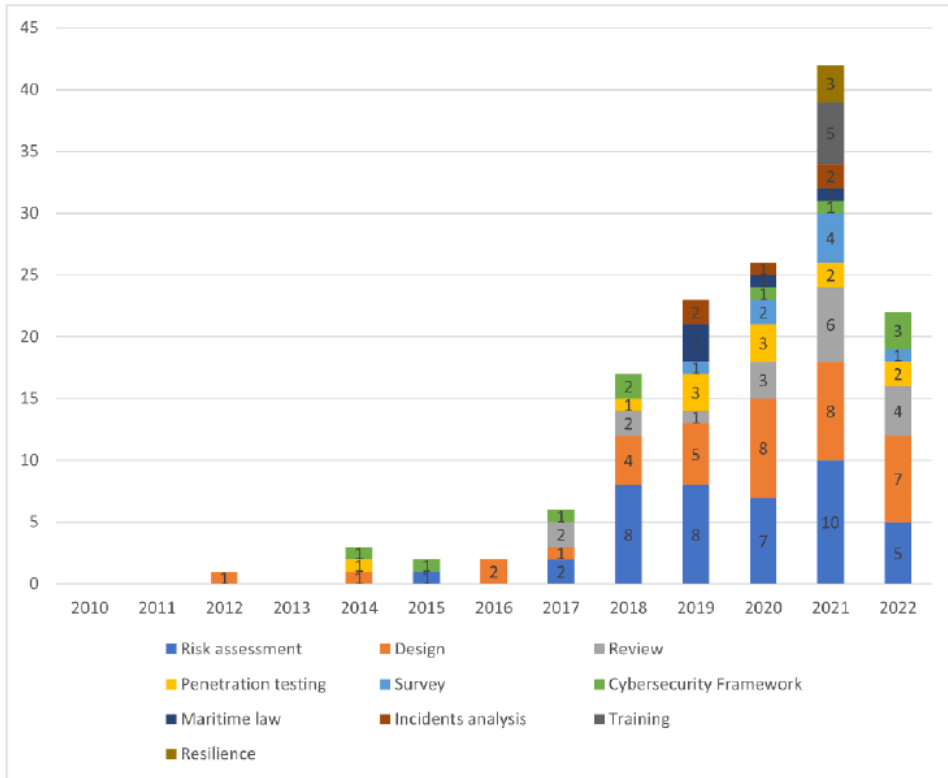


Figure 10 'Analysis of historical trends' (Bolbot et al., 2022, page 8)

Cyber incident in the maritime industry have also increased since 2015, as shown in Figure 4 'Incidents per year' (Meland et al., 2021), which correlates with Figure 10. Boyes (2014) describe IT systems onboard ships, the maritime cyber threat picture and the address the lack of awareness in maritime cyber security and emphasise that cyber security should be an integral part in training programs for all mariners. DiRenzo et al. (2015) noted that maritime cyber security is a problematic field of research and that the research is itself is not well studied, which correlate with Bolbot et al. (2022) findings. Jensen (2015) noted the challenges in maritime cyber resilience with an emphasis on the complexity of the industry and proposes that the maritime industry develops best practice guidelines to improve the situation. Fitton et al. (2015) highlights challenges in the maritime domain, including ships, ports, and logistics, and purposes a holistic approach to study maritime cyber security, with an emphasis on information, technology, and people. Bolbot et al. (2022) states maritime cyber security has recently become an intense research area and the leading countries in research are Norway, the United Kingdom, France, and the USA based on the weighted number of authors. The different research topics are presented in Figure 10.

To understand how maritime cyber security is treated in research today, it is important to take a step back and look at the origin of the theme. Cyber security derives from information security, and Von Solms and van Niekerk (2013) notes that information security sometimes only considers technical aspects, such as ICT (Information and Communication Technology, i.e., computers, networks, cables)

and argue for the importance of including human aspects. There are various definition of both and Von Solms and van Niekerk (2013) notes that information security usually define properties or characteristics that secure information should have. Von Solms and van Niekerk (2013) refers to Whitman and Mattord (2009) when considering what information security and cyber security is actually protecting. Whitman and Mattord (2009) notes that the protection of the Confidentiality, Integrity, and Availability (CIA triangle/triad) is important. What differs cyber security from information security is how the protection is covered, as protection of information security traditionally have only considered technical aspects, cyber security goes beyond the definition and include functions in cyberspace, as well as users and assets. Von Solms and van Niekerk (2013, page 101) concludes with a definition of cyber security as ‘cyber security can be defined as the protection of cyberspace itself, the electronic information, the ICTs that support cyberspace, and the users of cyberspace in their personal, societal and national capacity, including any of their interests, either tangible or intangible, that are vulnerable to attacks originating in cyberspace’. Hareide et al. (2018) argues that cyber security is context dependent and that it is necessary with a separate working definition for the maritime sector. In the maritime industry and on-board ships, ICT systems is more specified to the working environment, as information systems, computers, and network both handle administrative information, but also control physical processes. It is divided into IT (Information Technology) and OT (Operational Technology) systems. IT systems cover information processing systems and the software and hardware which makes the system work, whilst OT systems consider computer and cyber systems which monitor and control physical processes on the ship, for instance the rudder control system or engine control system (BIMCO, 2020). Hareide et al. (2018, page 3) expands Von Solms and van Niekerk (2013) definition by including the aspect of maritime security and explain maritime cyber security as ‘a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems, particularly concerning integrity and availability. In addition, MCS is concerned with the reduction of the consequences of cyber-attacks on maritime operations. Thus, the means of MCS are not merely technological, but also consist of information and people’. Von Solms and van Niekerk (2013) also emphasise that even though the aspects of the CIA triad is equally important, the weighting of the factors may differ depending on the scenario, which aligns with Hareide et al. (2018) standpoint. This is also emphasised by BIMCO (2020), which explains that integrity and availability is more important for ship systems than confidentiality. Several other papers address the challenges for maritime cyber security in the CIA triad (Boyes, 2014; Radmilo et al., 2017), amongst others.

In addition to Bolbot et al. (2022), there have also been conducted several other literature reviews of maritime cyber security the recent years, defining how maritime cyber security research have developed. Farah et al. (2022) conducted a literature review in Science Direct, Springer and IEEE and found relevant papers dated back to the 1990s. However, the papers before 2010 mostly consist of papers directed towards technological aspect of computer networking, topology and challenges, before the focus in research shifted towards cyber security. Farah et al. (2022) further provides a thorough introduction to maritime cyber security, providing an overview of recent cyber-attacks in the industry, proper overview of vessel/port infrastructure and onboard vessel systems, communicating types and network architecture. Afenyo and Caesar (2023) performed a literature review from 1970 to 2022 Web of Science and Scopus, where most of the relevant cited papers was after 2010. An finding to be mentioned in this literature review was Shah (2004), which explores the landscape of maritime cyber security in the wake of International Ship and Port Facility Security Code (ISPS) which was a result in the wake of the September 11th attacks in the United States of America. However, Shah (2004) takes a

more business and governance focus than what is the focus of this thesis. Further, Park et al. (2023) have conducted a literature review of in SCOPUS of documents related to the maritime industry. Park has identified six dimensions to categorise the maritime cyber threats, which are “Phishing”, “Malware”, “Man in the middle attack”, “Thief of credentials”, “Human factor”, and “Using outdated IT systems” (page 3). Park et al. (2023) identifies “Lacking knowledge of cybersecurity” as a core threat and highlight that education, training and awareness in human factors is key for reducing the risk. Another literature review is performed by Schinas and Metzger (2023) which highlights many important papers in the research field of maritime cyber security. The paper provides an interesting discussion cyber-seaworthiness and produce a list of seven bullet points of what is needed to claim that a ship is cyber-seaworthy, which for instance mentions that every crew member should be trained on cyber risks and system vulnerabilities for the systems they operate or maintain. In 2023, Yu et al. (2023) published a literature review of maritime cyber security. The paper then discusses several important research papers on maritime cyber security and recognizing the cyber vulnerabilities onboard ships, despite mentioning several limiting factors, such as the lack of proof of real-life cyber-attacks and that the reviewed approaches are theoretical approaches. The paper highlights mitigating factors of maritime cyber risk, and emphasize human factors and training are a key element, amongst other organizational and technical factors. The paper concludes with that maritime cyber security is a multidisciplinary subject, with both opportunities and challenges for researchers and the maritime industry for the years to come (Yu et al., 2023).

In addition to academic research, the maritime industry is also investigating the aspect of maritime cyber security through the use of industry frameworks and guidelines. The following section will explore the different industry and governance frameworks important for maritime cyber security in the maritime industry today.

4.1.2 Industry and governance frameworks for maritime cyber security

Today, the ISO 27001 standard is one of the most known information and cyber security standards. Without considering a specific sector, ISO 27001 provides a framework and guideline for establishing, implementing and managing an information security management system (ISO, 2017). Several of other frameworks refers to ISO 27001, which will be explained further in this section. The standard is broad and considers many aspects of information security and is not an industry specific cyber security framework. As mentioned in the previous section, the maritime industry is different from other industries and thus needs a more specified approach towards managing maritime cyber risks. IMO have published “MSC.FAL-1/Circ.3 Guideline on Maritime Cyber Risk Management” (International Maritime Organization, 2017a), which is referred to in the Resolution MSC.428(98) (International Maritime Organization, 2017b). The guideline acknowledges the diversity of the maritime industry and recognizes that no two organizations in the shipping industry is the same, which means that there is no one-size-fits-all solution. The guideline refers to the ISO 27001, as well as the BIMCO (The Baltic and International Maritime Council) ‘Guidelines on Cyber Security Onboard Ships’ and the NIST (The National Institute of Standards and Technology) ‘Framework for Improving Critical Infrastructure Cybersecurity’. NIST has created a cyber security framework that is modular and customizable. It operates on five core functions: Identify, Protect, Detect, Respond, and Recover. Designed as a U.S. federal standard, it has been globally adopted and focus on compliance with regulatory requirements and industry-specific concerns (NIST, 2018). Even though the framework is specified and comprehensive, it is not tailored to the maritime industry or ships. Therefore, BIMCO Guidelines have

published an industry-driven and practical approach to managing vulnerabilities both on ships and in shore-based operations. It includes recommendations for cyber risk assessment, the human element, and ship-to-shore interface. Its industry-centric approach makes it particularly relevant for maritime operators globally (BIMCO, 2020). Both ISO27001, the NIST framework and BIMCO is mentioned as best practice for implementation of cyber risk management in the IMO cyber risk management guidelines (International Maritime Organization, 2017a).

In contrary to the Resolution MSC.428(98) which is a requirement for ship operators, ISO 27001, NIST and BIMCO is per definition not a requirement for operating a ship, even though they are used as industry best practice standards. In 2022, International Association of Classification Societies (IACS) have published new Unified Requirements (UR) E26 Cyber Resilience of Ships (IACS, 2022b) and E27 Cyber resilience of on-board systems and equipment (IACS, 2022c), will be mandatory for all newbuilds which are classified by a IACS member after 1st January 2024. As IACS covers most of the world fleet of merchant ships, this will have global impact (IACS, 2022a). Previously, IACS have published the ‘Rec 166 – Recommendations on Cyber Resilience’ (IACS, 2020) which experienced less success than for instance the BIMCO guidelines. In contrary to UR E26 and E27, Rec 166 is not mandatory for classifying a ship.

There is also many other frameworks in the maritime industry, such as ENISA (European Union Agency for Cybersecurity et al., 2020) and NIS 2 Directive (European Union Parliament, 2022), but as these focus more on port security and governance level aspects and will be acknowledged but not investigated in detail in the thesis. NIST is also in September 2023 working on an update of the NIST Framework, which is drafted and aims to be ready in November 2023 (NIST, 2023). One of the main differences from the first framework is that it includes another core function, Govern, which considers a more organizational and management perspective to cyber security. As this framework is not yet published, and will be subject for changes, it will not be considered further in the thesis.

It is important to understand how the resolutions, guidelines and framework mechanisms in the maritime industry works, but as this thesis focuses on maritime cyber resilience rather than maritime cyber security, it is also necessary to investigate other suitable frameworks, such as the MITRE Cyber Resilience Framework (Bodeau et al., 2011). The MITRE Framework focuses on designing systems to be resilient to cyber threats rather than solely focusing on security measures. It spans enterprise architecture, system architecture, and operations and a key contribution is the shift towards cyber resilience, which aims to ensure that the system can adapt and recover from cyber-attacks. While not maritime-specific, it can be adapted to suit the unique requirements of maritime operations. The MITRE Framework is not vastly different from the NIST Framework, however, the focus is slightly different, as MITRE focus on resilience and NIST focus on security. Even though the terms are similar, they are not the same, as cyber security focuses on protecting against cyber threats, cyber resilience focuses on an organization's ability to handle cyber threats (Bodeau et al., 2011; NIST, 2018). MITRE defines cyber resilience as ‘the ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function’ (Bodeau et al., 2011). As this thesis is focused on the concept of maritime cyber resilience, the concepts of resilience and cyber resilience will be investigated further in the following sections.

4.2 Resilience and safety

The concept of resilience can be traced back to the roman empire and is addressed by several fields of science, such as ecology, psychology and health science (Bergström et al., 2015). de Bruijne et al. (2010) notes that in the recent century, resilience first appeared in psychology in the 1940s and 1950s, where studies of how humans coped with stressful implications or disorders, and that it was explored in the 1970s in the research field of ecology. According to a Horizon 2020 research project, there are numerous papers describing resilience and there are over 300 different definitions of resilience (Woltjer et al., 2015). Resilience have been used as a buzzword (Boin et al., 2010), and de Bruijne et al. (2010) emphasise that the concept of resilience is not clearly defined and must be understood with different meanings in different disciplines. The term varies in the different disciplines and research fields, and it is out of the scope of the thesis to provide a full untangling of the definition.

A research area the recent decades relevant to the maritime safety research is resilience engineering (Lutzhof & Oltedal, 2018; Lützhöft et al., 2006; Schröder-Hinrichs et al., 2016). In an ecology perspective, Holling (1973) defined resilience as a systems ability to absorb variable changes and still persist, which can be described as the emergence of the resilience engineering definition (Hollnagel et al., 2006; Schröder-Hinrichs et al., 2016). Schröder-Hinrichs et al. (2016) argues for the implementation of introducing resilience engineering into maritime safety, where the emphasis is on that the maritime industry have traditionally been a reactive and slow industry. Schröder-Hinrichs et al. (2016) further notes that the maritime industry is getting ever more complex, by for instance the implementation of modern technologies, and argues for that proactive and resilience engineering perspective in the maritime industry would benefit maritime safety. In a literature review Righi et al. (2015) describes resilience engineering research areas and trends. Righi et al. (2015) notes that “safety management tools” is a relevant research area for resilience engineering and involves risk assessment, identification and classification of resilience, analysis of accidents and training. As safety management (i.e., ISM code) and training (i.e., STCW code) is cornerstones in the maritime industry, this thesis and section will focus and investigate the past decades development of resilience engineering within the field of safety.

Resilience engineering have shifted safety science focus on errors towards focus on normal processes, where the emphasis is about operational success and study of normal work, more than errors and accidents (Bergström et al., 2015). Patriarca et al. (2018) have undertaken a comprehensive literature review of resilience engineering and describes resilience engineering encompass a paradigm shift of switching from accidental reactive accident handling perspective, to a proactive “normal work” perspective (Patriarca et al., 2018). According to Hollnagel (2014a) the previous focus can be called accidentology, where the idea is that safety is equal to no accidents. Hollnagel (2008) describes the traditional (i.e., historical) response to accidents mainly consist of reactive barriers to eliminate risks, which can create an illusion of safety. He further argues that barriers are effective against known threats (i.e., reactive measures), yet ineffective against irregular and unexampled threats (Hollnagel, 2008), such as a cyber threat. Resilience engineering considers looking into how an operation is done by addressing situations or conditions where they can occur (Hollnagel, 2008). Resilience engineering is defined as ‘the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under both expected and unexpected conditions.’ (Hollnagel, 2010). Hollnagel (2010) describe for cornerstones of resilience:

- Anticipate: To be able to understand developments of a future state of a system.
- Monitor: To be able to monitor its own performance and changes in the environment.
- Respond: To be able to understand what to do when a disruption happens in a timely and effective manner.
- Learn: To be able to understand what has happened and learn from experience, emphasizing what is important to learn (rather than easy to learn) to be better prepared for future events.

Hollnagel (2013) divides the reactive and proactive safety approaches into Safety-I and Safety-II, where Safety-I is the traditional reactive approach and Safety-II should consider what goes right in a situation by understanding what really is going on and hence is proactive. It is important to note that Safety-II is not a replacement of Safety-I, but rather a complementary view on safety (Hollnagel, 2014c, page 178). Hollnagel (2013) describes the basic differences between the concepts in Table 2, and Madni et al. (2020, page 4) presents a visual explanation of resilience in face of a disruption in Figure 11.

	Safety-I	Safety-II
Definition of safety	That as few things as possible go wrong	That as many things as possible go right
Safety management principle	Reactive, respond when something happens	Proactive, try to anticipate developments and events
Explanations of accidents	Accidents are caused by failures and malfunctions	Things basically happen in the same way, regardless of the outcome.
View of the human factor	Liability	Resource

Table 2 'Basic difference between Safety-I and Safety-II' (Hollnagel, 2013, page 8)

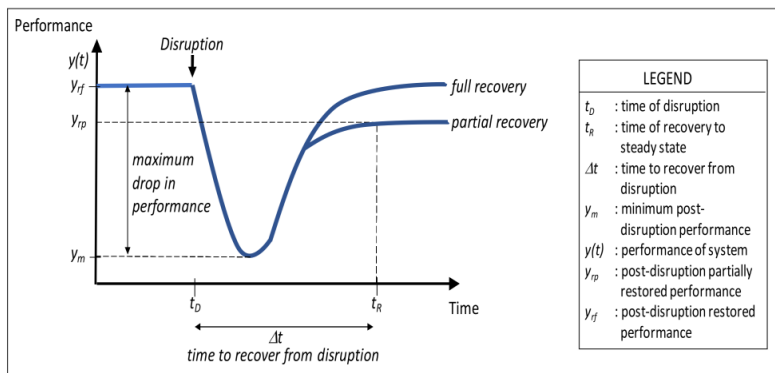


Figure 11 'General form of resilience curve for resilience defined as rebound.' (Madni et al., 2020, page 4)

Resilience engineering is a complex and evolving field, and there is no clear definition of what it means. This lack of a clear definition can make it difficult to apply resilience engineering principles in practice (Righi et al., 2015). There is an ongoing debate about whether or not there is a need for resilience, when

other theories are available, such as high reliability theory/high reliability organisations (HRO) and cognitive system engineering (CSE) (Bergström et al., 2015). HRO were developed through the 1980/90s, and RE was developed as a concept mainly after the 2000's, both history of the concepts is developed in the wake of the Three Mile Island accident in 1979 (Le Coze, 2019). Le Coze (2019) highlights the differences and similarities between the two schools, emphasising that both have contributed to the science of safety. Safety-I and Safety-II have also met critiques, such as Leveson (2016), where she write that Safety-I does not exist in reality as described by Hollnagel and that Safety-II is to focused around the human operator and that the design of the system around the human seems to be ignored. While the other theories and perspectives on resilience engineering are acknowledged, they will not be explored further as it is outside the scope of the thesis. This section has investigated the origins of resilience and the aspect of resilience engineering. The next section will investigate cyber resilience, as the next cornerstone in maritime cyber resilience.

4.3 Cyber resilience

As described in Section 4.1.2, the maritime industry intends to incorporate resilience principles through IMO Guidelines, BIMCO and the NIST framework, as the purpose of NIST Framework is to provide organisations with tools to improvise cyber security and resilience, regardless of the cyber security risk (NIST, 2018). Even though NIST (2018) mention resilience, the framework does not success to fully address it as a concept. Linkov and Kott (2019) notes that traditional risk assessment methods and the traditional approach of hardening cyber and IT systems are only partially sufficient, as cyber threats pose very unpredictable and introduce extreme uncertainty, thus, there is an imminent need for resilience in cyber systems. Björck et al. (2015) discusses the objective cyber resilience in contrast to cyber security and emphasise that the terms differ, as cyber resilience focus on keeping business goals intact, where cyber security encompasses the protection of IT systems. Thus, Björck et al. (2015) argue that the starting point from a cyber resilience perspective must be on business goals and continuity, rather than the IT systems. While the intention of cyber security is to build fail-safe systems, cyber resilience must acknowledge that any system can fail and rather highlight the importance of the ability to fail in a controlled manner (Björck et al., 2015). This aligns with Linkov and Kott (2019), describing that reaching a state of security is being free from danger and threat, which is not possible in a resilience lens. Such a state (free from danger / 100% safe or secure) is unreasonable when considering resilience, as the concept of resilience is about respond to an event and return to normal state as soon as possible (Hollnagel, 2014b). A protective measure, such as introducing more redundancy, more systems, more networks can increase the cyber resilience of a system, as it will increase the complexity of the system. However, it can at the same time decrease the cyber resilience, as the increased complexity can cause confusion for a human operator (Linkov & Kott, 2019). This thesis will focus on frameworks which specifically address cyber resilience, rather than cyber security.

The Danish research project CyberShip (Cyber resilience for the Shipping industry) (Estay, 2020) aim to propose a theoretical framework to aid decision-making for preventing and reacting to cyber-attacks in the shipping industry. The project focus more on a supply chain and management perspective than is relevant for this thesis, but a vital part of the project was to investigate the status of cyber resilience frameworks available in research, as presented by Sepúlveda Estay et al. (2020) in a SLR. A written limitation in the SLR is that it only considers peer reviewed journals, and can therefore not include industry frameworks, such as MITRE Framework, and urges future work to inclusion of such works.

Even though the SLR is part of the CyberShip project, it considers all kinds of industries, not just shipping and the maritime industry, resulting in a total of 208 journals that have published a cyber resilience framework. The frameworks specifically relevant for the shipping industry Sahay et al. (2019); Tam and Jones (2019). Sahay et al. (2019) purpose a framework for automated mitigation of cyber-attacks on ships communication infrastructure, based on Software-Defined Networking, which offers a high-level policy language and a translation mechanism for automated policy enforcement in the ship's communication network. Tam and Jones (2019) developed a model-based framework for maritime cyber-risk assessment. MaCRA focus on enabling interested parties to assess cyber risks in any maritime system, with the emphasis on criteria of the available vulnerability, criteria of ease-of-exploit, and cyber reward for the adverse actor, and further provides examples of the use of the frameworks with ship systems, but also human factors. In terms of relevance for the thesis, Sahay et al. (2019) examples is identified as too technical to be included. Tam and Jones (2019) serves as an insight how a wide variety of people can apply maritime specific cyber risk assessment and will be relevant on a pre-event aspect in a resilience perspective.

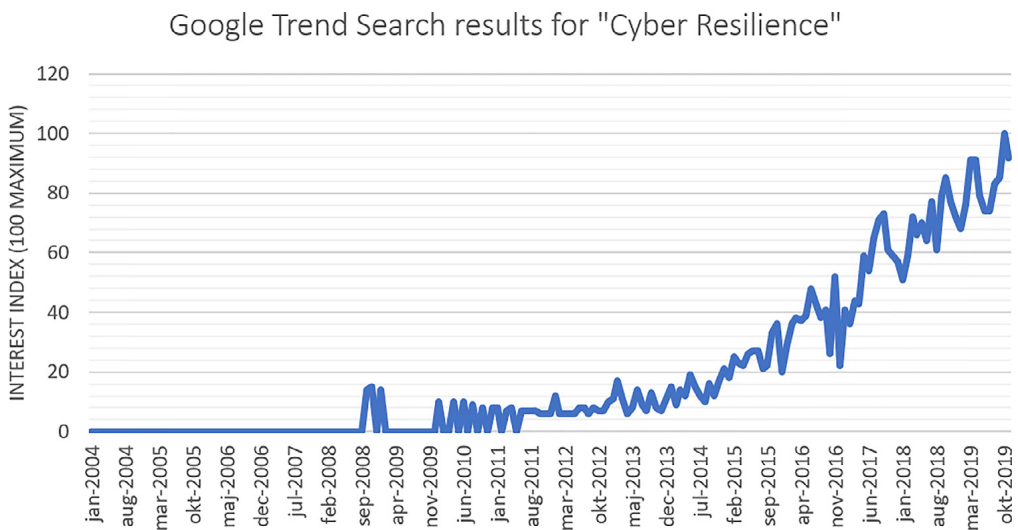


Figure 12 'Google search trends about cyber resilience since 2004' (Sepúlveda Estay et al., 2020, page 2)

As shown in Figure 12, there is an increased interest for cyber resilience over the last decade. The MITRE Cyber Resiliency Engineering Framework (CERF) was published in 2011 (Bodeau et al., 2011), and the framework has been developed and updated in 2015 with the "MITRE Cyber Resiliency Engineering Aid—The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques" (Bodeau et al., 2015). It is not a replacement of the original MITRE Framework, but rather provides additional information which system engineers and architects can use when deciding which cyber resilience techniques to apply.

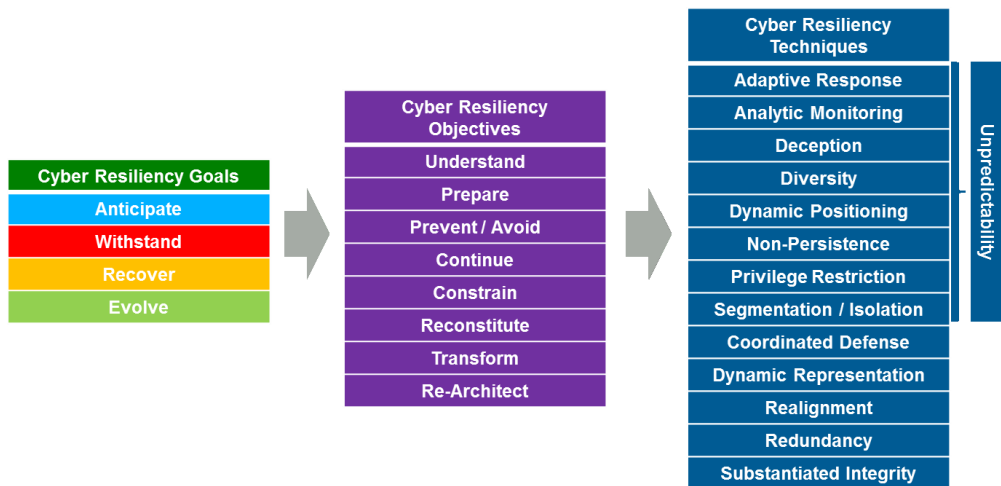


Figure 13 'Cyber Resilience Engineering Framework' (Bodeau et al., 2015, page 10)

Figure 13 presents the Cyber Resiliency Goals, Objectives, and Techniques, which are the elements of the CERF. The MITRE CERF Goals is founded on Madni and Jackson (2011) conceptual framework for resilience engineering which again is derives on the concepts of Hollnagel et al. (2006), amongst others, as explained in Bodeau et al. (2011), which also presents background on related engineering and resilience frameworks in Appendix B of the CERF. Originally, the MITRE Framework defined cyber resilience as 'the ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function' (Bodeau et al., 2011). Further, Bodeau et al. (2011) defined cyber resiliency engineering as 'The sub-discipline of mission assurance engineering which considers (i) the ways in which an evolving set of resilience practices can be applied to improve cyber resiliency, and (ii) the trade-offs associated with different strategies for applying those practices'. The as the framework is updated in 2015, CERF defines cyber resiliency as 'the ability of cyber systems and cyber-dependent missions to anticipate, continue to operate correctly in the face of, recover from, and evolve to better adapt to advanced cyber threats (Bodeau et al., 2015).

Even though the CERF was updated in 2015, that was not the end for the evolvement for cyber resilience engineering. Authors from both NIST and MITRE joined forces and published the NIST Special Publication 800-160 Vol 2 'Developing Cyber Resilient Systems: A systems Security Engineering Approach' (Ross et al., 2021). The NIST 800-160v2 is targeted towards system security engineers and other professionals working with system life cycle processes, and the purpose is to guide how to apply cyber resilience concepts as part of systems security engineering and risk management for systems and organisations (Ross et al., 2021). The publication is more technical and more like a handbook, than presenting the overarching strategy of the MITRE CERF. Moving over to a more context dependent focus, the next section will focus on maritime aspects of cyber resilience.

4.4 Maritime cyber resilience

When starting the PhD project, the maritime industry maturity towards maritime cyber security was rather low, and as pointed out by Bolbot et al. (2022), cyber resilience in research considering the

maritime industry have received less attention than maritime cyber security. Bolbot et al. (2022) mentions just three research paper directly related to maritime cyber resilience, whereas one of them is a paper produced in accordance with this thesis. Bolbot et al. (2022) also pinpoint that more empirical studies on maritime cyber resilience are required. The purpose of this section is to present the results of a SLR on maritime cyber resilience and to shed light of the status of how maritime research consider and treat cyber resilience today. The findings and themes presented based on theory from the previous section, more specifically the cyber resilience goals. To the best of the authors knowledge, there does not exist a structured literature review focusing solely on “maritime cyber resilience”. The SLR follows Okoli and Schabram (2010) method and the search phrase for the SLR was “maritime AND cyber (resili* OR safe*)”, which were applied to the databases Scopus, SpringerLink, Web of Science, EBSCO and Compendex. The date of search and data gathering was the 27th of June 2023. In-depth information about the SLR can be found in Annex II. A criterion in the SLR is that the paper found must include an aspect of either safety and/or resilience, only considering security is not enough. As explained previously, resilience and security are similar terms but not the same. In this thesis, maritime cyber resilience is treated to reflect more upon the operational safety of the vessels than maritime cyber security, hence the research question for the literature review is formulated as follows:

- What is the state-of-the-art status of maritime cyber resilience and safety within maritime cyber security research today?

4.4.1 Results from maritime cyber resilience literature review

This section presents the results from the literature review and the results is put in different categories related to the theory presented in Section 4.3 considering cyber resilience. The three first categories relate to Anticipate and Withstand, while the last relate to Recover and Evolve. The results from the literature review are divided into the following categories:

- Identification of cyber risks in shipboard equipment.
- Risk assessment practises for safety of ship
- Frameworks and guidelines
- Simulators, training, exercises, and education

4.4.1.1 Identification of cyber risks in shipboard equipment

The papers presented in this section do not necessarily provide information about how to operationally handle a cyber risk in shipboard equipment but will be beneficial to raise the cyber risk awareness for navigators and shipboard crew considering what risks which might have a safety impact on a ship. DiRenzo et al. (2015) acknowledged cyber risks in onboard systems on a more general basis and provides examples of several real-life cyber risks, attacks, and demonstrators. In addition to describing vulnerabilities for ships, DiRenzo et al. (2015) also describes rig, cargo and port operations. A cyber-attack at one end of the supply chain can affect other organizations, systems, and even the whole sector. Awan and Al Ghamdi (2019) conducted a review of historical evidence of vulnerabilities in ship bridge systems and discusses the vulnerabilities in digital components of an Integrated Bridge System (IBS) used onboard ships. The authors highlights various vulnerability patterns, their causes, and consequences. Meland et al. (2021) have registered and analysed 46 such maritime cyber incidents in the maritime industry, making a top-ten list of maritime cyber threats, ranging from threats in IT and OT systems, to economic fraud and manipulation of GNSS signals. Meland et al. (2021) notes that 46

incidents is not that high number for an industry compared to other industries, but at the same time the maritime sector could face some of the most severe consequences, compared to other sectors. Androjna and Perkovič (2021) discusses the vulnerabilities of the GNSS, ECDIS, and AIS to cyber threats, and provides recommendations highlighting the necessity for users to be aware of the vulnerabilities of modern navigation systems. Kessler et al. (2018) focus on cyber threats towards AIS, but still emphasize that the loss or alteration of AIS should not necessarily cripple the safe operation of ships, as ships have been sailed without electronic aids for a long time before the age of electronic navigation. Shapiro et al. (2018) discusses maritime threat actors, motives, tactics, and targets, and examines the vulnerabilities of the maritime transportation systems sector that could be exploited by those seeking to conduct a Trojan horse attack. Svilicic, Brčić, et al. (2019); Svilicic, Kristić, et al. (2020); Svilicic, Rudan, et al. (2019) investigates vulnerabilities in an ECDIS by the use of a vulnerability scanner and interviews shipboard crew of the findings. Svilicic, Rudan, et al. (2020) does the same, but for radars, as well as the authors provides information regarding how the cyber security posture is onboard the vessel where the radar has been tested. Both Svilicic, Rudan, et al. (2019) and Svilicic, Rudan, et al. (2020) claims to gain a holistic view of cyber security resilience of shipboard equipment, but fails to give the full picture of what that really means. All of these papers exhibit similar themes and methodological approaches, as the papers written by the same main author. Longo et al. (2022) discusses novel threats related to the radar system, which is one of the most security-sensitive components on a ship. The author presents malware which affects the radar displays and can easily affect the INS, and demonstrate that radar displays can be modified, i.e., remove or alter radar echoes. The authors also propose a detection system aimed at highlighting anomalies in the radar video feed, requiring no modifications to the target ship configuration.

4.4.1.2 Risk assessment methods for safety of ships

The result in this section relates to different risk assessments methods which have a safety or resilience impact on a ship. The author of the thesis acknowledge there are many other risk assessment methods for safety and security of ships, but as the literature review was based on inclusion and exclusion criteria, the following is the ones which will be noted. Kessler et al. (2018) provides a short risk assessment for AIS risks and scores on likelihood, severity and ease of exploit as well as the source of the risk (human, technical or nature). Melnyk et al. (2022) describes maritime cyber security risks, propose a conceptual model of ship security, and concludes that a ship is cyber vulnerable. Kechagias et al. (2022) presents the findings from real case study of a shipowner company, where the author wants to connect research with practice, by presenting the company systemic approach to cyber security. The authors use the Plan Do Check Act approach to review aspects of what the author find to be the three elements of cyber security: the procedures, human factors, and technology. The review is towards drills, policies, incident reporting schemes, amongst other things, all with reference to relevant regulatory frameworks such as ISM code. Alongside describing that shipowner companies need to raise cyber security awareness and get over outdated misconceptions and practices, the paper concludes with that cyber resiliency is the key for safely realizing the benefits of digital shipping and doing operations better (Kechagias et al., 2022). Oruc et al. (2022) discusses the cyber risks associated with INS on modern vessels. The study aims to assess the cyber risks of 25 components on the bridge by implementing FMECA (Failure Mode Effect and Criticality Analysis) and the MITRE ATT&CK framework, which provides adversarial tactics, techniques, and mitigation measures. The paper concludes that the ECDIS, Multi-Function Display (MFD) and radar is the only components of an INS which requires an operating system to run, and thus is more subject to cyber threats (Oruc et al., 2022). Tam and Jones (2019) developed MaCRA

which is a model-based framework for assessing maritime cyber risks, combining cyber and maritime factors. It offers risk characterization, measurements, and supports human decision-making. The authors provide examples of use of the framework and construct the assessment profile on ease-of-exploit, vulnerability in the system and reward for the cyber adverse actor. Karahalios (2020) uses STPA-SafeSec (Systems Theoretic Process Analysis) to identify communication and navigation constraints in three different shipowner companies and 15 different ships and identifies eight risks categories. The authors indicates that there are significant security gaps mainly due to lack of awareness from operators and seafarers. All these risk assessments methods presented in this section is proactive measures, as a risk assessment should be, but does not necessarily include aspects how to handle or mitigate risks which is unknown for the operation yet, which might emerge as the consequence of a cyber-attack.

4.4.1.3 Frameworks and guidelines

Frameworks and guidelines is an important part of how the maritime industry threat cyber issues, and this section emphasise the literature describing or critically review such frameworks or guidelines. Progoulakis et al. (2021) describe the cyber aspects of a maritime vessel, regulatory frameworks, the associated threats and risk factors and risk analysis methods. Further, the author presents an application of a Security Risk Assessment (SRA) method on a FPSO (Floating Production Storage and Offloading) vessel, before presenting an example of use of the Bow-Tie model. After reviewing industry and government directives and standards, solutions for maritime cyber security in the industry is not adequate. The reasoning for this is that the available documents focus on IT side of systems and fail to define mitigation measures and procedures that would guide asset owners and operators (Progoulakis et al., 2021, page 17). The author finalizes the discussion by emphasising that the human element and cyber security skills should be considered paramount, and that significant investments towards training of ship crew across the whole hierarchy of the shipowner company. Drazovich et al. (2021) seeks to enhance the resilience of maritime cyber security guidelines by reviewing eight guidelines and frameworks, such as NIST framework, BIMCO, IMO cyber security guidelines, and others provided by different class societies. The review the depth of the frameworks considering how effectively the frameworks can be used for ship design, risk management, the process to develop procedures, etc. Some of the findings the authors mention is that none of the frameworks is sufficient for proper cyber security posture by itself and that the frameworks lack grounding in literature and research. For improved outline of the frameworks and guidelines, Drazovich et al. (2021) purpose a system-of-systems perspective specific for the maritime context, define designated responsibilities amongst stakeholders and a devoted risk assessment, mitigation, and resiliency strategies. Considering resilience strategies, the author suggest that frameworks and guidelines should include directions that discusses cyber intrusion response and recovery plan as well as recommendations for redundant systems.

4.4.1.4 Training and education

Recover and evolving is an important part of cyber resilience, this section focus on the results connected to training and education, but also simulator and exercises for cyber safety and resilience. Hareide et al. (2018) discusses how cyber systems make situational awareness more complex for the modern navigator and demonstrates a real-life cyber-attack which shows how a cyber-attack can be performed against a modern maritime navigation system. The author suggests a working definition for maritime cyber security and emphasise how the cyber kill chain model can be used to prepare navigators for cyber-attacks. In addition to what is described about frameworks and guideline above, Progoulakis et al. (2021) mention the importance of training of ship crew and shore personnel but does not address how. Kuhn et

al. (2021) discusses the impact of COVID-19 on the maritime industry and the increased cyber risks that come with digitization. The paper reviews current events and introduces an exercise where participants at a NATO Centre of Excellency were shown scenarios involving maritime cyber incidents and evaluated on cyber risk perception. Further, the authors highlight the need to plan for cyberspace operations and ground cyber risks as a governing factor in maritime. The article also discusses the implications of COVID-19 on maritime cybersecurity, including the increase in cybercrime and cyber-attack rates in the maritime sector. The article concludes that COVID-19 has driven a major increase in cyber risk, and the maritime industry needs to prepare for secure use of cyberspace (Kuhn et al., 2021). Hopcraft (2021) investigates to develop maritime digital competencies by utilizing the NIST Framework. The author further describe how IMO works with safety and security and emphasise the Resolution which urges seafarers to consider cyber risk. It is challenging to address the maritime sector due to the diversity of the industry, but the author outlines how the NIST framework can contribute to outlining key competencies that seafarers and maritime personnel should have. Wolsing et al. (2022) describes a simulation environment for network attacks against marine radar systems and categorize seven classes of attacks against marine radar systems. The classes are denial of service, scaling, rotation, translation, object addition, object removal and object relocation. Potamos et al. (2023) focus on building a curriculum for all people across an organization to develop skills to handle a ransomware incident and purpose an example of a ransomware against an ECDIS onboard a ship, by using a cyber range simulator. The paper identifies learning objectives, such as understanding, cyber hygiene for minimizing risk and apply a ransomware incident response plan. Potamos et al. (2023) further emphasis active learning through kinesthetics learning, meaning the learners should focus on discuss, practice and teach others, to learn about the subject.

4.4.1.5 Summary

Based on the results of the SLR, none of the paper reviewed provide a definition or description of what maritime cyber resilience is. This is an important finding which means that this thesis must be consistent when handling the aspect of maritime cyber resilience. It must be based on previous theory and literature, as described in Section 4.1. How maritime cyber resilience is defined and treated in this thesis is further described in Section 5.1 'Paper I – An operational approach to maritime cyber resilience'. Even though none of the papers shed light on what maritime cyber resilience is, the knowledge about them will be important when discussing maritime cyber resilience.

4.5 Maritime training and education

The maritime industry have evolved significantly over the years, from educating celestial navigation to the modern age of navigation, where advanced electronic systems are being used (Bowditch, 2002). As the industry have evolved by the incidents mentioned in the previous section, the industry has also developed with new technology. This evolution also yields a development of the MET to equip maritime professionals with the right skills and knowledge, and today maritime professional is required by law to have extensive training in onboard systems, according to the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) (International Maritime Organization, 2016). STCW is implemented by IMO, meaning it applies to all seafarers all around the world, sailing a ship over a certain size and/or with certain characteristics. Previously, maritime training was based on experience and passed on from senior crew to junior crew (Erstad, Hopcraft, Vineetha Harish, et al., 2023). While STCW are have contributed to a level of uniformity and standard for training of seafarers,

STCW is not keeping up with rapid challenging technologies and fails to adapt aspects such as cyber security (Heering et al., 2021; Hopcraft, 2021). Maritime navigators use improvised coping strategies for maritime cyber challenges today, but does not fully understand the extent of the risk (Erstad, Lund, et al., 2022).

STCW does not explicitly mention cyber risk education, but still does not mention that maritime universities should not consider it (International Maritime Organization, 2016). As the ISM now require ship SMS system to consider cyber risk (International Maritime Organization, 2017b), STCW should also consider necessary aspects of cyber risk. How to perform such teaching is not mentioned, which means that maritime universities / MET institutions (METI) are free to implement it in whatever extent the METI finds reasonable. MET and METI have become increasingly reliant on computer systems and considering navigational training, METI today utilise highly technological maritime simulators, which are full scale, full mission replica of a generic ship bridge (Hontvedt & Arnseth, 2013). Sellberg (2017) notes that simulators have been used in MET since they first appeared in 1950s. Maritime simulators are primarily used for training on ship handling and collision avoidance per Convention on the International Regulations for Preventing Collisions at Sea (COLREG) (Cockcroft & Lameijer, 2011; Sellberg et al., 2018). Today, modern maritime simulators are used for both training navigational skills, instrument specific skills, human resource and communication skills (e.g., Bridge Resource Management (BRM)), ship handling skills (Sellberg, 2017), and now even Virtual Reality (VR) and cloud based (CB) internet simulators have made it entrance into MET (Kim et al., 2021; Mallam et al., 2019). What is often associated with maritime simulators is fidelity, which describes the degree of realism in a simulator (Hontvedt & Arnseth, 2013; Kim et al., 2021; Wahl, 2020). Kim et al. (2021) discusses four types of simulators used in maritime education and training, which are desktop-based, full-mission, VR, and CB simulators, and further discusses their advantages and limitations of each. Kim et al. (2021) also discuss remote learning in a post-COVID-19 era and recommends future research explorations to further develop and improve the use of simulators in MET. The list below provides a summary of the strengths and weaknesses of each type of simulator Kim et al. (2021):

- Desktop-based simulators:
 - Strengths: Low cost, easy to use, and accessible.
 - Weaknesses: Limited functionality, low fidelity, and lack of realism.
- Full-mission simulators:
 - Strengths: High fidelity, realistic, and provide a complete replication of the ship's bridge.
 - Weaknesses: Expensive, require dedicated space, and limited scalability.
- Virtual reality simulators:
 - Strengths: High immersion, interactive, and provide a realistic experience.
 - Weaknesses: Expensive, require specialized hardware, and limited scalability.
- Cloud-based simulators:
 - Strengths: High scalability, accessible from anywhere, and cost-effective.
 - Weaknesses: Limited fidelity, require a stable internet connection, and lack of physical interaction.

Hontvedt and Arnseth (2013) notes that simulator is considered a central strategy for improving maritime safety. In traditional maritime studies, the focus has primarily been on navigational safety,

encompassing elements like vessel construction, weather predictions, and human skill (Bowditch, 2002; International Maritime Organization, 2016). Wahl et al. (2020) have thoroughly investigated resilience training in maritime simulators, by study at Safety-I and Safety-II aspects considering practical resilience skills for operators of Dynamical Positioning (DP) vessels (i.e., highly technological and complex vessels designed for precision positioning and navigation). Considering learning, Wahl et al. (2020) describe that the goal of simulator training is learning, and highlights different aspects of experience based learning to trigger reflection and experience sharing amongst learners to gain increased knowledge. Wahl et al. (2020, page 3) describe the relation between training focus and training process for Safety-I and Safety-II in the table below.

	Training focus	Training process
Safety-I	Prevent things from going wrong in the future by looking at accidents and adverse events in the past.	Rigorous training focusing on standardised processes and compliance with procedures to handle known system failures.
Safety-II	Increase things that go right in the future by looking at experienced successes in normal and non-normal operations.	Flexible training based on joint reflection and operator experience to increase the ability to handle unknown system failures.

Table 3 'Balancing Safety-I and Safety-II in DPO training' (Wahl et al., 2020, page 3)

As noted by Wahl (2020), there is a need to bridge the gap between technology design and learning theories considering simulator training. It is therefore important to investigate theories which can benefit both traditional MET as well as incorporating new challenges, such as maritime cyber security issues. As stated previously, there is still a lack of reporting of incidents in the maritime industry considering cyber incidents. Therefore, it is important to look into other learning theories, which also can benefit the previous experience based learning principle, but also include new and unknown aspects. People learn differently (Oommen, 2020). There are many different schools of learning theories, but several of them emerged after the technological revolution, from behaviourism in the early 20th century to constructivism, cognitivism and humanism in the 1950-1970's (Illeris, 2018). Constructivism emphasizes that learning is best in the real world, where the learner is constructing their own understanding of new information based on their prior knowledge and experiences (UoB, 2022; Watson, 2001). However, as new technology finds its way into MET, it is also important to adapt the learning to fit new aspects and tools of learning, and connectivism is such a learning theory (Siemens, 2004). According to this theory, learning is not an individual effort but a networked process, facilitated by the connection of information nodes like databases, human experts, or other informational resources (Siemens, 2004). Connectivism argues that in a fast-changing world, the ability to continually acquire new knowledge through various networks is more crucial than the knowledge itself. Connecting cyber risk to maritime simulator scenarios to construct knowledge about how to increase resilience for maritime operations will be important for the safety of ships. Even though not explicitly mentioned in STCW, cyber should still be addressed by METI's, as there is emphasis on learning aspects from the ISM code (International Maritime Organization, 2016).

5 Research results and contributions

The research results are presented in four academic papers and one workshop report. In addition, this thesis contains information about the results and the simulator exercises. This section presents the research results and the contributions from the papers associated with the thesis. Critical reflection of the papers is described in Section 5.6.5.

	RQ 1	RQ 2	RQ 3
Paper I	●		
Paper II		● ●	
Paper III			● ●
Paper IV		● ●	
Workshop		● ●	● ●

● Research questions
 ● Academic impact
 ● Industrial impact

Figure 14 - Research results and how they relate to research questions.

5.1 Paper I – An operational approach to maritime cyber resilience

Paper I was set out to define the boundaries for the thesis and provided the foundation necessary to plan the project and define a way forward. The main scope for Paper I was to find a working definition of maritime cyber resilience. In early phases of the project, from about April 2020 and until the finalizing of Paper I in March 2021, “maritime cyber resilience” was used as a buzzword by the maritime industry, without a clear definition of the term. As stated in Paper I, over 300 different definitions of the term “resilience” exist, and zero definitions of “maritime cyber resilience” was to be found. Thus, the paper provides results of a literature review of “maritime cyber resilience”, with few results. The paper continues to break the term into what is found to be important, based on the literature review; “maritime operations”, “maritime cyber security” and “cyber resilience”.

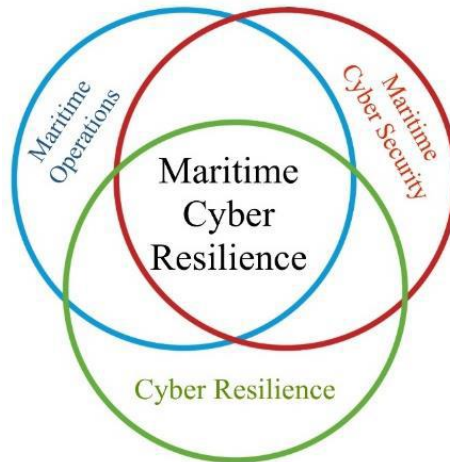


Figure 15 "Origins of Maritime Cyber Resilience" (Erstad et al., 2021)

The synthesis of these terms led to the formulation of a working definition of “maritime cyber resilience”, defined as “a nautical system’s ability to learn how to maintain and evolve a normal operation, as well as anticipate, withstand, recover and evolve from a cyber threat, in the minimum amount of time possible.” (Erstad et al., 2021, page 31). This definition transcends a purely technical scope to incorporate human factors, recognizing the critical role of navigators in maritime cyber resilience.

Paper I main intent to answer RQ1 and the sub-question associated with it. In addition to providing a working definition for the thesis, it describes how a cyber situation onboard differs from fire onboard and elaborates why the navigator is a crucial risk handling capability onboard, in addition to why it is important to focus on learning and evolving. A fire is a more known and more tangible kind of crisis, which navigators and essential crew have certified practical training to handle, which is not the case for a cyber-attack. Further, Paper I investigates important resilience factors such a situation, where the emphasis is on the factors; anticipate, withstand, recover, and evolve.

5.2 Paper II – Navigating through cyber threats, a maritime navigator’s experience

Following the HCD process, the subsequent phase following Paper I is concentrated on identifying and specifying the user requirements. The identification of needs is important and the focus should be towards which user needs to achieve and identify if there is any constraints (ISO, 2019a). The planning of Paper II an outcome of Paper I, presenting the result of interviews with ten Norwegian maritime navigators employed across various maritime sub-sectors.

Table 1. Categories and sub-categories.

Category	Sub-category
The digital era	Trust in technology
What is actually a cyber threat?	The un-hackable and indispensable RADAR
	The intangible term of “Cyber threat”
	Intentional vs unintentional
Improvised coping strategies towards cyber threats	Satellite navigation related issues
	Ad hoc improvising
The unaddressed cyber issue	Unwritten rules
	Lack of awareness and training
	Lack of policies, procedures, and regulatory standards
	“Old school” vs “new school”
The complex nature of consequences	Causes and consequences
	Capacity of functions
	“It depends”

Figure 16 - Categories and sub-categories (Erstad, Lund, et al., 2022)

Employing the Structured Thematic Content (STC) procedure (Malterud, 2012), the paper segmented findings into categories and sub-categories, as shown in Figure 16. This thematic classification aimed to offer readers an understanding of the topics discussed in the interviews and the corresponding collective perspectives. The sub-categories are nuances of the categories, highlighting how the interviewees talked about the various aspects of the categories. The overarching theme across the interviews was that cyber threats were something new and generally unknown for navigators, which both is intangible and complex in nature and consequence. In contrast to some of the interviewees, a cyber threat was even classified as just another technical error, which can mean that navigators do not consider that there is a deliberate human threat actor behind a cyber risk, in contrary to a technical error.

Paper II concludes with a critique of the maritime industry's insufficient engagement with the issue of cyber threats, despite the escalating international focus on maritime cyber security and resilience. This emphasis the urgent need for training and educational initiatives addressing cyber risks. Problem solving for navigators at the sharp end of the operation are normally pragmatically handled and understanding how navigators interprets cyber threats will be beneficial for the development of HCD focused training.

Paper II serves as an insight paper of how a selection of maritime navigators interpret maritime cyber threats and contribute on several stages of the thesis research process. First, it gives clear input to the HCD process and investigates how to best continue the research process to produce a solution which fits the user. This paper proves that the STC is a suitable method for interviewing process in a HCD project, especially considering that the method is as descriptive as it is and gives a clear roadmap over the analysing process, which often can be confusing for novice researchers. Further, the paper offers maritime industry researchers, training facilitators and stakeholders' valuable information for how navigators understand treat cyber threats today. It offers empirical data that can be leveraged to customize formal education plans, but also life-long-learning courses (e.g., industry courses) as well as a foundation for cultural development in a shipowner company, or even as basis of knowledge for companies providing cyber risk insurance.

5.3 Paper III – A human-centred design approach for the development and conducting of maritime cyber resilience training

“Design decisions have a major impact on the user experience” (ISO, 2019a, p.15), a notion equally applicable to “Ironies of Automation” (Bainbridge, 1983). From the previous papers in the project, it was clear that there is a need for training and education towards maritime cyber resilience. When designing educational or training programs, the aspect of learning theories is important to consider, as they are the basis for the design of the education. Being educated as a seafarer myself, I also have experienced the ‘learning-by-doing’-tradition, as well as experienced how the industry is heavily dependent on professional on-the-job-learning and learning from more experienced crew onboard.

This paper focuses on development and conducting of one specific maritime cyber resilience simulator scenario, where the system under consideration in the scenario is the ballast water management system (BWS) and the potential vulnerabilities of such systems. In short, the BWS makes sure that the ship is on even keel, for example despite of uneven loaded cargo. One can compensate with ballast on starboard side of a ship if there is loaded heavy cargo or equipment on the port side of a ship.

The HCD activities and descriptions in this paper offers an easy-to-use roadmap, yet detailed enough to highlight the aspects which are important to consider when developing such simulator scenarios. Unlike traditional maritime simulators that primarily train for rule-based scenarios like collision avoidance as per COLREG (Cockcroft & Lameijer, 2011; Sellberg et al., 2018), this innovative simulator scenario acknowledges that cyber risk demands a different skill set that deviate from the conventional handling of technical errors. There is no fixed solution to this problem, as the cyber-attack (or incident) does not follow a pre-described procedure or method, which means that handling cyber-attacks require handling which might not be the same as normal technical error handling. The paper’s uniqueness lies in its interdisciplinary approach, seamlessly integrating Human-Centered Design (HCD) methods, educational learning theories, and simulator training. The presented HCD roadmap serves as a comprehensive yet accessible guide, accentuating the nuances crucial for the effective development of maritime cyber resilience simulator scenarios.

5.4 Paper IV – CERP: A maritime cyber risk decision making tool

The maritime industry's emphasis on procedures and policies for the safe operation of ships is clear, as noted in Paper I and Paper II. As a response, Paper IV introduces the Cyber Emergency Response Procedure (CERP) to address the industry's gap in practical, operational-level tools for crew members dealing with cyber incidents.

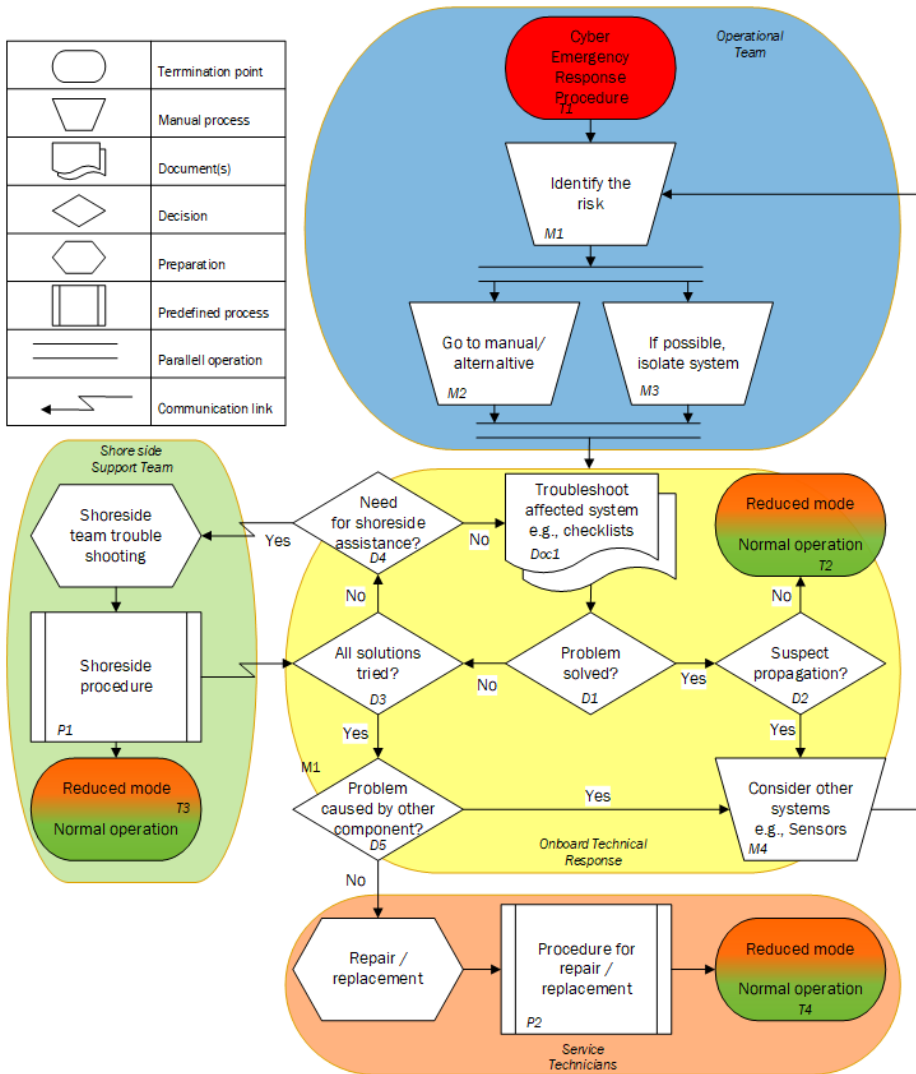


Figure 17 - Flowchart for the Cyber Emergency Response Procedure (CERP) (Erstad, Hopcraft, Misas, et al., 2023)

To ensure usability of the tool and to uphold the HCD principles, actors from the industry was invited to participate in discussion and development of the procedure. The flowchart is based on known flowchart standards (ISO, 1985), and relies on practical examples for explanation of the CERP. Further, the paper investigates and explains the different potential roles and responsibilities in a cyber risk situation, where it is an emphasis on shore – ship collaboration. The shore personnel do not have onboard situation awareness or experience, and the ship personnel does not have sufficient cyber risk awareness in IT/OT systems. The paper also points towards implementation of the CERP into maritime operations, where development of specific checklists, development of cyber response teams, and training are emphasised as important points. As there is a plethora of maritime operations and different ships around

the world, each organization needs to develop their own specific systems considering cyber, as the business models and risk profiles is very varied across the maritime industry.

The CERP serves three purposes; Firstly, it provides a blueprint that allows organisations to include cyber incident response within their standard incident response procedures. Secondly, it provides a high-level decision-making tool that guides crew through the response to a cyber incident. Thirdly, the CERP sets out to demonstrate the need for, and procedure for attaining, external support in the face of a cyber incident the crew cannot handle independently (Erstad, Hopcraft, Misas, et al., 2023). One of the CERP's defining features is its simplicity, designed for immediate reference with minimal training. As a flexible template, it can be adapted to suit the diverse needs of commercial ships and organizations, given the industry's varied risk profiles and business models.

5.5 Workshop, focus groups and simulator experiment

All the papers described in the sections above have been on a theoretical level, however, the quality of user requirements specification must be practically ensured and evaluated. ISO (2019a) emphasize that such can be achieved through testing, verification by stakeholders, internally consistent and updated as necessary during the life of the project (ISO, 2019a). Therefore, two workshops with focus groups and simulator experiments have been conducted, where project partners, ship crew and stakeholders from the maritime industry was participating. The first workshop was part of the second phase of the HCD process and focused on specifying user requirements. It served as a contributor to the interviews performed in Paper II providing further foundation for the project and Paper III. The first workshop is published as a workshop report (Erstad, Larsen, et al., 2022). The second workshop acted as a testing and evaluating arena for the HCD process, where aspects which is discussed in the papers were brought into practice, where the workshop also were a practical seance after conducting maritime cyber simulator scenarios as a part of M.Sc. level course, developed by the author and a co-research fellow. As described in Paper II Erstad, Lund, et al. (2022), improvised coping strategies is used against cyber threats in the maritime industry, as well as cyber itself is an unaddressed issue. The findings of the second paper verifies that there is no standardized form for training or education in the maritime industry for how to tackle cyber-attacks. This also result in that navigators interpret cyber risks in separate ways, which result in less operational resilience, as the understanding of the situation might not be correct.

The scope of the first workshop was to get stakeholders to take part in discussions to map out potential cyber-attack simulator scenarios which can be implemented in maritime training. Simulators are already extensively used in traditional maritime training, a training platform well familiar to the navigators and the known risks such as jamming and spoofing is already being taught in maritime simulators (Erstad, Lund, et al., 2022). 22 persons attended the workshop from over 12 different maritime companies, ranging from offshore shipping companies and academic institutions to naval and government authorities. In addition, three persons hosted the workshop. The workshop report lists up potential cyber simulator scenarios which could be used in maritime cyber education and training. The participants were eager to share what they found important to consider when designing scenarios. The identified scenarios range from unintended cyber incidents as a consequence of a mistake, to advanced cyber-attack which can be exploited by adverse actors and harm the ship and crew. The workshop concludes that simulator training, if customized and tailored to mariners, can help enhance maritime cyber resilience.

In addition to the workshop and the papers, the author of this thesis has contributed to developing a course on M.Sc. level for operational maritime cyber risk management together with a fellow student. The second workshop was part of this course, where there were held theoretical lessons considering maritime cyber risk management and conducted practical maritime cyber resilience scenarios. The aim of the simulator scenarios was to test the scenario presented in Paper III in practice, and the scope of the workshop was to evaluate the use of cyber scenarios in a maritime simulator environment.

Both workshops in the project serves as milestones and contributors to validation. It was important to get feedback from the industry that the project was on the right track and to identify potential next steps.

5.6 Reflection of papers

Evaluation is an important criterion in the HCD method and is even supposed to be applied in the earliest stage of the process, to ensure and obtain a better understanding of user needs, even though the “Evaluating the design” itself is a later phase of the HCD process (ISO, 2019a). Even though the step in the procedure emphasise user testing and inspection based testing by for instance stakeholders (ISO, 2019a), it is found that self-reflection could be useful, as the thesis have been developed over a long period of time.

5.6.1 Reflections - Paper I

Entering a new research domain while simultaneously adapting to academic methodologies was a dual challenge. The paper acted as an initial step into maritime cyber security and resilience, benefiting from a prior understanding of maritime operations. Despite the lack of results from the initial literature review, there's an acknowledgment that the approach could have been more methodical. As a corrective measure, Section 4.3 is dedicated to review of maritime cyber resilience literature.

A key issue in this research area has been the ambiguous use of the term "maritime cyber resilience" in industry and research contexts. Many industry webinars and advertisements have been marketing “maritime cyber resilient solutions” as broad-spectrum solutions for maritime challenges. The concern arises when these solutions don't clarify their resilience mechanisms, especially regarding safety during unexpected events, where the navigator needs to take the wheel. This gap emphasized the need for the first paper in the thesis and highlighted the importance of establishing a concrete definition to guide the study.

5.6.2 Reflections – Paper II

Interviews are a craft (Creswell et al., 2018, page 164) and this was the first time the author of the thesis conducted a scientific interview. Given the space constraint in the paper, the paper primarily focused on the findings and results of the interview analysis, rather than the research method and process, as the STC procedure is described in detail by Malterud (2012). Although the STC framework is straightforward, data transcription and analysis were conducted manually, utilizing rudimentary tools like Microsoft Word and Excel. The timeline of the interviews spanned from September 2020 to May 2021, adding another layer of contextual complexity. Moreover, the paper could have been further strengthened by concentrating on how navigators perceive 'cyber risk' rather than 'cyber threat,' a distinction that resonates significantly in research literature (Refsdal et al., 2015). The rationale for the focus on cyber threats over cyber risks is underpinned by the resilience-based assumption that absolute

safety is unattainable, making the likelihood component of the risk equation less relevant. And considering how navigators understand cyber risk (i.e., cyber risk perception), a parallel research project is conducted on the matter (Larsen & Lund, 2021; Larsen et al., 2022)

5.6.3 Reflections – Paper III

The HCD method recommends that the designer or researcher should focus on what of the user needs which is important, rather than how to achieve the need. As a researcher, I am coloured by my background, as I have experienced maritime education, sea going service and many hours in simulator. As the simulator can be considered as a tool to achieve the goal of enhanced maritime cyber resilience, one of the MarCy project goals was to produce simulator demonstrators. This meaning that the process has not been fully unbiased, however, due to the transparency, methodology and methods used in the research project, this is not considered as an obstacle.

HCD methods, although robust, are both time-intensive and costly, presenting practical challenges for simulator instructors who must also adhere to existing regulations like STCW (International Maritime Organization, 2016). Given that cyber security is not yet formally included in the STCW requirements (September 2023), justifying the resource allocation for this level of detailed HCD can be challenging. However, Paper III serves as a blueprint for a maritime cyber resilience simulator scenario and as a precursor for a future how cyber resilience training can be integrated into STCW curricula, thereby as a relevant contribution to the field.

5.6.4 Reflections – Paper IV

Paper IV presents a novel tool for handling maritime cyber risks, and to the best of the authors knowledge, the paper is the first of its kind considering operational maritime cyber incident handling. Validation have been an important aspect in the process of development, however, to ensure the usability a larger selection of users and stakeholders should be involved. For a more comprehensive evaluation of the usability, key personnel likely to be involved in cyber incidents should be invited for practical testing of the tool, for instance using simulator scenarios. This could involve multiple iterations of the scenarios, both with and without the CERP, as well as control groups unfamiliar with cyber risk and the CERP. This would not only verify the CERP's effectiveness but also adjust it for broader application.

5.6.5 Reflections - Workshops

The workshops were conducted with multiple purposes. First, it was to gather industry actors to contribute to the project. Additionally, it was to get feedback to evaluate if the project was on the right path, or if adjustments needed to be made. User based testing and inspection-based evaluation is covered by the workshops and the maritime digital security course, which are important aspects in the HCD process. The scenarios which was demonstrated in the first workshop were developed on the basis of what is already being taught in nautical education (Erstad, Lund, et al., 2022), such as GNSS jamming and spoofing, and therefore the participants should have some basic knowledge about it in advance, as they both have interest and knowledge of nautical education and cyber risks, even if not half of the participants was educated as navigators.

Reflecting on the process of the workshops, the author of the thesis did not participate personally in all the workshop groups. However, only the author transcribed and condensed the audio recordings, to get

an overview over the results from each discussion. The workshop report connected with this thesis is in addition not a scientific, peer reviewed paper. Also, in contrary to the first workshop, it does not exist a report for the second workshop. This was evaluated as not necessary, as the workshop was also concluding the maritime cyber resilience course, which was developed with a co-research fellow.

6 Discussion

The integration of digital systems into maritime operations has undoubtedly brought about significant advantages, such as increased efficiency and improved communication. However, this integration also presents new challenges, primarily concerning cyber risks. The maritime industry, ships, and MET now faces the dual challenge of ensuring traditional safety while adapting to the new demands of digital security. In recent years, the intersection between maritime operations and cyber security and resilience has increased in research and industry concerns. Findings from Paper I to Paper IV indicate that this intersection is far from complete. To ensure that the maritime industry remains robust and adaptable in the face of emerging cyber threats, it is imperative to evaluate the role of maritime training and education, both for new personnel introduced to the maritime industry, but also seasoned professionals. Maritime cyber resilience and security must be tailored to the human operator, as they are still in charge of any emergency onboard a ship, cyber-attacks included. Central to this discussion is the role of MET in addressing these emerging cyber challenges. This section aims to further explore maritime cyber resilience, its impact on maritime education and training, and the critical task of bridging the gap between maritime safety and cyber security. The research question for the thesis was formulated as follows:

- **Research question 1:** How can maritime cyber resilience be defined, and what is the state-of-the-art research within the concept of maritime cyber resilience?
- **Research question 2:** What is required to enhance maritime cyber resilience in maritime operations?
- **Research question 3:** What strategies can be used to make operations on maritime vessels more resilient to cyber risks, and how can the strategies be tested and evaluated?

In this section the integration of safety and resilience into maritime cyber security with the evolving of maritime cyber resilience education and training modules will be discussed. The discussion will further conclude with the relevance and usability of the HCD process for the thesis.

6.1 Integrating of resilience into maritime cyber security and maritime training and education

Maritime cyber security have seen a growing focus in the recent years, largely due to a high number of cyber-attacks that have brought attention to the vulnerabilities in the maritime industry, like the Not Petya attack on Maersk (Ashford, 2019) and the incidents reported by Meland et al. (2021). The current paradigm emphasizes on technical protection measures such as the detection and prevention of malicious attacks, espionage and other cyber threats (Kessler & Shepard, 2020). These aspects are particularly important as they bring light towards maritime cyber resilience, where evolving and learning is paramount. Professionals within traditional cyber security tends not to have the operational focus which is required in the maritime domain, and the maritime industry lag behind compared to other sectors, like critical infrastructure, considering cyber security (Stoker et al., 2022). The focus should not only be on protecting the systems and putting up barriers for keeping malicious actors out, but also consider defensive and reactive measures, where people are aligned with the technology. This also highlight the aspect of secondary effects, meaning that if a ship first is harmed by a sophisticated cyber incident, the ship crew must assume that a mitigation measure might lead to other consequences other

parts in the supply chain which the ship is part of. The maritime cyber risk management which exists today still mostly focus on mitigating risks with technical measures (Linkov & Kott, 2019). If the risk is mitigated to ALARP (or a state where the risk is believed to be ALARP), then it would be reasonable to think that risk managers will proceed to the next risk, as the risk is accepted. However, considering the concept of resilience, a risk manager have to acknowledge that the systems are never free for risk (Hollnagel, 2014b). Still, this should not be an argument to see resilience and security as opposites, rather the contrary, as the maritime industry would benefit from an integrated approach (Linkov & Kott, 2019).

A security-only focus tends to focus on external threat, often deploying highly sophisticated technologies and strategies to counteract malicious actors. However, such an approach can sometimes neglect a systems safety, in this case the ships safety. If only technical and information security measures are considered, shipowners and crew can end up in a state of false safety, which aligns with Linkov and Kott (2019)'s arguments. As Paper I points out, a cyber-attack onboard a ship can be quite different from a normal type of risk or incident. Even what could be considered a minor error for a seafarer without cyber training, such as a wrong USB-stick into the wrong computer, can lead to significant loss of life, property, and environmental harm. A scenario to describe such a situation can be an offshore vessel close to an oil rig, where situations like a black-out (loss of power for entire ship) occur due to the wrong USB-flash drive connected to the wrong computer at the wrong time. This would of course also relate to high-speed ferries in congested waters, cyber incidents at the wrong time can have major consequences for the navigation and hence the safety of the ship and the passengers. MV *Sleipner* grounding in 1999, where 16 people was killed (one amongst them never found), is an example of what the potential consequences may be in the case of insufficient navigation (Justis- og beredskapsdepartementet, 2000), or if a cyber-attack against a steering system (Tam et al., 2021) or a navigation system (Lund, Hareide, et al., 2018), or even both, is initiated on a high speed craft (HSC) in congested waters. The report concludes that even though the navigators held the necessary required competence at the time of the accident, the navigators did not sufficiently used navigational aids and did not complied with established sailing routines (Justis- og beredskapsdepartementet, 2000, page 10). A main recommendation in the report is to work proactively to avoid accidents, and a central element will be sufficient training in navigational instruments and simulator training, and well-established routines, especially amongst the navigators (Justis- og beredskapsdepartementet, 2000, page 13). Today, navigators of HSC navigating in Norway are bound by the High Speed Craft Code (International Maritime Organization, 2021) and national law (Nærings- og fiskeridepartementet, 2012) considering competence and understanding of high speed crafts. A main focus of the HSC course is BRM where training on cooperation, communication, procedures and routines are highly emphasized, and (Scanlan et al., 2022) suggest that revisiting the BRM concepts when equipping seafarers with education considering knowledge and management of cyber risks. Hence, understanding of the systems is hence paramount (Hareide et al., 2018), and maritime cyber resilience is place emphasis on ability to learn how to maintain and evolve a normal operation (Erstad et al., 2021).

Considering resilience skills, Wahl et al. (2020) proves that resilience skills can be taught by simulator emphasis three resilience skills (page 9):

1. The ability to recognise anomalies and solve problems in a flexible manner.
2. The ability to define limits of action through shared knowledge with peers.

3. The ability to operate the system with confidence.

These correlate well with the resilience goals of anticipate, withstand, recover and evolve (Bodeau et al., 2011). Wahl et al. (2020) further emphasise that the simulator training alone is not automatically generating these skills, but that the training philosophy of balancing Safety-I and Safety-II is contributing to the success. In the same way, simulator instructors meaning to teach maritime cyber resilience education and training must be conscious of how learning theories affect cyber resilience training. Even though Wahl et al. (2020) study was not related to cyber aspects, the findings is relevant to a maritime cyber context. Wahl et al. (2020) considers the simulator and the ship itself as a system, but when considering cyber resilience aspects, it is important to understand systems and process beyond own working environment, such as the shipowner office, other vessels, ports, customers, even national authorities. Maritime cyber resilience training should offer a more holistic approach in training for digital maritime operations, considering that a cyber incident might not just be a technical error and that there is always someone who have designed and delivered the attack. Considering training, the everyday work for navigators could benefit from handling situations and work more manually, than only be a monitoring agent. Still, doing full scale cyber exercises onboard a real ship is costly, unreasonable and can potentially be dangerous for the ship, crew, and environment, hence, simulator training where learners can participate in worst case scenarios with more parties than just own onboard crew would be beneficial. As clearly noted by Lützhöft and Dekker (2002, page 94), increased automation does not reduce the human weaknesses, in contrary it may amplify the weaknesses and create new ones, as also described by Bainbridge (1983). What differs Lützhöft and Dekker (2002) example from a cyber-attack is that they considers a “normal” emergency situation (i.e., a grounding) due to over reliance on automation, hence not intended by an adverse actors, which would be the case with a cyber-attack. A core difference between a human and a computer or cyber system, is the skill and ability to improvise when things go bad, such as in a cyber emergency. This leaves the question; how can an operator monitor that a system is working correctly, if they do not have 100% control over the systems? There is a need for high degree of situational awareness is essential to be able to make good informed navigation decisions (Hareide et al., 2018, page 11). Bainbridge (1983) raise the question of who will notice a change, if the alarm function of a complex system is not working properly? In a cyber-attack situation an alarm may be engineered to be not functioning by an adverse actor, such as the alarm suppression technique (Oruc et al., 2022), which will alter the navigators system awareness.

Bainbridge (1983) highlight that in a normal situation, the human tends to let the computer carry the most of the assignment responsibility, but when a problem occurs, the human often wants to take over the wheel and over-ride the computer decisions, which aligns with Lützhöft and Dekker (2002) which says that mariners are more assisted by technology in calm situations than high-stress ones. This causes a problem for the today’s navigators monitoring an INS. Considering a possible cyber crisis where the navigator is fighting against an adverse actor rather than a technical error, the navigator needs to gain full system of awareness, where the navigator must accept that the adverse actor potentially has manipulated the system, forcing it to show wrong or altered information. Such attacks have clearly demonstrated by Lund, Hareide, et al. (2018) where the ECIDS and ship positions can be spoofed and slowly drift towards incorrect presentation of position. On a bright and shiny day, with little to no traffic, one can imagine this could easily be detected by the navigator. However, on a foggy day, with snow and dense traffic, as well as a tired or exhausted navigator, things could be worse. Seafarers are exposed to procedures, policies, and flowcharts every day onboard and such documentation is core elements of

the ship SMS and safe operations. On the other hand, it can also be cause information overload, as there can be too much documentation and procedures to follow to fulfil daily jobs. That is also a reason why seafarers are brought up to be sceptic to new paperwork, and seafarers are used to handle problems pragmatically (Erstad, Lund, et al., 2022). The CERP demonstrates a practical approach to integrating cybersecurity into day-to-day maritime operations. Training modules that use such operational tools can enhance the crew's ability to handle cyber incidents effectively, reinforcing the bridge between safety and security. To ensure usability integrity of the flowchart, validation and verification is a vital part of the paper. The paper describes several situations where the CERP can be used, as well as it is developed in close collaboration with a shipowner company and a national authority organ (which also is a shipowner company per say).

Papers II and III highlighted the gap between navigators' experience of cyber threats and the reality of these challenges. Traditional maritime training has always prioritized safety, as it should be. However, as cyber threats evolve, there's a growing need to incorporate cyber resilience within the maritime training curriculum, ensuring that personnel can handle both conventional and digital threats. Unlike traditional maritime challenges, which remain relatively constant in nature, cyber threats are dynamic. It implies that maritime training and education must be equally dynamic, emphasizing continuous learning and adaptation. This iterative approach to training, combining foundational principles with regular updates on emerging threats, ensures that maritime personnel remain well-equipped to handle evolving challenges.

<u>MITRE Cyber resiliency goals and objectives</u>	<u>Categories and sub-categories of navigators' experience</u>
<p>Anticipate: Predict, Prevent, Prepare</p>	<p>The digital era: Trust in technology</p> <p>What is actually a cyber threat?: The intangible term of “Cyber threat, Intentional vs unintentional.</p> <p>The complex nature of consequences: Causes and consequences, Capacity of functions, “It depends”</p>
<p>Withstand: “Fight through” an attack, defeat adversary actions</p>	<p>Improvised coping strategies towards cyber threats: Ad hoc improvising, Unwritten rules</p>
<p>Recover: Determine damages, restore capabilities, determine reliability</p>	<p>The unaddressed cyber issue: Lack of awareness and training, Lack of policies, procedures, and regulatory standards, “Old school” vs “new school”</p>
<p>Evolve: Transform existing processes or behaviour, re-architect</p>	

Table 4 Cyber resiliency goals compared to categories of navigators cyber experience

When looking back at the results from Paper II compared to the cyber resilience goals and objectives (Bodeau et al., 2011), one can draw lines between the what is found in the interviews and what is

described by MITRE, as shown in Table 4. It can be discussed if the findings is basis for a lack of maritime cyber resilience, but either way, the results suit well as a foundation for tailoring cyber training, considering how to develop an exercise or a course. Considering the first goal, Anticipate, there is need for more common ground amongst navigators, regarding what a cyber-attack really is, how it impacts the vessels operation and the supply chain. For the second goal, Withstand, there is obvious that shipping management need to implement improved procedures and policies for handling cyber incidents. Navigators (at least some, if not all) treat cyber incidents as just another technical error, not properly reflecting that there is an adverse actor on the opposite side of the incident. Considering the specific finding of improvised strategies, maybe shipping management can benefit from that ship crew is traditionally creative problem solvers (Erstad, Lund, et al., 2022, page 87). Although navigators do not know all aspects of cyber risks, they are without doubt the experts of their own systems and a potential angle of enhancement is to utilize this importance of understanding own systems, as discussed and described earlier. The navigators were also confident that a cyber-attack would not compromise the ships safety. Hence, it would be beneficial to include ship crew in designing solutions (i.e., HCD) for handling cyber incidents, which also serve as an argument for designing the CERP. Considering the final goals (recover and evolve), it is only one category related to these, The unaddressed cyber issue. The category also tilts more, if not completely, towards Recover than Evolve. There is un undoubtedly a lack of several contributing factors for increased cyber resilience, such as awareness, training, procedures, and that there is a difference between navigators. Shipping management should strive to raise the bar equally for crew onboard ship, to avoid old school vs new school-categorisation. It is easy to believe that if a crewmember does not self believe they could understand computers or cyber-attacks, they would put less effort into learning it. Considering evolving as a resilience goal, it would seem unreasonable to think that ship crew could evolve rapidly, as the foundation of knowledge considering cyber risks is as low as they describe.

An innovative approach to be to flip the cyber risk to an opportunity, by using cyber resilience training as an opportunity to train the users in systems, perform problem shooting of the systems and become in-depth experts. Both connectivism (Siemens, 2004) and constructivism (Watson, 2001) offer novel approaches to understanding how the modern mariner learns, and more importantly, how maritime training programs could be designed. In summary, the theoretical frameworks of connectivism and constructivism offer valuable lenses which can adapt and evolve maritime training for the 21st century. As cyber risks become increasingly pertinent in maritime operations, the integration of these theories into MET becomes not just advantageous, but necessary. Maritime cyber risk is imminent towards both ships and shore installations. Thus, it is important to consider the aspect of risk when investigating learning theories. Handling and reflecting on risk and consequences is a vital component of how maritime cyber resilience training should be conducted. Whilst not directly focusing on risk aspects or adverse actors, constructivism and connectivism can emphasise risk in the frameworks as they are. Maritime cyber risk can be a node of its own in connectivism, and the teachers or facilitators can provide opportunities for learners to collaborate and share their perspectives on risk assessment and management. While maritime operations have increasingly integrated digital technologies, MET has been relatively slow to incorporate cybersecurity as a core component of education (Heering et al., 2021). The maritime industry has specific cyber risks, such as vulnerabilities in shipboard systems (Kessler & Shepard, 2020), that are not typically covered. This poses a considerable challenge, especially given the prevalence of cyber-attacks targeting maritime assets (Meland et al., 2021). In addition to maritime cyber resilience, the cyber security gap existing in MET curricula could be framed

around theories of risk perception (Larsen et al., 2022), for understanding human behaviour in face of cyber threats. While technical education, as most of STCW are, emphasis calculable and tangible risks, it should also focus on the intangible risks (Erstad, Lund, et al., 2022), and focus on how a cyber risk differs from a ‘traditional’ risk (Erstad et al., 2021). Current MET models focus on either traditional maritime skills or specialized areas such as cyber security, but rarely offer an integrated approach (International Maritime Organization, 2016). This absence highlights the necessity for a new theoretical framework that combines both dimensions, preparing maritime workers for the integrated challenges of cyber security. Today there is a need for cyber seamanship.

6.2 Relevance and usability of Human-Centered Design

The HCD method has acted as a central theme throughout the thesis and all papers, even though not explicitly mentioned in Paper I. Paper I concluded with a working definition of maritime cyber resilience, with an emphasis on learning, and highlighted the importance of the navigator (i.e., human operator) as a central actor at the sharp end of the operation in case of a cyber situation onboard a ship. The purpose of the HCD ‘Identifying the context of use’ is to identify the users, characteristics, goals and tasks, as performed in Paper I. Therefore, it was decided to focus more on user needs and hence navigator experiences in the following paper. By focusing on the navigators and their requirements, training can be tailored to address both the technological and human aspects of maritime operations, making them more intuitive and efficient. Paper II concludes that problem solving for navigators are normally pragmatically handled and that the maritime industry is slow, or even reluctant, to address cyber risk, both in operation but also training and education. The paper argues for why HCD method is suitable when designing cyber awareness training for navigators and the aim of the paper was to provide MET instructors and facilitator with insight knowledge of how navigators experience cyber threat. To put this into practice, Paper III investigated in particular the HCD approach by developing a scenario and training module that both address cyber risk and underlines the importance of understanding the end-users. Even though the navigator has been the primary focus for the thesis, this paper exceeds the navigator and takes a more holistic approach by including a wider number of maritime stakeholders. When working on the HCD process and the maritime cyber simulator scenario, the authors also found that there was a lack of operational tools, procedures, and policies, covering maritime cyber risk situations. Thus, the CERP was invented in Paper IV, in close collaboration with industry actors, more specifically workers in a shipowner company with nautical and IT competence, as well as a Norwegian authority representative with competence within navigation and development of digital solutions. In addition to provide the CERP, Paper IV also investigated the transition from traditional incident handling towards handling of cyber threats, while still focusing on navigators pragmatic handling of problems, as found in Paper II. However, as navigators does not still have formal competence of cyber risk or in-depth competence of management of on-board computer systems, the paper included shore side assistance as a vital part of the response procedure. HCD was not mentioned explicitly in Paper IV either, but the paper indeed acted as a spin-off result of the HCD method, where the focus was to develop solutions for end users.

The result of the HCD process should be usable, thus usability is paramount. Usability is the ‘extent to which a system, product or service can be used by specified user to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use’ (ISO, 2019a, page 3). Effectiveness considers the accuracy and completeness with which users achieve specified goals,

efficiency address resources in relation to the results achieved and satisfaction encompass the extent to which the user's physical, cognitive and emotional responses that result from the use of a system, product or service meet the user's needs and expectations (ISO, 2019a, page 2-3). ISO (2019b) provides a guide on how to implement and assess the HCD process (ISO, 2019a), and in Annex E of the document Human-centred quality is described.

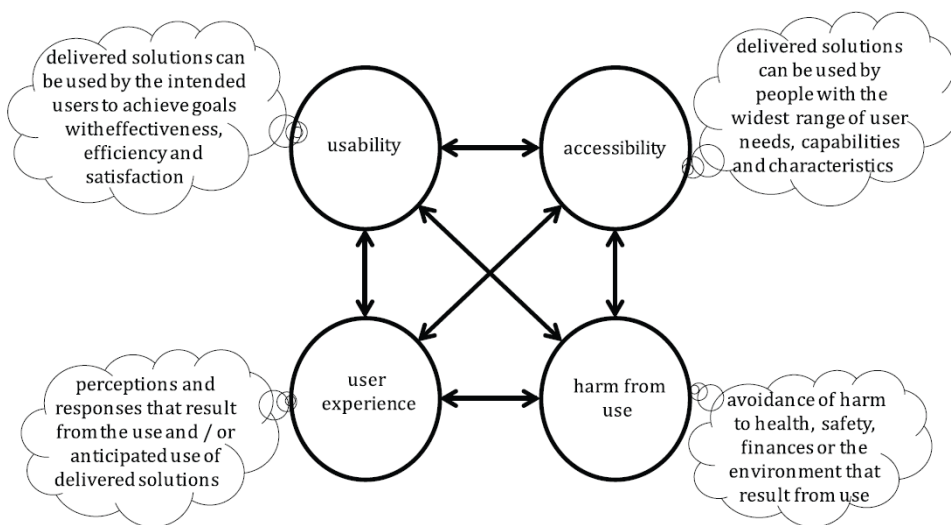


Figure 18 'Human-centred quality' (ISO, 2019b, page 78)

The project followed the HCD process from start to finish and was subject to evaluation and feedback a number of times. In addition to local feedback from the university community, both inspection-based testing and user-based testing was conducted. The maritime cyber resilience scenario was developed as a result of the interviews in Paper II, further developed and presented for a local shipowner conference for Island Offshore AS at university premises where approximately 80 ship officers attended, both deck and engine. In order to disseminate to a larger number of people, the scenario was developed into a movie, with accompanying table-top exercise and presented on an open maritime industry conference, Rederikonferansen, for shipowners and shipping management personnel where approximately 200 persons attended. All these things affected the practical development of the maritime cyber resilience scenarios which were finally conducted as part of a M.Sc. level course in the beginning of 2023, where 18 students attended. Despite diverse backgrounds, ranging from deck officers to IT personnel, a substantial portion of the students replied they learned much from the simulator exercises. On a scale from 1 to 5, where 5 is the highest, nine persons rated 5, seven persons rated 4 and 1 persons rated 3. Feedback form can be found in Annex IV – Course feedback scheme.

7 Conclusions

MET has seen significant advancements over the years, yet gaps remain in addressing the emergent risks associated with modern maritime operations, in particular cyber security concerns. By understanding and integrating various academic theories and perspectives into a new, holistic model for MET, one can bridge the gap from physical safety to cyber safety.

The conceptual frameworks for risk and vulnerability in maritime operations have evolved to include cyber risks. Unlike traditional maritime risks, which have been covered in the theoretical background to this section, the cyber domain poses a different kind of challenge. These require a conceptual shift from safeguarding against known threats to a more proactive, resilience-based approach. As the maritime industry continues to digitalize, the focus should not solely be on maritime cyber security but should equally prioritize maritime cyber resilience. This broader approach would contribute to a more resilient, robust, and holistic maritime cyber maturity. Ignoring this transition could lead to overemphasis on external threats, at the potential cost of overlooking vulnerabilities that could pass the barriers and make an impact within. In a complex, interconnected and inherently risky maritime environment.

In sum, the nexus between maritime training and cyber resilience isn't merely a new topic of interest, it is a necessary evolution in the industry. As the maritime realm grows increasingly interconnected and digital, the training methodologies and curriculum must advance in tandem to ensure the dual goals of maritime safety and cybersecurity are met. This thesis was set out to enhance operational training for maritime cyber resilience, by bridging safety and security through maritime education and training. The project has been conducted through investigating research questions which is answered through scientific published papers, workshops, simulator exercises, and this thesis.

RQ1 is answered through Paper I, the literature review and the theoretical background presented in this thesis. Maritime cyber resilience is understood as an ability which will describe how well a nautical system which is harmed by a cyber incident will endure and return to normal state.

RQ 2 is answered through Paper II and Paper IV and is supported by the workshop report. In order to enhance maritime cyber resilience, both MET, and the maritime industry would benefit of integrating cyber aspects in the normal, day-to-day work, and not as a standalone subject.

RQ 3 is answered through Paper III, supported by the workshops and the practical simulator experiments. By integrating including other learning theories, organizational aspects and a wide range of players, a cyber exercise can enhance both the individual, but also the groups maritime cyber resilience.

The following sections will highlight the thesis academic and industrial impacts and contributions.

7.1 Academic impact and contributions

Considering academic contributions, the thesis has combined Human-Centred Design theory with the development of maritime cyber resilience strategies. HCD is originally intended for the design and development of computer-based interactive systems, however, this thesis proves that HCD theory also fits to design and develop aspects around learning, such as cyber resilience in a maritime education and

training perspective. The thesis has also shed light on and unfolded the combination of theories between maritime safety, cyber security, and cyber resilience. The thesis novelty lies within combining theories of maritime cyber security and resilience engineering, in a human-centred perspective.

Considering academic impacts, the thesis has contributed to creating new courses specific for maritime cyber security and resilience, where the course is designed to be both a M.Sc. level course for active students but also a three-module life-long learning course for professionals. The course has utilized HCD method to develop cyber resilience simulator exercises, which is novel, as it is an innovative way to utilize maritime simulators. It must be explicitly noted that this was not an individual effort, it was in good collaboration with a fellow PhD student. Even though it is argued that cyber should not be a standalone aspect, integrating cyber on the same level as safety in the maritime industry will take time, and the course can be considered a starting point. The thesis has also led to several collaborations between academia and the industry on a national level and led to international projects between different universities.

7.2 Industrial impact and contributions

The maritime industry's interest for maritime cyber resilience have increased rapidly the recent years. By inviting the industry to take an active part in shaping how to develop maritime cyber resilience training, the thesis has contributed to the maritime industry, meeting them on their ground.

Considering the industry specifically, both the simulator exercises in the life-long learning course modules for maritime cyber resilience and the CERP have impacted the industry. The CERP was developed in close collaboration with maritime industry actors and will function as a blueprint when the company will develop their own specific cyber emergency procedures.

The workshops and the simulator exercises served the opportunity to gather people from the industry, with the intent to give something back, as the research project is dependent on industry input and perspectives. The simulator exercises have contributed to a higher acceptance of the cyber problem amongst workers in the industry, as the management could invite workers into the simulators to visualize how a cyber-attack can evolve and further discuss plan of action.

The thesis and the project have proven that academia can be a trusted partner when the industry meet problems which can be seen as a drawback when it comes to competitive advantage in the market. Even though many companies today say they don't compete on safety and security, there have been an increase in demand for cyber security and resilience competence. Even though not original for this project, the thesis has proven that academia can act as a platform for the industry to collaborate, where the simulator has been a "sandbox" considering visualising and handling a known and realistic cyber-attack. In addition, the project has made an impact on shipowner conferences, contributing to sharing knowledge and ideas of maritime cyber resilience.

7.3 Future research

Maritime cyber resilience and this project itself foster many new areas of future research. Firstly, it is imperative to consider other departments on board a ship than just the navigator. The engine department and others, such as deck and welfare departments, are just as important in protecting the ship in terms of cyber risks and vulnerabilities.

The thesis also let autonomous vessels specifically out of scope of this project. There is a lot of new research considering cyber security and autonomous vessels, but it would be a whole other setting than having a human operator on board, controlling the vessel, rather than a vessel being controlled from land or by itself. It would require a specific set of knowledge to understand what cyber risks which affect a remote operation centre for controlling autonomous vessels.

In 2023, there has been an increase in the development of Artificial Intelligence (AI). AI can be seen both as a blessing and a curse. First, it is easy to imagine that adverse actors exploit this tool, making cyber-attacks even more sophisticated with a lower cost and find new ways to exploit cyber risk. On the other hand, one can imagine that AI can be an effective and low-cost extra training instructor considering maritime cyber resilience, aiding the maritime education, and training staff or other course instructors in the industry. AI can make work more effective and is already implemented in cyber security research.

Finally, maritime education and training is a never-ending story. STCW needs to be developed in the years to come with even more implementation of technology, creating new opportunities and new, unimagined risks.

8 References

- Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, 236, 106493. <https://doi.org/https://doi.org/10.1016/j.ocecoaman.2023.106493>
- Alexandrova, A. (2012). Well-being as an object of science. *Philosophy of Science*, 79(5), 678-689.
- Androjna, A., & Perkovič, M. (2021). Impact of spoofing of navigation systems on maritime situational awareness. *Transactions on Maritime Science*, 10(02), 361-373.
- Ashford, W. (2019). *NotPetya offers industry-wide lessons, says Maersk's tech chief*. ComputerWeekly.com. Retrieved 23 November from <https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief>
- Awan, M. S. K., & Al Ghamdi, M. A. (2019). Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). *Journal of Marine Science and Engineering*, 7(10), 350.
- Bainbridge, L. (1983). Ironies of automation. In *Analysis, design and evaluation of man-machine systems* (pp. 129-135). Elsevier.
- Bergström, J., van Winsen, R., & Henriqson, E. (2015). On the rationale of resilience in the domain of safety: A literature review. *Reliability Engineering & System Safety*, 141, 131-141. <https://doi.org/https://doi.org/10.1016/j.res.2015.03.008>
- BIMCO. (2020). The Guidelines on Cyber Security onboard Ships Version 4.0. In *BIMCO (ed.) Version 4.0*.
- Björck, F., Henkel, M., Stirna, J., & Zdravkovic, J. (2015). Cyber Resilience – Fundamentals for a Definition. In A. Rocha, A. M. Correia, S. Costanzo, & L. P. Reis, *New Contributions in Information Systems and Technologies* Cham.
- Blessing, L. T. M., & Chakrabarti, A. (2009). *DRM, a Design Research Methodology* (1. Aufl. ed.). London: Springer Verlag London Limited. <https://doi.org/10.1007/978-1-84882-587-1>
- Bodeau, D., Graubart, R., Heinbockel, W., & Laderman, E. (2015). *Cyber Resiliency Engineering Aid–The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques*. <https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf>
- Bodeau, D., Graubart, R., Picciotto, J., & McQuaid, R. (2011). *Cyber resiliency engineering framework* (MTR110237, MITRECorporation, Issue. https://www.mitre.org/sites/default/files/media/publication/11_4436_2.pdf
- Boin, A., Comfort, L. K., & Demchak, C. C. (2010). THE RISE OF RESILIENCE. In (pp. 1). University of Pittsburgh Press. <https://doi.org/10.2307/j.ctt5hj0c.5>
- Bolbot, V., Kulkarni, K., Brunou, P., Banda, O. V., & Musharraf, M. (2022). Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. *International Journal of Critical Infrastructure Protection*, 100571. <https://doi.org/https://doi.org/10.1016/j.ijcip.2022.100571>
- Bowditch, N. (2002). *The American practical navigator : an epitome of navigation* (Bicentennial ed., Vol. No. 9). National Imagery and Mapping Agency.
- Boyes, H. (2014). Maritime cyber security—securing the digital seaways. *Engineering & Technology Reference*, 1(1), 56-62. <https://doi.org/10.1049/etr.2014.0009>
- Cartwright, N., & Montuschi, E. (2014). *Philosophy of social science: A new introduction*. OUP UK.
- COAST GUARD WASHINGTON DC. (2015). The Coast Guard Proceedings of the Marine Safety and Security Council. Volume 71, Number 4, Winter 2014-2015. <https://apps.dtic.mil/sti/citations/ADA618312>
- Cockcroft, A. N., & Lameijer, J. N. F. (2011). *A guide to the collision avoidance rules : International Regulations for Preventing Collisions at Sea* (7th ed.). Elsevier.
- Creswell, J. W., Poth, C. N., & Creswell, J. W. (2018). *Qualitative inquiry & research design : choosing among five approaches* (4th edition. ed.). Sage.

- Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, 147(2), 432-448. <https://doi.org/https://doi.org/10.1016/j.jfineco.2022.12.002>
- de Bruijne, M., Boin, A., & van Eeten, M. (2010). RESILIENCE: EXPLORING THE CONCEPT AND ITS MEANINGS. In (pp. 13). University of Pittsburgh Press. <https://doi.org/10.2307/j.ctt5hj0c.6>
- Dinu, O., & Ilie, A. (2015). Maritime vessel obsolescence, life cycle cost and design service life. IOP conference series: materials science and engineering,
- DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015). The little-known challenge of maritime cyber security. 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA),
- Douglas, H. (2014). Values in social science. *Philosophy of social science: A new introduction*, 162-182.
- Drazovich, L., Brew, L., & Wetzel, S. (2021, 26-28 July 2021). Advancing the State of Maritime Cybersecurity Guidelines to Improve the Resilience of the Maritime Transportation System. 2021 IEEE International Conference on Cyber Security and Resilience (CSR),
- ENISA. (2011). *ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR*. E. U. A. f. Cybersecurity. <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1>
- Erstad, E., Hopcraft, R., Misas, J. P., & Tam, K. (2023). CERP: A Maritime Cyber Risk Decision Making Tool. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 7, 269-279. <https://doi.org/https://doi.org/10.12716/1001.17.02.02>
- Erstad, E., Hopcraft, R., Vineetha Harish, A., & Tam, K. (2023). A human-centred design approach for the development and conducting of maritime cyber resilience training. *WMU Journal of Maritime Affairs*, 22(2), 241-266. <https://doi.org/10.1007/s13437-023-00304-7>
- Erstad, E., Larsen, M. H., Lund, M. S., & Ostnes, R. (2022). Maritime Cyber Simulator Scenario Workshop report. <https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3037765>
- Erstad, E., Lund, M. S., & Ostnes, R. (2022). Navigating Through Cyber Threats, A Maritime Navigator's Experience. <https://doi.org/https://doi.org/10.54941/ahfe1002205>
- Erstad, E., Ostnes, R., & Lund, M. S. (2021). An Operational Approach to Maritime Cyber Resilience. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15(1), 27-34. <https://doi.org/https://doi.org/10.12716/1001.15.01.01>
- Estay, D. S. (2020). CyberShip Project: Cyber resilience for the shipping industry. <https://orbit.dtu.dk/en/publications/cybership-project-final-project-report>
- European Union Agency for Cybersecurity, Drougkas, A., Sarri, A., & Kyranoudi, P. (2020). *Cyber risk management for ports – Guidelines for cyber security in the maritime sector*. European Network and Information Security Agency. <https://doi.org/doi/10.2824/671060>
- European Union Parliament. (2022). DIRECTIVE (EU) 2022/2555. In *DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*. Official Journal of the European Union: European Union Parliament.
- Farah, M. A. B., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information*, 13(1), 22.
- Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the Future of Cyber War. *Survival*, 53(1), 23-40. <https://doi.org/10.1080/00396338.2011.555586>
- Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. In: Lancaster University.
- Gassmann, O., Frankenberger, K., & Csik, M. (2013). The St. Gallen business model navigator.
- Hareide, O. S. (2020). Coastal Navigation—in a digital era. <https://doi.org/https://fhs.brage.unit.no/fhs-xmlui/handle/11250/2683218>

- Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R., & Helkala, K. (2018). Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, 71(5), 1025-1039. <https://doi.org/10.1017/S0373463318000164>
- Heering, D., Maennel, O., & Venables, A. (2021). Shortcomings in cybersecurity education for seafarers. In *Developments in Maritime Technology and Engineering* (pp. 49-61). CRC Press. <https://doi.org/https://doi.org/10.1201/9781003216582-06>
- Holling, C. S. (1973). Resilience and Stability of Ecological Systems. *Annual review of ecology and systematics*, 4(1), 1-23. <https://doi.org/10.1146/annurev.es.04.110173.000245>
- Hollnagel, E. (2008). Risk + barriers = safety? *Safety Science*, 46(2), 221-229. <https://doi.org/10.1016/j.ssci.2007.06.028>
- Hollnagel, E. (2010). *Resilience engineering in practice : a guidebook* (1st edition. ed.). Ashgate.
- Hollnagel, E. (2013). A tale of two safeties. *Nuclear Safety and Simulation*, 4(1), 1-9.
- Hollnagel, E. (2014a). Is safety a subject for science? *Safety Science*, 67, 21-24. <https://doi.org/https://doi.org/10.1016/j.ssci.2013.07.025>
- Hollnagel, E. (2014b). Resilience engineering and the built environment. *Building Research & Information*, 42(2), 221-228. <https://doi.org/10.1080/09613218.2014.862607>
- Hollnagel, E. (2014c). *Safety-I and safety-II: the past and future of safety management* (1 ed.). Farnham: Ashgate Publishing Ltd. <https://doi.org/10.1201/9781315607511>
- Hollnagel, E., Woods, D. D., & Hollnagel, E. P. (2006). *Resilience Engineering: Concepts and Precepts* (1 ed.). Abingdon: CRC Press. <https://doi.org/10.1201/9781315605685>
- Hontvedt, M., & Arnseth, H. C. (2013). On the bridge to learn: Analysing the social organization of nautical instruction in a ship simulator. *International Journal of Computer-Supported Collaborative Learning*, 8(1), 89-112. <https://doi.org/https://doi.org/10.1007/s11412-013-9166-3>
- Hopcraft, R. (2021). Developing Maritime Digital Competencies. *IEEE Communications Standards Magazine*, 5(3), 12-18. <https://doi.org/https://doi.org/10.1109/mcomstd.101.2000073>
- Hopcraft, R., Harish, A. V., Tam, K., & Jones, K. (2023). Raising the Standard of Maritime Voyage Data Recorder Security. *Journal of Marine Science and Engineering*, 11(2), 267.
- Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation - the case for a cyber code [Article]. *Journal of the Indian Ocean Region*, 14(3), 354-366. <https://doi.org/10.1080/19480881.2018.1519056>
- HP Online Store. (2022). *What is the Average Lifespan of a Computer?* HP. Retrieved 2023 from <https://www.hp.com/in-en/shop/tech-takes/post/average-computer-lifespan>
- IACS. (2020). Rec 166 - Recommendation on Cyber Resilience. In.
- IACS. (2022a). *IACS adopts new requirements on cyber safety*. IACS. Retrieved 20 February from <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/>
- IACS. (2022b). IACS UR E26 Cyber resilience of ships. In. <https://iacs.org.uk/>: International Association of Classification Societies
- IACS. (2022c). IACS UR E27 Cyber resilience of ships equipment. In. <https://iacs.org.uk/>: International Association of Classification Societies
- Illeris, K. (2018). An overview of the history of learning theory. *European Journal of Education*, 53(1), 86-101. <https://doi.org/https://doi.org/10.1111/ejed.12265>
- International Maritime Organization. (2015). *MSC.1/Circ.1512*.
- Guideline on Software Assurance and Human-Centred Design for e-Navigation*
- International Maritime Organization. (2016). *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)*.
- International Maritime Organization. (2017a). *MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management* [http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/Pages/Cyber-security.aspx](http://www.imo.org/en/OurWork/Security/Guide%20to%20Maritime%20Security/Pages/Cyber-security.aspx)
- International Maritime Organization. (2017b). *Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems*

[http://www.imo.org/en/OurWork/Security/Guide to Maritime Security/Pages/Cyber-security.aspx](http://www.imo.org/en/OurWork/Security/Guide%20to%20Maritime%20Security/Pages/Cyber-security.aspx)

- International Maritime Organization. (2020). *SOLAS, Consolidated Edition, 2020*. International Maritime Organization.
- International Maritime Organization. (2021). *2000 HSC Code Edition 2021 Ed.*
- International Maritime Organization. (2023). *The International Safety Management (ISM) Code*. IMO. Retrieved 23 February from <https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx>
- ISO. (1985). ISO 5807:1985 Information processing — Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts. iso.org: ISO.
- ISO. (2017). ISO/IEC 27001:2017 Information security, cybersecurity and privacy protection — Information security management systems — Requirements. In. iso.org: ISO.
- ISO. (2019a). 9241-210: 2019 Ergonomics of human-system interaction. In *Part 210: Human-Centred Design for Interactive Systems* (pp. 33). iso.org: International Organization for Standardization.
- ISO. (2019b). 9241-220:2019. In *Part 220: Processes for enabling, executing and assessing human-centred design within organizations*. iso.org: International Organization for Standardization.
- Jensen, L. (2015). Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*, 5(4), 35-39. <https://doi.org/10.22215/timreview/889>
- Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. Justis- og beredskapsdepartementet. (2000). *NOU 2000: 31 - Hurtigbåten MS Sleipners forlis 26. november 1999*. <https://www.regjeringen.no/no/dokumenter/nou-2000-31/id143395/>
- Karahalios, H. (2020). Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. *Journal of transportation security*, 13(3), 179-201. <https://doi.org/10.1007/s12198-020-00223-1>
- Kechagias, E. P., Chatzistelios, G., Papadopoulos, G. A., & Apostolou, P. (2022). Digital transformation of the maritime industry: A cybersecurity systemic approach. *International Journal of Critical Infrastructure Protection*, 37, 100526. <https://doi.org/https://doi.org/10.1016/j.ijcip.2022.100526>
- Kessler, G. C., Craiger, J. P., & Haass, J. C. (2018). A Taxonomy Framework for Maritime Cybersecurity: A Demonstration Using the Automatic Identification System [Article]. *TransNav: International Journal on Marine Navigation & Safety of Sea Transportation*, 12(3), 429-437. <https://doi.org/10.12716/1001.12.03.01>
- Kessler, G. C., & Shepard, S. D. (2020). *Maritime Cybersecurity: A Guide for Leaders and Managers*. Kessler & Shepard.
- Kim, T.-e., Sharma, A., Bustgaard, M., Gyldensten, W. C., Nymoen, O. K., Tusher, H. M., & Nazir, S. (2021). The continuum of simulator-based maritime training and education. *WMU Journal of Maritime Affairs*, 20(2), 135-150. <https://doi.org/10.1007/s13437-021-00242-2>
- Kuhn, K., Bicakci, S., & Shaikh, S. A. (2021). COVID-19 digitization in maritime: understanding cyber risks. *WMU Journal of Maritime Affairs*, 20(2), 193-214.
- Larsen, M. H., & Lund, M. S. (2021). Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. *IEEE Access*, 9, 144895-144905. <https://doi.org/10.1109/ACCESS.2021.3122433>
- Larsen, M. H., Lund, M. S., & Bjørneseth, F. B. (2022). A model of factors influencing deck officers' cyber risk perception in offshore operations. *Maritime Transport Research*, 3, 100065. <https://doi.org/https://doi.org/10.1016/j.martra.2022.100065>
- Le Coze, J. C. (2019). Vive la diversité! High Reliability Organisation (HRO) and Resilience Engineering (RE). *Safety Science*, 117, 469-478. <https://doi.org/https://doi.org/10.1016/j.ssci.2016.04.006>
- Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety*. The MIT Press.
- Linkov, I., & Kott, A. (2019). Fundamental Concepts of Cyber Resilience: Introduction and Overview. In A. Kott & I. Linkov (Eds.), *Cyber Resilience of Systems and Networks* (pp. 1-25). Springer International Publishing. https://doi.org/10.1007/978-3-319-77492-3_1

- Longo, G., Russo, E., Armando, A., & Merlo, A. (2022). Attacking (and defending) the Maritime Radar System. *arXiv preprint arXiv:2207.05623*.
- Lund, M. S., Gulland, J. E., Hareide, O. S., Jøsok, Ø., & Weum, K. O. C. (2018). Integrity of Integrated Navigation Systems. In: IEEE.
- Lund, M. S., Hareide, O. S., & Jøsok, Ø. (2018). An Attack on an Integrated Navigation System. In: Sjøkrigsskolen.
- Lutzhöft, M., & Oltedal, H. A. (2018). *Managing Maritime Safety* (1 ed.). Milton: Routledge. <https://doi.org/10.4324/9780203712979>
- Lützhöft, M., Sherwood Jones, B., Earthy, J., & Bergquist, C. (2006). Making safety by tying the knot: examining resilience in shipping. Proceedings of The 2nd Symposium on Resilience Engineering. Juan-les-Pins, France, November,
- Lützhöft, M., & Vu, V. D. (2018). Design for safety. In *Managing maritime safety* (pp. 106-140). Routledge.
- Lützhöft, M. H., & Dekker, S. W. A. (2002). On Your Watch: Automation on the Bridge. *The Journal of Navigation*, 55(1), 83-96. <https://doi.org/10.1017/S0373463301001588>
- Madni, A. M., Erwin, D., & Sievers, M. (2020). Constructing models for systems resilience: challenges, concepts, and formal methods. *Systems (Basel)*, 8(1), 1-14. <https://doi.org/10.3390/systems8010003>
- Madni, A. M., & Jackson, S. (2011). Towards a conceptual framework for resilience engineering. *IEEE Engineering Management Review*, 39(4), 85-102. <https://doi.org/10.1109/EMR.2011.6093891>
- Mallam, S. C., Nazir, S., & Renganayagalu, S. K. (2019). Rethinking Maritime Education, Training, and Operations in the Digital Era: Applications for Emerging Immersive Technologies. *Journal of Marine Science and Engineering*, 7(12), 428. <https://www.mdpi.com/2077-1312/7/12/428>
- Malterud, K. (2012). Systematic text condensation: a strategy for qualitative analysis. *Scandinavian journal of public health*, 40(8), 795-805.
- Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø., & Nesheim, D. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*. <https://doi.org/https://doi.org/10.12716/1001.15.03.04>
- Melnikovas, A. (2018). Towards an Explicit Research Methodology: Adapting Research Onion Model for Futures Studies. *Journal of futures Studies*, 23(2).
- Melnyk, O., Onyshchenko, S., Pavlova, N., Kravchenko, O., & Borovyk, S. (2022). Integrated Ship Cybersecurity Management as a Part of Maritime Safety and Security System. *International Journal of Computer Science and Network Security*, 22(03), 135-140.
- NHL Stenden. (2023). *MCAD Maritime Cyber Attack Database*. NHL Stenden. Retrieved 13.09 from <https://maritimecybersecurity.nl/>
- NIST, G. M. (2023). *The NIST Cybersecurity Framework 2.0*. <http://dx.doi.org/10.6028/nist.cswp.29.ipd>
- NIST, N. I. o. S. a. T. (2018). Framework for improving critical infrastructure cybersecurity. In *Version 1.1*.
- NORMA Cyber. (2022). *NORMA Cyber Annual Threat Assessment 2022*. <https://www.normacyber.no/news/norma-annual-threat-assessment-2022>
- NORMA Cyber. (2023). *NORMA Cyber Annual Threat Assessment 2023*. <https://www.normacyber.no/news/48o1qpgi66klzqspdg7jg3kwta3172>
- Norman, D. (2013). *The design of everyday things: Revised and expanded edition*. Basic books.
- FOR-2011-12-22-1523 Forskrift om kvalifikasjoner og sertifikater for sjøfolk, (2012). https://lovdata.no/dokument/SF/forskrift/2011-12-22-1523/*#*
- Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research.
- Oommen, P. G. (2020). Learning Theories – Taking a Critical Look at Current Learning Theories and the Ideas Proposed By Their Authors. *Asian Journal of Research in Education and Social Sciences*(1), 27-32% V 22. <https://myjms.mohe.gov.my/index.php/ajress/article/view/8730>

- Oruc, A., Amro, A., & Gkioulos, V. (2022). Assessing Cyber Risks of an INS Using the MITRE ATT&CK Framework [Article]. *Sensors* (14248220), 22(22), 8745. <https://doi.org/10.3390/s22228745>
- Park, C., Kontovas, C., Yang, Z., & Chang, C.-H. (2023). A BN driven FMEA approach to assess maritime cybersecurity risks. *Ocean & Coastal Management*, 235, 106480. <https://doi.org/https://doi.org/10.1016/j.ocecoaman.2023.106480>
- Parsons, J., & Allen, C. (2018). The history of safety management. In (1 ed., pp. 16-31). United Kingdom: Routledge. <https://doi.org/10.4324/9780203712979-3>
- Patriarca, R., Bergström, J., Di Gravio, G., & Costantino, F. (2018). Resilience engineering: Current status of the research and future challenges. *Safety Science*, 102, 79-100. <https://doi.org/https://doi.org/10.1016/j.ssci.2017.10.005>
- Potamos, G., Theodoulou, S., Stavrou, E., & Stavrou, S. (2023). Building Maritime Cybersecurity Capacity Against Ransomware Attacks. Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science 2022; 20–21 June; Wales,
- Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber Physical Systems Security for Maritime Assets. *Journal of Marine Science and Engineering*, 9(12), 1384. <https://www.mdpi.com/2077-1312/9/12/1384>
- Radmilo, I., Gudelj, A., & Ristov, P. (2017). Information Security in Maritime Domain. International Maritime Science Conference,
- Rausand, M. (2013). *Risk assessment: theory, methods, and applications* (Vol. 115). John Wiley & Sons. <https://doi.org/10.1002/9781118281116>
- Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management* (pp. 33-47). Springer. https://doi.org/https://doi.org/10.1007/978-3-319-23570-7_5
- Relling, T., Lützhöft, M., Ostnes, R., & Hildre, H. P. (2018). A human perspective on maritime autonomy. International Conference on Augmented Cognition,
- Righi, A. W., Saurin, T. A., & Wachs, P. (2015). A systematic literature review of resilience engineering: Research areas and a research agenda proposal. *Reliability Engineering & System Safety*, 141, 142-152. <https://doi.org/https://doi.org/10.1016/j.ress.2015.03.007>
- Ringdal, K. (2018). *Enhet og mangfold : samfunnsvitenskapelig forskning og kvantitativ metode* (4. utg. ed.). Fagbokforl.
- Roeser, S. (2012). *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk* (Vol. 1). Springer Science & Business Media. <https://doi.org/http://dx.doi.org/10.1007/978-94-007-1433-5>
- Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2021). *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*. N. I. o. S. a. T. (U.S.). <http://dx.doi.org/10.6028/nist.sp.800-160v2r1>
- Sahay, R., Meng, W., Estay, D. A. S., Jensen, C. D., & Barfod, M. B. (2019). CyberShip-IoT: A dynamic and adaptive SDN-based security policy enforcement framework for ships. *Future Generation Computer Systems*, 100, 736-750. <https://doi.org/https://doi.org/10.1016/j.future.2019.05.049>
- Saunders, M. N. K., Lewis, P., & Thornhill, A. (2016). *Research methods for business students* (7th ed.). Pearson.
- Scanlan, J., Hopcraft, R., Cowburn, R., Trovåg, J. M., & Lützhöft, M. (2022). Maritime Education for a Digital Industry. *Necesse*, 7(1), 75. <https://fhs.brage.unit.no/fhs-xmlui/handle/11250/3001473>
- Schinas, O., & Metzger, D. (2023). Cyber-seaworthiness: A critical review of the literature. *Marine Policy*, 151, 105592. <https://doi.org/https://doi.org/10.1016/j.marpol.2023.105592>
- Schröder-Hinrichs, J.-U., Praetorius, G., Graziano, A., Kataria, A., & Baldauf, M. (2016, 2016). Introducing the Concept of Resilience into Maritime Safety.
- Searle, J. R. (2006). Social ontology: Some basic principles. *Anthropological theory*, 6(1), 12-29. <https://doi.org/https://doi.org/10.5565/rev/papers/v80n0.1769>
- Sellberg, C. (2017). Simulators in bridge operations training and assessment: a systematic review and qualitative synthesis. *WMU Journal of Maritime Affairs*, 16(2), 247-263. <https://doi.org/10.1007/s13437-016-0114-8>

- Sellberg, C., Lindmark, O., & Rystedt, H. (2018). Learning to navigate: the centrality of instructions and assessments for developing students' professional competencies in simulator-based training. *WMU Journal of Maritime Affairs*, 17(2), 249-265. <https://doi.org/https://doi.org/10.1007/s13437-018-0139-2>
- Sepúlveda Estay, D. A., Sahay, R., Barfod, M. B., & Jensen, C. D. (2020). A systematic review of cyber-resilience assessment frameworks. *Computers & Security*, 97, 101996. <https://doi.org/https://doi.org/10.1016/j.cose.2020.101996>
- Shah, S. K. (2004). *The Evolving Landscape of Maritime Cybersecurity* [30]. [Jamaica, N.Y.] :
- Shapiro, L. R., Maras, M.-H., Velotti, L., Pickman, S., Wei, H.-L., & Till, R. (2018). Trojan horse risks in the maritime transportation systems sector. *Journal of transportation security*, 11(3), 65-83. <https://doi.org/10.1007/s12198-018-0191-3>
- Siemens, G. (2004). Connectivism: A learning theory for the digital age. elearnspace. In.
- Slovic, P. (1987). Perception of risk. *Science*, 236(4799), 280-285. <https://doi.org/http://dx.doi.org/10.4324/9781315661773>
- Stoker, G., Greer, J., Clark, U., & Chiego, C. (2022). Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution. Proceedings of the EDSIG Conference ISSN,
- Strauch, B. (2018). Ironies of Automation: Still Unresolved After All These Years. *IEEE Transactions on Human-Machine Systems*, 48(5), 419-433. <https://doi.org/10.1109/THMS.2017.2732506>
- Svilicic, B., Brčić, D., Žulkin, S., & Kalebic, D. (2019). Raising Awareness on Cyber Security of ECDIS. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 13(1), 231-236. <https://doi.org/10.12716/1001.13.01.24>
- Svilicic, B., Kristić, M., Žuškin, S., & Brčić, D. (2020). Paperless ship navigation: cyber security weaknesses. *Journal of transportation security*, 13(3), 203-214. <https://doi.org/10.1007/s12198-020-00222-2>
- Svilicic, B., Rudan, I., Frančić, V., & Mohović, D. (2020). Towards a Cyber Secure Shipboard Radar. *The Journal of Navigation*, 73(3), 547-558. <https://doi.org/10.1017/S0373463319000808>
- Svilicic, B., Rudan, I., Jugović, A., & Zec, D. (2019). A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *Journal of Marine Science and Engineering*, 7(10), 364. <https://www.mdpi.com/2077-1312/7/10/364>
- Tam, K., Hopcraft, R., Moara-Nkwe, K., Misas, J. P., Andrews, W., Harish, A. V., Giménez, P., Crichton, T., & Jones, K. (2021). Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. <https://doi.org/https://doi.org/10.4236/jts.2022.121001>
- Tam, K., & Jones, K. (2019). MaCRA: a model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1), 129-163.
- Tjora, A. H., & Tjora, A. H. (2021). *Kvalitative forskningsmetoder i praksis* (4. utgave. ed.). Gyldendal.
- Tongur, S., & Engwall, M. (2014). The business model dilemma of technology shifts. *Technovation*, 34(9), 525-535. <https://doi.org/https://doi.org/10.1016/j.technovation.2014.02.006>
- UoB, U. o. B. (2022). *Constructivism*. Univeristy of Buffalo. Retrieved 18 November from <https://www.buffalo.edu/catt/develop/theory/constructivism.html>
- Von Solms, R., & van Niekerk, J. (2013). From information security to cyber security. *Computers & Security*, 38(C), 97-102. <https://doi.org/10.1016/j.cose.2013.04.004>
- Vu, V., & Lützhöft, M. (2020). Human-Centred Design application in the Maritime Industry Challenges and Opportunities. Human Factors, London.
- Wahl, A., Kongsvik, T., & Antonsen, S. (2020). Balancing Safety I and Safety II: Learning to manage performance variability at sea using simulator-based training. *Reliability Engineering and System Safety*, 195. <https://doi.org/10.1016/j.ress.2019.106698>
- Wahl, A. M. (2020). Expanding the concept of simulator fidelity: the use of technology and collaborative activities in training maritime officers. *Cognition, Technology & Work*, 22(1), 209-222. <https://doi.org/https://doi.org/10.1007/s10111-019-00549-4>
- Watson, J. (2001). Social constructivism in the classroom. *Support for Learning*, 16(3), 140-147. <https://doi.org/https://doi.org/10.1111/1467-9604.00206>
- Whitman, M. E., & Mattord, H. J. (2009). *Principles of information security 3rd Edition*. Cengage learning.

- Wolsing, K., Saillard, A., Bauer, J., Wagner, E., Sloun, C. v., Fink, I. B., Schmidt, M., Wehrle, K., & Henze, M. (2022, 26-29 Sept. 2022). Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset. 2022 IEEE 47th Conference on Local Computer Networks (LCN),
- Woltjer, R., Nevhage, B., Nilsson, S., Oskarsson, P., Hermelin, J., Trnka, J., & Cedrini, V. (2015). *Consolidation of resilience concepts and practices for crisis management*. https://h2020darwin.eu/project-deliverables/#link_acc-deliverable_d1-1
- World Economic Forum. (2023). *The Global Risks Report 2023*. <https://www.weforum.org/reports/global-risks-report-2023/>
- Yu, H., Meng, Q., Fang, Z., & Liu, J. (2023). Literature review on maritime cybersecurity: state-of-the-art. *The Journal of Navigation*, 1-14. <https://doi.org/10.1017/S0373463323000164>
- Ölçer, A. I., Kitada, M., Lagdami, K., Ballini, F., Alamouh, A. S., & Masodzadeh, P. G. E. (2023). *Transport 2040: Impact of Technology on Seafarers - The Future of Work*. https://commons.wmu.se/lib_reports/78/

Annex I – Published scientific papers and workshop report

Paper I

An operational approach to maritime cyber resilience

An Operational Approach to Maritime Cyber Resilience

E. Erstad¹, R. Ostnes¹ & M.S. Lund²

¹Norwegian University of Science and Technology, Ålesund, Norway

²Norwegian Defence University College, Lillehammer, Norway

ABSTRACT: As a result of the last decades development of technology and increased connectivity of maritime vessels, the need for maritime cyber security is undoubtedly present. In 2017, IMO officially recognized "... the urgent need to raise awareness on cyber threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks". Thus, Maritime Cyber Resilience is seen as key by IMO in the improvement of the maritime cyber security. It is assumed that human error is the cause of more than half successful cyber-attacks. If technology somehow fails, in example because of a cyber threat, the human is expected to handle the problem and provide a solution. It is therefore necessary to focus on the human aspect when considering maritime cyber threats. This paper aims to provide a working definition of "Maritime Cyber Resilience". Further, the paper argues why the human should be a focus of study, as the human is at the sharp edge in a potential maritime cyber emergency.

1 INTRODUCTION

There is no longer a question of "if" an organization is harmed by a cyber incident, but "when" [41]. There is therefore a need for cyber resiliency in maritime operations. International Maritime Organization (IMO) recognizes in the resolution "Maritime Cyber Risk Management in the Safety Management Systems" [31] that shipping needs to be operationally resilient towards cyber risks. Thus, the concept of "Maritime Cyber Resilience" can be seen as of importance in the improvement of maritime cyber security.

IMO, as the global standard-setting authority for the safety and security in shipping, further provides the "Guidelines on Cyber Risk Management" [29], as a result of the resolution [31]. The guidelines provide high-level recommendations for maritime cyber risk management and includes functional elements to mitigate cyber risks. IMO urges ship owners to

implement a cyber risk management approach, which is meant to be resilient towards cyber risks. This raises the question regarding what maritime cyber resilience is and how it can be defined. Resilience and risk, as well as robustness, are connected terms, yet not the same thing [38]. "Cyber risk management" is properly addressed in the Guidelines and means "... the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders." [29]. Even though maritime cyber resilience is also addressed by IMO, it is not as properly defined in the way that cyber risk management is. As maritime cyber resilience is stated of importance for IMO, it should be useful to provide a working definition of the term for future research.

A literature review was conducted in March 2021, aiming to find a definition of "Maritime Cyber

Resilience". The search phrase "Maritime Cyber Resilience" was searched for in the "International Journal on Marine Navigation and Safety of Sea Transportation" (TransNav) [55], Sage Journals [49], as well as Springer Link [51], which provided zero results and no definition. In addition, a search on Orin [46], the Norwegian University of Science and Technology (NTNU) library search engine covering the most of what NTNU University Library has to offer, only four different articles [13, 34, 36, 44] were provided as results, whereas none of the articles provided a definition of what maritime cyber resilience is. This article aims to provide a working definition of "maritime cyber resilience" which can be used in future research. This will be achieved through breaking up the term and analyze what is important to consider in each momentum of the term. In addition, the operational aspect of maritime cyber resilience will be explored, by investigating the human aspect in maritime cyber resilience.

Traditionally, there are two ways to address a maritime risk: by technological measures or by human factors [17]. Commercial cyber security protection measures provided by companies aiming to make ship systems cyber secure are mostly technical protection mechanisms. Fitton, Prince, Germond and Lacy [16] describe the maritime environment as divided into three elements: information, technology, and people. However, more attention is given to the technical aspect of cyber security [4, 8, 27], than the human aspect. Furthermore, several guidelines emphasize the importance of technical maritime cyber security and resilience [5, 15, 26]. The solutions provide less considerations to operational aspect of maritime cyber security and resilience, and what the human, e.g. the navigator, are supposed to do if e.g. the navigational systems fail to function. Humans are often considered the weak link in a sociotechnical system, however, also the agent of a system which can bring order to an emergency situation [11]. There is a connection between unexpected events and lack of control [58], and when technology fails the human is expected to "take the wheel" [3]. It is important to note that the implementation of more technology in a maritime system does not necessarily cohere with the reduction of human error [48]. Maritime organizations are different [29], and every maritime vessel may be considered a prototype [7]. This may argue why the human aspect is important for the concept of maritime cyber resilience, especially in a nautical operation.

Section 1 has provided background and introduction to the paper, as well as a literature review of "Maritime Cyber Resilience". Section 2 will explore what a maritime operation is, emphasizing the nautical part of a maritime operation, as well as the problems connected with navigation. Section 3 explores the concept maritime cyber security, what is threatening the operation of navigation and how the cyber threats have been tackled traditionally. Further, section 4 investigates the concept of cyber resilience, deriving from the concept cyber security being merged with the concept of resilience. The three previous sections will be synthesized in section 5, explaining how maritime cyber resilience can be defined. Section 6 will describe how a cyber threat situation is different from a more known emergency, and further emphasize why the human is important in

this setting. Section 7 provides summary and conclusion.

2 MARITIME OPERATION

This section will explore the nautical part of a "maritime operation", as well as highlighting what is important for such operations. All over the world there are maritime operations going on, such as offshore operations, fishing, military operations, and passenger/cargo operations. A maritime operation can even be the remote operation of a vessel from land, or the coordination of a search- and rescue operation from a rescue coordination centre. The maritime operation will be dependent on the context of the operation. The words by themselves have a board meaning, as "maritime" can be defined as "connected with human activities at sea" or "near the sea or coast" [9], and "operation" can be defined as "an activity that is planned to achieve something" [10]. Thus, maritime operations can be many things, but at least it must be related to human activities to achieve something at sea, or in relation to the sea. One very important aspect of most maritime operations is the need to know one's position and direction, which makes the concept of navigation of importance to the maritime operations.

A ship's bridge can be considered as a socio-technical system [11] on which the navigator is the responsible actor expected to ensure the vessel's safety and security. The navigator interacts with the navigational instruments, as well as with other crew members of the bridge team and others in the maritime traffic system. The navigator has three main duties: navigation, collision avoidance and ship management [7], and part of this is the navigator's responsibility to find and fix the vessel's position. Traditionally this was carried out manually, while navigators today work more like system operators, monitoring the vessel's automatic presented position on the ECDIS (Electronic Chart Display and Information System) [7], usually with the input of a GNSS (Global Navigation Satellite System) sensor [20]. This gives the navigator the opportunity to perform also other tasks, as the vessel's position is automatically projected on the ECDIS.

Navigation is a technology driven practice [29], ranging from celestial navigation with relatively unprecise precision, to electronical navigation with high precision [7], close to centimeter positioning of the vessel. From earlier days, a ship's position was determined by the stars and the sun, and as the technology developed, more advanced instruments have been introduced to the ship bridge. Several types of navigation are available, for example dead reckoning, piloting, celestial navigation, radio navigation, RADAR (Radio Detection And Ranging) navigation and satellite navigation [7, 12]. Whatever methods a navigator chooses to use, there are usually three challenges to be solved considering navigation. These are the determination of position, direction and distance [12], which will provide the navigator with the vessel's previous-, present-, and predicted future position. The International Convention for the Safety of Life at Sea (SOLAS), chapter V/15 provides

regulations regarding bridge design as well as SOLAS V/18 provides performance standards of type approved navigational systems. Also, Integrated Navigation Systems (INS) are recommended by IMO [30] to be installed on ships built after 2011.

Today, the vessels are operated by both IT (Information Technology) and OT (Operational Technology) systems [5]. IT-systems are used for storing and processing data information, such as information on persons onboard the vessel and their next of kin, the different policies and procedures relevant for the vessel, the vessel's certificates and compliance documents, amongst other information. OT-systems are used for controlling the vessel and its movement, as well as controlling the industrial systems onboard, such as thruster direction and force, rudder angle, cargo handling, ballast water handling, power distribution and navigational aiding system [5]. As the navigational systems are becoming more digitalized and increasingly being networked, the ships are getting more dependent on cyber systems for safe and efficient navigation [20].

To summarize this section, the nautical operation can be claimed to be of great importance for maritime operations where ships are involved. The navigator needs to know where the vessel is to carry out safe operations. In next section, maritime cyber security will be explored.

3 MARITIME CYBER SECURITY

There is a lot of problems connected with the concept of maritime cyber security and the research area is not well studied [14]. "Cyber security" derives from "information security", and are similar terms, but not the same [50]. What distinguish these terms are what they are protecting. Information in itself can both be in knowledge, material or electronic form [36], however, in this paper only the electronic form will be addressed. Information security concerns the protection of data information, such as administration of business plans and procedures, as well as the technological structures and protection measures around the information. In its most general sense, cyber security concerns the protection of cyber-systems against cyber threats [47]. Cyber security comprehends a broader meaning than information security, including everything from the protection of people using the cyber systems to the protection of national infrastructure depending on cyber-systems [50]. Traditionally, the confidentiality, integrity and availability has been seen as the characteristics in need of protection [5], when considering information security and cyber security [32, 33]. For IT-systems, this considers the protection of the information within the system and the technology storing, processing, and protecting that information. For maritime OT-systems this also considers the projection of the right information at the right time for the navigator, i.e. using the INS for safe navigation. The navigator is then dependent on the correct input of position, as well as the vessel's speed, to be able to determine situations of collision avoidance. This implies further that what is most important for the maritime cyber security aspect of nautical operations is the integrity

and availability of the information presented and the system functionality, with less attention paid to the confidentiality aspect [5]. Still, as the level of complexity in information systems are increasing, these characteristics are important to protect, but no longer adequate [50, 57]. New protection measures and models which exceeds these characteristics must be implemented, and [57] urges the need to implement accuracy, authenticity, utility, and possession. These measures will most probably aid the security process, yet these protection measures are only technological measures, paying less attention to the operational aspect. This may serve as an argument to emphasize the navigator as an important asset. As the cyber security vendors often only consider the technological parts of the maritime environment, it is vital to remember that a single part of the system cannot be seen in isolation, but rather must be seen in relation to other parts. In contrast to a technical computer system, a human cannot be as easily patched, corrected, or rewritten. The human can be trained to avoid danger, yet there is always a possibility of error, manipulation, coercion, or sedition in every human-machine interaction [16].

A vessel's IT and OT systems have previously been protected from cyber threats, as the vessels have been "air gaped", meaning the ships have been isolated at sea, unconnected to the internet. In addition, the onboard IT and OT systems have been segregated. However, today the demand for remote monitoring and control, as well as increased connectivity and interconnections due to more complex vessels are threatening this natural protection. One of today's emerging challenges is the cyber threat towards safe navigation, which is also a reason why IMO has addressed the issue. Today there is an overweight of electronically navigated vessels, which makes the vessels vulnerable to cyber-attacks. IMO urges the need for safe and secure shipping, and IMO places "Maritime Cyber Risk" [29, 31] under banner of "Maritime Security" [28]. The idea of maritime cyber security is to protect the given system from cyber risk. "Maritime Cyber Security" can be defined as "... a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems..." and "... maritime cyber security is concerned with the reduction of the consequences of cyber-attacks on maritime operations" [20]. A cyber risk can be defined as a risk caused by a cyber threat, and cyber threat is a "threat that exploits cyberspace" [47]. Thus, a "maritime cyber threat" is here understood as a cyber threat affecting the maritime domain, in this paper related to the cyber threats which affect navigational systems on board ships, as well as the navigator operating the navigation system. Cyber risks, as financially risks, affects a company's bottom line, by driving up costs and can bring harm to the revenue [4]. This can be a factor with regards to the secrecy of cyber incidents in the maritime industry [37, 43], where for example the fear of losing a charter contract may succeed the cost of paying ransom to a hacker. What are reported in the media are only the huge cyber accidents, and there is reason to believe there are huge dark numbers, as 47% of seafarers report that they have been the target of a cyber-attack [37]. A cyber security consultancy company reported recently that as much as up to 75% of the vessels the company had been studying, had

interconnected IT and OT systems, even though the network diagrams showed the systems to be segregated and the vessels superintendents told them the networks were segregated [45]. As ships are becoming highly technological and complex systems, the potential surface for cyber-attacks is also increasing, yet there is apparently only a small amount of seafarers which have received any form of cyber training [37]. Recent research [2, 20, 39, 52–54] shows that cyber-attacks can interfere with either one or several of the tasks of navigation.

In this paper, the authors emphasize Hareide's [20] definition of "maritime cyber security", which will be understood as the protection from cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. In the next section, the paper will explore the concept of "cyber resilience", as cyber resilience can be viewed as part of cyber security [6], and further investigate how cyber resilience can be applied to nautical operations.

4 CYBER RESILIENCE

Resilience can be ecological, financial, psychological, technical, and organizational [42], amongst many others forms. Literature reviews indicates there are over 300 different definitions of the term "resilience" [58]. Resilience can be many things, depending on the context of the matter [18]. The aim of this paper is not to untangle the definition of resilience itself, but it is important to understand that also resilience is dependent on the context.

The goal of risk management is to be in a state "free from danger or threat", while resilience management focus on system recovery [38]. A way to say this is that resilience management processes acknowledge that "free from danger or threat" is an impossible system state. This view matches with Hollnagel's approach to resilience [21]. For enhancing risk assessment process and risk management process, Johnsen [35] emphasizes the need to implement resilience principles, which further strengthen the resilience to be a part of something, and not necessarily a standalone concept or ability. Resilience should be considered during the risk assessment and management processes, as any other risk mitigation action [35].

The navigational equipment of a vessel is its critical infrastructure because that makes the ship move safely from A to B, which is controlled by the navigator. Resilience is a highly desirable property for critical infrastructure [35], and Hollnagel [22] argues that a system cannot be resilient but can have resilient abilities. A key feature of a resilient organization is that it does not lose control and is able to continue and recover [35]. Hollnagel [21] argues that the concept of resilience is changing from considering materials or structures and shifting towards the functioning or performance of a system, and as previously highlighted, a ship bridge can be considered a sociotechnical system. Resilience focuses on enhancing a system's response to crisis rather than on the crisis itself and its causes [1]. Resilience also

needs to consider emerging and unknown threats [38], which further supports the resilience assumption that a system cannot be free from danger or threat. The goal of increased resilience is overall improved system functionality, and what is particularly interesting for this paper is the concept of cyber resilience.

As stated earlier, IMO urges the maritime industry to incorporate resilience principles in the maritime cyber risk management. IMO applies National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" [4] principles to the risk management approach, where the following steps are emphasized; Identify, Protect, Detect, Respond and Recover. The purpose of the framework is quite clear, to provide organizations with tools to improve the cyber security and resilience of the organization, regardless of the size or degree of cyber security risk and cyber security sophistication. However, when considering resilience, the framework almost stops after the process of "Recover". Cyber resilience should be treated as an iterative and simultaneously process [40]. The framework also implies that "recovery plan is executed during or after a cybersecurity incident". This raises the question if it even is possible to plan for what one does not have knowledge of, and do not see the consequences of, until it is too late. As demonstrated by Lund [39] this can potentially be the case with cyber incident.

Bodeau and Graubart [6] urges that people engaging in enhancing cyber resilience, must understand the context of where they aim to improve cyber resilience. This means there is a need for a framework to apply, as well as identify technologies and practices which could be integrated into the relevant systems and operations. The MITRE "Cyber Resilience Engineering Framework" [6] defines cyber resiliency as: "The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function." This concept is not so different from the NIST frameworks principles, yet includes the momentum of evolving, which is seen as an important ability of the concept of resilience. The NIST framework emphasized by IMO can be claimed to lack the momentum of learning and evolving, still, the NIST framework are more directed to the cyber security aspect of the cyber risk mitigation. Hollnagel [24] also addresses this issue when addressing resilience engineering, by emphasizing the momentum of "Learning" as an important aspect of resilience. The MITRE framework highlights that the momentum of evolving corresponds with Hollnagel's momentum of learning [6].

As resilience can be seen as an emergent property, cyber resilience must be engineered [6]. The MITRE framework has a strong fundament in Madni's conceptual framework for Resilience Engineering [40], which again is founded partly on Hollnagel's principles of resilience engineering [23]. The MITRE resilience goals are Anticipate, Withstand, Recover and Evolve, which will further be treated as the resilience abilities under study in this paper. A vital

difference between a computer and a human, is that the computer only needs to learn things once, however, a computer cannot do things it has not learned, as the human can. A maritime vessel can be seen independently as a “working machine”, but also conforms a society of different types of seafarers, such as navigators, engineers, and sailors. Hence, it might be need for a combination of the mentioned perspective of cyber resilience and take both organizational and engineering/infrastructural cyber resilience into account [38]. In this section, cyber resilience abilities have been explored on a holistic level and the next section will synthesize the findings from the previous sections.

5 MARITIME CYBER RESILIENCE

The previous chapters have explored the terminology of “maritime operations”, “maritime cyber security” and “cyber resilience”. This section aims to synthesize the findings of the previous chapters, presenting a working definition for “maritime cyber resilience”.

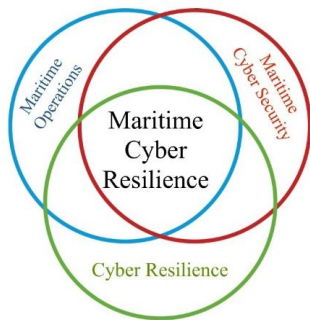


Figure 1. Origins of Maritime Cyber Resilience

We have seen that a maritime operation in its most general sense must be understood as human activities to achieve something at sea and that a resilient organization is one that does not lose control and is able to continue, recover and learn. A resilient maritime operation must then be an activity at sea conducted by an organization that does not lose control of the activity and is able to continue and recover the activity in the face of challenges. As we have seen and will illustrate further later in the paper, navigation is an important part of these activities, so the resilient organization must in this case be able to continue and recover its ability to navigate. What can be threatening the maritime domain today are the potential cyber threats, which put both the vessel and the crew on board at risk. The usual way to address this issue is by highlighting maritime cyber security, which is here understood as the protection from cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. We have also seen that cyber resilience should be a part of the risk mitigation process, as the traditional models for risk mitigation might not cover the emerging cyber threats in the maritime domain. The bridge on board a ship is a complex maritime sociotechnical system, which needs to consider both human and technical aspects, as one

cannot exist without the other (for now). Furthermore, “maritime cyber resilience” will be defined as a nautical system’s ability to learn how to maintain and evolve a normal operation, as well as anticipate, withstand, recover and evolve from a cyber threat, in the minimum amount of time possible.

By investigating the concept of maritime cyber resilience, it seems that term is meaningless without consideration of the human aspect, which in this paper refers to the navigator. This will be further considered in the next section, which will argue why the human is important in maritime cyber resilience.

6 THE IMPORTANCE OF THE NAVIGATOR

In this section, we will describe how a cyber threat situation is different from a commonly known emergency, and further emphasize why the human is important in the handling of an emergency.

The complexity of sociotechnical systems can make the procedures of operational situations underspecified, and the designers of such systems cannot anticipate everything in advance. Johnsen [35] argues that functions cannot be seen as a bimodal (functioning or not functioning), as seen in [20] where the ECDIS was gradually compromised, giving no alarms even when the system was hacked. A cyber-attack does not need to be immediate and visible; it can be lurking in the background without any warning of its occurrence. The navigator needs to be prepared to be surprised [35], which means that unexpected situations should be assumed to occur at any given time. According to Johnsen [35] a key resilience principle is “Reduction in Complexity”, which contradicts with the concept of INS [30] and the increasing complexity of navigational technology [48], which increase the risk of losing control. The purpose of an INS is to make every navigational tool readily available when the navigator needs it. This may affect the concept of maritime cyber resilience, especially if the navigator is not alert.

There is an unthinkable number of different crisis scenarios which can occur on a vessel; however, an easily approachable and very plausible example is fire detected on board in the engine room department of the vessel. IMO provides regulations in SOLAS, stating how onboard equipment should be made fire-safe and preventing fire from occurring and spreading. This makes the ship and its system more robust, as the fire should not easily emerge if every component is designed to be fire safe. It is a common fact that wear and tear happen to equipment, as well as an engine room is a place where work is conducted with tools, fuel and lubricating oils and rags in narrow and high-temperature compartments. This can increase the risk of fire, even if the components are designed to be fire safe in the first place. Aiding to mitigate the risk of fire, every modern ship is fitted with fire detecting and firefighting equipment, as regulated by IMO in SOLAS. This increase the navigator’s resilience ability of anticipating, as the firefighting system provides early detection of known characteristics of fire, such as temperature, smoke, or gas. This aids the navigator responsible for the

firefighting- and detection equipment on board to investigate an alarm more closely. The firefighting itself is related to the capacity of withstanding, as the operation must continue, and the navigator must fight the (potential) fire on board. The navigator is at the sharp end of the operation and needs to handle crisis as they emerge.

However, if the risk has become a reality and the normal situation have turned into a crisis, it is up to the planning, handling and response of the crew to get control over the fire which have occurred, using the predefined emergency procedures for fire, as well as improvisational "know-how" from the vessel's crew. We are now in the recovery part of resilience, where the navigator must determine damages and restore the vessel's capabilities. The goal is of course getting the vessel back to normal operation, as soon as possible. Time is, without doubt, a crucial factor in such a crisis, which means this is an important factor of the resilience abilities combined [23]. If the fire is put out, the crew enters the evolving state, debriefing the situation and learning from the incident and how to avoid the situation from emerging again. This also urges re-architecture of either technical barriers, policies, and procedures.

Resilience can relate to the ability to put things together after they have fallen apart [56]. Most crisis which can occur on board a vessel is expected to be described in the Emergency Manual, and the crew is expected to be regularly drilled and tested in these crisis scenarios, where everyone has a dedicated role. The role of the navigator is often a decision maker, as i.e. the captain is responsible for deciding if, and when, the fixed firefighting system in the engine room is to be released, as this system (depending on the onboard solution) also may have the capacity to kill a person being in the engine room at the time of the release of the gas. The Chief Mate is normally responsible for leading the deck crew in firefighting, making quick and effective plans, having control of persons on board, as well as who is not accounted for, and send the crew who are designated as smoke divers and firefighters to find any missing persons. The crisis of fire on board a vessel, as well as all the other "well-known" crisis a vessel can find itself in, are usually tangible and to one extent comprehensible to the decision makers on board. Cyber-attacks, in contrast to a fire, may not be as tangible and visible, and are not yet addressed in standardized training of the seafarers [25], such as the emergency of a on board fire is.

Considering the resilience abilities of anticipate, withstand, and recover, it could be difficult for a navigator to maintain these abilities, who never have encountered, or even heard of, a cyber threat. This is what makes the factor of evolving and learning important, as the threat is being recognized in the maritime industry. That again urges the re-architecting of systems and procedures and transforming of processes and behavior. Depending on the operation that is undertaken, the implementation will of course vary. The consequences of not having a high-precision position are different for a crude-oil tanker in the middle of the Pacific Ocean sailing with low to medium speed, compared to a high-speed passenger vessel sailing along the

shores of Norway. Still, both vessels must undertake the process of changing in the face of the prominent threats of today, in order to be able to maintain safe operation and navigation.

Hollnagel describes an organization going through "states" in an event of an emergency, and that it is vital for the organization to know what the current state (i.e. normal operation) is and know when that state is changing. This may be hard with a cyber threat, as what can seem to be a normal situation actually is a disturbed operation state, depending on the cyber threat. A system can be claimed to have three states; stopped, idle and running. If a system finds itself in a matter of emergency, the system needs first to go to an "idle" state, to be able to return to "normal state" [23]. This can also be applied to a vessel. In an example where the navigator loses the control of steering from the autopilot, the navigator needs to take an active choice to steer the vessel manually, to maintain normal operation. This taken into consideration, the navigator needs to know he is in an emergency state. Lund [39] exemplifies that a cyber emergency onboard a vessel might not be as imminent and visible as one might think. This urges the navigator to be the most important cross check sensor on-board [19].

Recovery is often a result of a function of the scale of damage and frequency of the type of the crisis [56]. This can be one of the reasons the emergency response plans are standardized, addressing previously known problems which can occur on a vessel. Fire on board is addressed because of earlier ship emergencies and have thus received attention in the regulations for safe and secure shipping. As discussed above, being resilient is about evolving and adapting to the challenges at hand. The shipowners today need to be resilient in their approach to cyber threats, and not have a passive attitude, hoping to avoid being struck by a cyber-attack.

This section has now discussed an "normal" and very well-known emergency which can occur on board a vessel. A fire onboard is a very visible, tangible and "easy-to-visualize" kind of crisis. A cyber crisis can be described as the exact opposite of that. A cyber crisis may not be tangible, not easy to comprehend and not easy to visualize, especially if the persons who are responsible for handling the crisis have not encountered a cyber incident before. This is also why evolving of the human is important when considering maritime cyber resilience, as the human is capable of adjusting to the situation, whereas emphasizing the good qualities of a "normal operation" and applying resilience principles to the everyday work.

6. CONCLUSION

In this article, the authors have argued for the lack of a definition of the term "Maritime Cyber Resilience" and aimed at providing a working definition for future research.

What is an emerging problem today is the cyber threats and risks towards nautical operations. Maritime cyber security concerns the protection from

cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. In order to apply resilient attributes to the nautical operations, the people undertaking such operations must be able to protect the ongoing operations from a potential cyber threats and risks, as well as constantly expect the unexpected, evolving and learning from own operations.

“Maritime Cyber Resilience” has been defined as a nautical system’s ability to learn how to maintain and evolve a normal operation, as well as anticipate, withstand, recover and evolve from a cyber threat in the minimum amount of time possible. The authors have also argued for why the navigator should be the focus of study when considering maritime cyber resilience, as the navigator is at the sharp edge of the operation, maybe being the only agent able of detecting an unwanted variation to a situation. Furthermore, the navigator is expected to take the wheel when the technology fails. One assumption when considering maritime cyber resilience is that the navigator needs to accept that the safety of the situation can, and eventually will be, compromised.

This article has discussed that robust systems can fail, and even technical resilient systems can fail. In this case, the navigator, who is a major decision maker onboard needs to take command to take control over the situation. The article mentions that there are many types of cyber-attacks and many of them are not yet known. A cyber-attack can be lurking in the system, not to cause any trouble, before a given time or position. This means that the navigator and the human aspect is key, when considering Maritime Cyber Resilience.

ACKNOWLEDGEMENT

This paper is part of the research project MarCy (Maritime Cyber Resilience). The MarCy project has received funding from the Research Council of Norway, with project number 295077. Contents reflects only the authors’ views, and the Research Council of Norway, nor the project partners, are not responsible for any use may be made of the information it contains.

REFERENCES

1. Anholt, R., Boersma, F.K.: From security to resilience: New vistas for international responses to protracted crises. In: Linkov, I., Florin, M.-V., and Trump, B.D. (eds.) *Resilience (Volume 2, 2018)*. pp. 25–32 International Risk Governance Center (2018). <https://doi.org/10.5075/epfl-irgc-262527>.
2. Awan, M.S., Al Ghamdi, M.A.: Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). *Journal of Marine Science and Engineering*. 7, 10, (2019). <https://doi.org/10.3390/jmse7100350>.
3. Bainbridge, L.: Ironies of automation. *Automatica*. 19, 6, 775–779 (1983). [https://doi.org/10.1016/0005-1098\(83\)90046-8](https://doi.org/10.1016/0005-1098(83)90046-8).
4. Barrett, M.: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, <https://doi.org/10.6028/NIST.CSWP.04162018>, (2018).
5. Bimco, Cia, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council: The

Guidelines on Cyber Security onboard Ships. BIMCO (ed.) Version 4.0 (2020).

6. Bodeau, D.J., Graubart, R.D., Picciotto, J., McQuaid, R.: *Cyber Resiliency Engineering Framework*. The MITRE Corporation (2011).
7. Bowditch, N.: *The American practical navigator: an epitome of navigation*. National Imagery and Mapping Agency (2002).
8. Boyes, H., Isbell, R.: *Code of Practice: Cyber Security for Ships*. Institution of Engineering and Technology, London, United Kingdom (2017).
9. Cambridge Online Dictionary: Maritime. Cambridge University Press (2021).
10. Cambridge Online Dictionary: Operation. Cambridge University Press (2021).
11. da Conceição, V.P., Dahlman, J., Navarro, A.: What is maritime navigation? Unfolding the complexity of a Sociotechnical System. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*. 61, 1, 267–271 (2017). <https://doi.org/10.1177/1541931213601549>.
12. Cutler, T.J.: *Dutton’s Nautical Navigation*. Naval Institute Press; (2004).
13. Daum, O.: Cyber Security in the Maritime Sector. *J. Mar. L. & Com.* 50, 1–19 (2019).
14. DiRenzo, J., Goward, D.A., Roberts, F.S.: The little-known challenge of maritime cyber security. In: 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA). pp. 1–5 (2015). <https://doi.org/10.1109/IISA.2015.7388071>.
15. DNV: Cyber security resilience management for ships and mobile offshore units in operation, <https://www.dnv.com/maritime/dnvg1-rp-0496-recommended-practice-cyber-security-download.html>, last accessed 2021/04/15.
16. Fitton, O., Prince, D., Germond, B., Lacy, M.: *The future of maritime cyber security*. Lancaster University (2015).
17. Giacomello, G., Pescaroli, G.: *Managing Human Factors*. In: Kott, A. and Linkov, I. (eds.) *Cyber Resilience of Systems and Networks*. pp. 247–263 Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-77492-3_11.
18. Haimes, Y.Y.: On the Definition of Resilience in Systems. *Risk Analysis*. 29, 4, 498–501 (2009). <https://doi.org/10.1111/j.1539-6924.2009.01216.x>.
19. Hareide, O.S.: Podkast: Teknologi og mennesket som “sensor,” <https://www.kystverket.no/Nyheter/2021/januar/ny-podkast-teknologi-og-mennesket-som-sensor/>, last accessed 2021/04/16.
20. Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K.: Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*. 71, 5, 1025–1039 (2018). <https://doi.org/10.1017/S0373463318000164>.
21. Hollnagel, E.: Resilience engineering and the built environment. *null*. 42, 2, 221–228 (2014). <https://doi.org/10.1080/09613218.2014.862607>.
22. Hollnagel, E., Pariès, J., Woods, D., Wreathall, J.: Epilogue: RAG – The Resilience Analysis Grid. In: *Resilience Engineering in Practice*. pp. 275–296 CRC Press, London, United Kingdom (2011). <https://doi.org/10.1201/9781317065265-19>.
23. Hollnagel, E., Woods, D.D., Leveson, N.: *Resilience Engineering: Concepts and Precepts*. CRC Press (2006).
24. Hollnagel, Erik: How resilient is your organisation? In: *An Introduction to the Resilience Analysis Grid (RAG)*. Toronto, Canada (2010).
25. Hopcraft, R., Martin, K.M.: Effective maritime cybersecurity regulation – the case for a cyber code. *null*. 14, 3, 354–366 (2018). <https://doi.org/10.1080/19480881.2018.1519056>.
26. IACS: Rec 166 - Recommendation on Cyber Resilience, <http://www.iacs.org.uk/publications/recommendations/161-180/>, last accessed 2021/04/15.

27. Inmarsat: Best Practice Information and Communications Technology (ICT) Recommendations, <https://www.inmarsat.com/en/insights/maritime/2019/best-practice-ict-guide.html>, last accessed 2021/04/15.
28. International Maritime Organization: Maritime cyber risk, <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>, last accessed 2021/04/15.
29. International Maritime Organization: MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management, <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>, last accessed 2021/04/15.
30. International Maritime Organization: Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS).
31. International Maritime Organization: Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>, last accessed 2021/04/15.
32. ISO: ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, <https://www.iso.org/standard/54533.html>, last accessed 2021/04/15.
33. ITU: ITU-Tx. 1205. Interfaces. 10, 20–X, 49 (2008).
34. Jensen, L.: Challenges in Maritime Cyber-Resilience. *Technology Innovation Management Review*. 5, 4, 35–39 (2015). <https://doi.org/10.22215/timreview/889>.
35. Johnsen, S.: Resilience in Risk Analysis and Risk Assessment. In: Moore, T. and Shenoi, S. (eds.) *Critical Infrastructure Protection IV*. pp. 215–227 Springer Berlin Heidelberg, Berlin, Heidelberg (2010).
36. Karahalios, H.: Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. *Journal of Transportation Security*. 13, 3, 179–201 (2020). <https://doi.org/10.1007/s12198-020-00223-1>.
37. KVH Intelsat: Crew Connectivity 2018 Survey Report, <http://www.crewconnectivity.com/?product=2018-crew-connectivity-survey-report>, last accessed 2021/04/15.
38. Linkov, I., Kott, A.: Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A. and Linkov, I. (eds.) *Cyber Resilience of Systems and Networks*. pp. 1–25 Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-77492-3_1.
39. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An Attack on an Integrated Navigation System. *Nesse*. 3, 2, 149–163 (2018). <https://doi.org/10.21339/2464-353x.3.2.149>.
40. Madni, A.M., Jackson, S.: Towards a conceptual framework for resilience engineering. *IEEE Engineering Management Review*. 39, 4, 85–102 (2011). <https://doi.org/10.1109/EMR.2011.6093891>.
41. Markit, I.: Safety at Sea and BIMCO cyber security white paper, <https://ihsmarkit.com/Info/0819/cyber-security-survey.html>, last accessed 2021/04/15.
42. Martin-Breen, P., Anderies, J.M.: Resilience: A literature review, <https://opendocs.ids.ac.uk/opendocs/handle/20.500.1241/3/3692>, last accessed 2021/04/15.
43. McGillivray, P.: Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed. *Marine Technology Society Journal*. 52, 5, 44–57 (2018). <https://doi.org/doi:10.4031/MTSJ.52.5.11>.
44. Mileski, J., Clott, C., Galvao, C.B.: Cyberattacks on ships: a wicked problem approach. *Maritime Business Review*. 3, 4, 414–430 (2018). <https://doi.org/10.1108/MABR-08-2018-0026>.
45. Ng, D.: Safety first: maritime cyber security, IMO guidelines and the maritime supply chain. *Riviera Maritime Media* (2021).
46. NTNU: Literature review of “Maritime Cyber Resilience,” https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/search?query=any,contains,%22maritime%20cyber%20resilience%22&tab=default_tab&search_scope=default_scope&vid=NTNU_UB&offset=0, last accessed 2021/04/15.
47. Refsdal, A., Solhaug, B., Stolen, K.: *Cyber-Risk Management*. Springer International Publishing (2015). <https://doi.org/10.1007/978-3-319-23570-7>.
48. Relling, T., Lützhöft, M., Ostnes, R., Hildre, H.P.: A Human Perspective on Maritime Autonomy. In: Schmorow, D.D. and Fidopastis, C.M. (eds.) *Augmented Cognition: Users and Contexts*. pp. 350–362 Springer International Publishing, Cham (2018).
49. SAGE Journals: Literature review of “Maritime Cyber Resilience,” <https://journals.sagepub.com/action/doSearch?filterOption=allJournal&AllField=%22maritime+cyber+resilience%22>, last accessed 2021/04/15.
50. von Solms, R., van Niekerk, J.: From information security to cyber security. *Computers & Security*. 38, 97–102 (2013). <https://doi.org/10.1016/j.cose.2013.04.004>.
51. Springer: Literature review of “Maritime Cyber Resilience,” <https://link.springer.com/search?query=%22maritime+cyber+resilience%22>, last accessed 2021/04/15.
52. Svilicic, B., Brčić, D., Žuškin, S., Kalebić, D.: Raising Awareness on Cyber Security of ECDIS. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*. 13, 1, 231–236 (2019). <https://doi.org/10.12716/1001.13.01.24>.
53. Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: Maritime Cyber Risk Management: An Experimental Ship Assessment. *Journal of Navigation*. 72, 5, 1108–1120 (2019). <https://doi.org/10.1017/S0373463318001157>.
54. Svilicic, B., Rudan, I., Jugović, A., Zec, D.: A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. *Journal of Marine Science and Engineering*. 7, 10, (2019). <https://doi.org/10.3390/jmse7100364>.
55. TransNav.eu: Literature review of “Maritime Cyber Resilience,” https://www.transnav.eu/Search_maritime%20cyber%20resilience.html, last accessed 2021/04/15.
56. Westrum, R.: A Typology of Resilience Situations. In: Hollnagel, E., Woods, D.D., and Leveson, N. (eds.) *Resilience Engineering: Concepts and Precepts*. pp. 55–65 CRC Press, London, United Kingdom (2006). <https://doi.org/10.1201/9781315605685-8>.
57. Whitman, M.E., Mattord, H.J.: *Principles of Information Security*. Cengage Learning (2017).
58. Woltjer, R.: Deliverable D1.1 Consolidation of resilience concepts and practices for crisis management, <https://h2020darwin.eu/project-deliverables/>, last accessed 2021/04/15.

Paper II

Navigating through cyber threats, a maritime navigator's experience

Navigating Through Cyber Threats, A Maritime Navigator's Experience

Erlend Erstad¹, Mass Soldal Lund^{2,3}, and Runar Ostnes¹

¹Norwegian University of Science and Technology, Ålesund, Norway

²Inland Norway University of Applied Sciences, Rena, Norway

³Norwegian Defence University College, Lillehammer, Norway

ABSTRACT

Cyber threats are emerging as a risk in the maritime industry. If the navigational systems on board a ship somehow fail to function because of a cyber incident, the navigator is an important asset who is expected to handle the problem and provide a solution to maintain the safety of the crew, the vessel, and the environment. The International Maritime Organization (IMO) urges the shipping industry to be resilient towards cyber threats. To facilitate for enhanced operational maritime cyber resilience, there is a need to understand how navigators interpret cyber threats, which can be essential to safely conduct nautical operations. This paper presents a qualitative study of navigators' understanding of cyber threats based on interviews with ten navigators, and further provides recommendations for how use of this knowledge can contribute to enhanced maritime cyber resilience.

Keywords: Maritime cyber resilience, Maritime cyber security, Cyber threat, Cyber crisis, Cyber-attack

INTRODUCTION

The increasing connectivity and technological development in the maritime industry is making the industry more efficient and provides great business benefits, but also introduces cyber threats which can endanger maritime digital control systems (Ben Farah et al., 2022). Maritime navigators use such control systems to determine the position of the ship, to keep clear of hazardous waters and avoid dangerous situations. Correct navigation is thus necessary for the ship's safety, and the navigator is at the sharp end of the operation (Erstad et al., 2021). Modern navigation is performed swiftly and automatically using an Electronic Chart Display and Information System (ECDIS), instead of paper charts. The ECDIS gets real-time position input from Global Navigation Satellite System (GNSS), such as GPS, providing the navigator with instantaneous position fix for the ship. It is therefore vital for the navigator to maintain system awareness and understand the potential threats towards the systems being used. A cyber threat exploits cyberspace, which can lead to a cyber incident (Refsdal et al., 2015). One potential cyber incident can be falsified position input to the ECDIS, potentially sending the ship into unknown waters. The maritime digital control systems are vulnerable to cyber-attacks if not protected (Kessler and Shepard, 2020), and

the number of cyber incidents towards the maritime industry is increasing (Meland et al., 2021).

Learning and evolving are important aspects of operational maritime cyber resilience, and a proactive approach is vital to succeed. Cyber-security awareness is key for enhanced protection against cyber threats (Ben Farah et al., 2022), and training for such awareness is important (Tam and Jones, 2019). To provide purposeful training for navigators, and aid maritime stakeholders for mitigating cyber risks, there is a need to understand how navigators experience and interpret cyber threats. Human-Centred Design (HCD) (ISO, 2019) has proven beneficial when developing a solution to a user problem, for example training programs to navigators. A key element in HCD is to involve the user in the process of designing the solution to the problem at hand (ISO, 2019). To ensure such user involvement, a qualitative study of interviews with navigators was conducted.

This article aims to serve as an insight paper on how a selection of Norwegian navigators interpret maritime cyber threats. This paper is limited to the operational aspect of maritime cyber resilience, not investigating any technical aspects. The interviews will contribute to the HCD-process for developing maritime cyber training and awareness simulator scenarios. Ten Norwegian navigators have been interviewed, and the interviews were analyzed using Systematic Text Condensation method (STC), which is founded in psychological phenomenology (Malterud, 2012). An important prerequisite in phenomenological analysis is that all participants have experienced the same phenomenon (Creswell and Poth, 2018), and this article investigates how navigators experience cyber threats. The participants were chosen as all had experience and knowledge of cyber threats, and all participants are navigators holding a deck certificate, actively sailing or not, still working in the maritime industry.

FINDINGS

Categorization of the themes which were conversed in the interview aids to describe the navigators' interpretation of cyber threats in a structured way. Similar statements and expressions were grouped and organized, which formed the foundation for five different categories of themes, as shown in Table 1. The sub-categories are nuances of the categories, highlighting how the interviewees talked about the different aspects of the categories. The findings also present authentic illustrative quotation (AIQ) (Malterud, 2012), which has the intention to give the reader a sense of understanding how the interviewer interpreted the interview. An AIQ are not necessarily a direct citation of what the interviewees said, but a descriptive synthesized quotation, aiming to grasp the essence of interviewees meaning.

Further, a summary of each category will be presented, as well as an AIQ for each category.

The Digital Era

The interviewees appreciate the opportunities the technology offers, as it saves a lot of time, for example with chart updates. Previously, chart updates

Table 1. Categories and sub-categories.

Category	Sub-category
The digital era	Trust in technology
What is actually a cyber threat?	The un-hackable and indispensable RADAR
	The intangible term of “Cyber threat”
	Intentional vs unintentional
Improvised coping strategies towards cyber threats	Satellite navigation related issues
	Ad hoc improvising
The unaddressed cyber issue	Unwritten rules
	Lack of awareness and training
	Lack of policies, procedures, and regulatory standards
	“Old school” vs “new school”
The complex nature of consequences	Causes and consequences
	Capacity of functions
	“It depends”

were manual work in paper charts. Today it is often performed by putting an USB-memory stick into the system and uploading all the relevant data to the electronical charts. However, when talking to the interviewees, it felt like they meant that the common navigator trusts the technology too much, uncritical of potential cyber threats, for example by using an infected and unsafe USB-stick for update. On the other hand, most of the candidates concluded that if the ECDIS was compromised, at least they had confidence in that the ships radar could not be hacked. However, an interviewee reflected that the radar also is operated by a computer, sometimes interconnected with the ECDIS.

AIQ: As I told you previously, we have become very dependent on the easy form of navigation. I feel the technology today is so great that I can do other tasks in addition to navigating. If we lose our GPS system, we must slow down, and the situation could turn into a challenge. But then again, we have the radar, which always is correct. It cannot be hacked, can it?

What is Actually a Cyber Threat?

The interviewees had some struggles to define what a cyber threat is. Some reflected that it could be the same as a technical error, as they did not see the difference if the consequences were the same for a cyber-attack and a technical error. All interviewees had experienced cyber threats, however, all interviewees had somewhat different explanations of what a cyber threat and a cyber-attack is. A cyber threat, according to the interviewees, could have many different forms, characteristics, and consequences. Some of the interviewees highlighted the importance of the operational technology, such as the navigation systems, and others mentioned the importance of the information technology, such as email and administration systems. Jamming and spoofing of satellite navigation systems is well known among the interviewees. It is a part of the simulated ECDIS-training for seafarers. There was also consensus

of that there is a difference between targeted or intentional cyber-attacks, and random or unintentional cyber-attacks.

AIQ: A GPS problem is just as normal as navigating in fog. It is harder, but operation keeps on going. However, cyber-attacks can be directed to you personally, or to everyone, such as your grandparents. Everybody has received a billion dollars lottery email from a shady email address. Considering as something as strange as a cyber-attack ... I don't know ... there is so many weird things now, as ransomware. What is actually ransomware?

Improvised Coping Strategies Towards Cyber Threats

Seafarers have traditionally taken care of problems on their own, as ships are mostly sailing on the ocean, out of reach for service technicians or external help. This means, if a problem occurs on board, it must normally be handled by the crew. If it is a broken pump which needs fixing or replacing, or a stow-away is discovered, both “problems” needs immediate attention and action. Seafarers are therefore creative and adapts to the situations as they emerge.

AIQ: We don't have any procedures for preventing cyber-attacks. We have a this is how we do it on board-kind of thing. For example, we only use the ECDIS-USB-stick for the chart updates, that is not the problem. If we were victim to a cyber-attack, we would have found a solution, I am certain of it. I don't think a cyber-attack would have affected the safety, but to keep the ship operational could have been a problem.

The Unaddressed Cyber Issue

All interviewees reported little to no education or formalized training considering cyber threats. However, the interviewees acknowledged the emerging cyber problem, as they hear of cyber incidents in the media and from colleagues in the industry. The interviewees also mention the difference in age between seafarers. Maybe the more experienced navigators are not the best to adapt to new computer systems, but the young navigators would have encountered problems if some equipment should not function properly. The interviewees experience the cyber threat issue as not properly addressed by the educational institutions, and only started recently to get proper attention by the shipping companies. It is highlighted that the maritime industry is a profit driven industry, and some interviewees believe that nothing will happen of any significance, until it is properly addressed by the regulatory organizations. The lack of policies, training and regulatory standards are reflected in how seafarers today uncritically use the vessels computer and control systems. Even though some computers are dedicated for a purpose, for example as ECDIS workstations, seafarers find a way to use it for other things, as watching TV or playing solitaire. Seafarers does not consider this as a problem, as cyber threats are not properly addressed.

AIQ: Our schoolbook was written in 1956. We have had practically no education regarding maritime cyber security. Sailing a ship have changed from navigating a vessel to operating a computer. Shipping is a stingy

industry by tradition, and shipowners does not spend more money than necessary. If cyber security is not required by law, it is most likely not implemented. I don't think we have any cyber policies or procedures, maybe it is mentioned somewhere in the system.

The Complex Nature of Consequences

When talking about cyber threats, the respondents reflected considerably on the possible consequences and what equipment could be affected. Navigation aiding systems are often mentioned in the conversations, and these operational systems are seen as critical equipment for the navigators. Visible faults, as “blue screen of death”, is seen as less severe, than faults gradually degrading the navigation systems. It is easier to detect a sudden loss of position, than a small drift in the ships position. All interviewees agreed that capacity and functionality of equipment was important for them as deck officers, however, there is questions raised regarding how and why the potential hackers could affect the operational systems. The interviewees are also reflecting on the underlying causes for the cyber threats, as the causation is not quite clear. A cyber-attack clearly is mentioned to have consequences for the operation, mostly seen as a cause for collateral damage to charterers and a threat to the economical perspectives of the maritime supply chain. The consequence of a cyber threat affecting an operation is described as “it depends”, meaning the consequences is dependent on the situation the vessel finds itself in. A cyber threat itself may be harmless, but on top of dense traffic, heavy seas and bad weather, things can go differently.

AIQ: These cyber-attacks, I don't know how they do it, or why they should attack us. But I guess the risk of getting infected is big. A dangerous situation will be you losing the integrity of the navigation system, without being aware of it. As an invisible fault, which you do not know is there before it is too late. No matter what happens on board, in the end it is all about if it affects the economy or not. Cyber incidents could cause some serious consequential errors for the charterers and other ships after us. The size of the ship, the weather, the waves, the level of automation, the location, the traffic are just some of the factors that will threaten a situation. Will a cyber-attack become a problem? Well, it depends...

DISCUSSION

Ships are becoming increasingly technological and complex, and even remote operated ships and autonomous ships are being built and tested today. Navigators have changed from actively navigating agents to passive operative agents (Lützhöft et al., 2011). This corresponds with the findings the interviewees are describing in “the digital era”. Previously, navigators relied on several instruments and calculations to find the position of the vessel in the paper chart. Today, the game has changed, and the navigators rely on single systems to determine position, such as GNSS (Hareide et al., 2018). Because of ships’ complexity and interconnectivity, single errors in a digital control system can affect other systems on board, for example integrated navigations

systems. Bearing in mind the category of “the complex nature of consequences”, the interviewees are highlighting the potential damage to the maritime supply chain. In a situation where a ship is undertaking an oceanic voyage and navigation system is compromised, displaying false information, without the navigator noticing it, the ship will eventually end up in the wrong place. A ship ending up the wrong position at the wrong time, can have several impacts on the logistics chain the ship is a part of, even the safety of the ship itself, if it is in hazardous waters. Being an active navigating agent can be difficult when operating highly automated systems in a supply chain with tight time schedules, as the ships often needs to deliver the goods or the service at the shortest time possible. However, navigators would be more resilient towards threats with increased system knowledge, which makes hands-on operating reasonable, even if the system is highly automated. Combined with cyber threat aspects in training and education, it could facilitate for increased maritime resilience.

Bainbridge (1983) points out that unknown situations cannot be simulated or trained for, and thus operators must be trained in general strategies to receive knowledge for responding to specific situations. The findings reveal that cyber threats are complex issues, yet simulated training, such as ECDIS jamming, is beneficial for awareness. Navigator competence can be increased by introducing cyber-attack scenarios to maritime training (Hareide et al., 2018), and simulator scenario training can facilitate for cyber security awareness (Tam et al., 2021). Simulator training as an integrated part of a training philosophy designed for enhanced resilience can have positive effects on operator skills (Wahl et al., 2020). Training in maritime simulators (i.e., ship simulators) is a major part of the practical education for navigators for developing nautical skills for maritime problem solving (IMO, 2017a).

In an HCD-perspective, the abovementioned talks in favor for tailoring practical training scenarios, where the importance of system knowledge (both technical and organizational) is emphasized. However, it is unethical to expose any kind of student for a threat that not yet have been taught to the student. To identify and train for threats should be the responsibility of the organization and the educational institutions, especially when the threat is known, such as cyber threats are today.

Despite today's navigation depends on a functioning ECDIS, all our respondents said that they were confident in the trustworthiness of the radar. If the radar can be subject to a cyber-attack or not, is out of scope for this paper. However, it was highlighted how hard it could be to “switch” the mode of navigation, from observing position of vessel and other vessels (passive agent) to fixing own vessel position and other vessels position (active agent). According to Bainbridge (1983), skills deteriorate over time when not used, and it is unreasonable expect navigators whom have been passively navigating for a long time, to instantly become an active navigating agent. This means cyber threats can affect normal operations. The interviewees emphasized that the cyber threat picture is dependent on the situation. Compromised navigation systems such as loss of chart system or vessel heading on board

a slow speed freight carrier will have different effects than high-speed crafts, navigating in narrow waters.

The maritime industry relies on rules and regulations to improve the safety, and can be claimed to be a reactive industry (Lützhöft et al., 2011). Cyber risks are now to be implemented as a part in the vessels safety and risk management systems, as acknowledged by IMO (IMO, 2017b), yet the maritime industry still lacks cyber situational awareness (Tam and Jones, 2019). This probably contributes to the category “the unaddressed cyber issue”, as the navigators are expected to consider and implement new risks and threats they do not understand in the ships safety management system.

Today, simulated jamming and spoofing is integrated as a part of ECDIS training (IMO, 2012), which is probably a reason why navigators have awareness of this type of threat. Jammed GNSS signals is closely related to loss of GNSS signals, which is a normal technical error on board. Maybe cyber threats have been unintentionally ignored, as there are no regulated education or training for seafarers. Considering HCD it is important to define the users requirement at an early stage (ISO, 2019). In order to design and produce training methods tailored to navigators where the aim is mitigation of cyber threats, the voice of the navigators should be heard.

CONCLUSION

The cyber threat is an emerging concern in the international maritime industry. This paper provides an insight of how a selection of navigators describe how they interpret the maritime cyber threat, and how they perceive the issue is treated by the maritime industry. The cyber threat issue is experienced as not properly addressed, despite the growing international interests for enhanced maritime cyber security and resilience. Problem solving for navigators at the sharp end of the operation are normally pragmatically handled. As it is stated in the findings, the navigators are creative and would have looked for the best solution. Utilizing HCD principles when designing for cyber awareness training and education should aid designers and facilitators of the training for the navigators. Understanding how navigators interprets cyber threats will be beneficial for the development of such training, as the understanding of the problem (i.e., cyber threat) is a specific deliverable in the HCD process. Cyber threat simulator training will better enable navigators to consider if the problem they are encountering is a cyber threat or not, at an early stage in problem solving process.

Training for unknown threats is seen as unreasonable. However, one can train for known threats, which stimulates for system awareness and ingenuity. Navigators have knowledge of jamming and spoofing threats, as it is implemented as part of the ECDIS training, and the problem is considered as normal disturbance. Simulator training in maritime education is already an acknowledged method for practical problem solving and learning. Therefore, it is reasonable to implement specific training for known cyber threats and situations in a safe simulator environment, aiming to enhance navigators' operational maritime cyber resilience.

ACKNOWLEDGMENT

This paper is part of the project called Maritime Cyber Resilience (MarCy), which has received funding from the Research Council of Norway, with project number 295077. All participants gave written consent to participate in the interview process.

REFERENCES

- Bainbridge, L. 1983. Ironies of automation. *Analysis, design and evaluation of man-machine systems*. Elsevier.
- Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. & Bellekens, X. 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information*, 13, 22.
- Creswell, J. W. & Poth, C. N. 2018. *Qualitative inquiry & research design : choosing among five approaches*, Thousand Oaks, Calif, Sage.
- Erstad, E., Ostnes, R. & Lund, M. S. 2021. An Operational Approach to Maritime Cyber Resilience. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15, 27–34.
- Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R. & Helkala, K. 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, 71, 1025–1039.
- IMO, I. M. O. 2012. Operational Use of Electronic Chart Display and Information Systems (ECDIS). *Model Course 1.27 (2012 Edition)*. London.
- IMO, I. M. O. 2017a. *International Convention on standards of Training and Watchkeeping for Seafarers (STCW) 1978, consolidated edition 2017*.
- IMO, I. M. O. 2017b. Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems.
- ISO, I. 2019. 9241-210: 2019 Ergonomics of human-system interaction. *Part 210: Human-Centred Design for Interactive Systems*.
- Kessler, G. C. & Shepard, S. D. 2020. *Maritime Cybersecurity: A Guide for Leaders and Managers*, Daytona Beach, Kessler & Shepard.
- Lützhöft, M., Grech, M. R. & Porathe, T. 2011. Information Environment, Fatigue, and Culture in the Maritime Domain. *Reviews of Human Factors and Ergonomics*, 7, 280–322.
- Malterud, K. 2012. Systematic text condensation: A strategy for qualitative analysis. *Scand J Public Health*, 40, 795–805.
- Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø. & Nesheim, D. 2021. A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*.
- Refsdal, A., Solhaug, B. & Stølen, K. 2015. Cyber-risk management. *Cyber-Risk Management*. Springer.
- Tam, K. & Jones, K. 2019. Situational awareness: Examining factors that affect cyber-risks in the maritime sector.
- Tam, K., Moara-Nkwe, K. & Jones, K. 2021. The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research*, 3.
- Wahl, A., Kongsvik, T. & Antonsen, S. 2020. Balancing Safety I and Safety II: Learning to manage performance variability at sea using simulator-based training. *Reliability Engineering & System Safety*, 195, 106698.

Paper III

A human-centred design approach for the development and conducting of maritime cyber resilience training



A human-centred design approach for the development and conducting of maritime cyber resilience training

Erlend Erstad¹ · Rory Hopcraft² · Avanthika Vineetha Harish² · Kimberly Tam²

Received: 12 December 2022 / Accepted: 14 February 2023
© The Author(s) 2023

Abstract

Due to the increase in the digitalization on board ships, the potential consequences of a cyber-induced incident can threaten the safety of the ships. A known challenge in the maritime industry is communication between ship owner management onshore and the crew on board a ship, especially during incident handling. To mitigate this issue and enhance cooperation in the digital age, crew and ship owner management need to meet, train for, and discuss cyber risks and their challenges. One way to enhance cohesive teams and effective communication is through the application of a human-centred design (HCD) approach to holistic team training. This paper proposes how simulator instructors should utilise HCD for the development of maritime cyber resilience training, tailored to a variety of maritime stakeholders including ship's crew and onshore support personnel. To do this, this paper will explore relevant learning theories and current maritime and cyber-related training methods. The paper will then demonstrate, through a practical application, the effectiveness of adopting HCD when designing maritime cyber resilience training. This application will argue that maritime simulators present an effective training solution for new cyber-related incidents. The authors demonstrate the application of HCD by showcasing a ballast water handling system cyber incident designed for the simulator. The development of such a training resource allows all participants to experience the consequences of a cyber-attack in a safe environment whilst enhancing their ability to respond (i.e. communicate with each other) effectively.

Keywords Maritime cyber risk management · Maritime cyber resilience · Human-centred design · Maritime simulator · Maritime cyber security

✉ Erlend Erstad
erlend.erstad@ntnu.no

¹ Department of Ocean Operations and Civil Engineering, Norwegian University of Science and Technology, Ålesund, Norway

² Faculty of Science & Engineering, University of Plymouth, Plymouth, UK

1 Introduction

The maritime industry has seen a large increase in digital technology being implemented into everyday nautical operations. As a result of this digitalisation, many nautical operations, such as navigation and sailing, have transformed from manual operations to auto-assisted operations, where the seafarer primarily monitors the vessel control systems to ensure they function properly (Erstad et al. 2021). However, this increase in technology also increases the cyber risk to the vessel, leaving navigation and control systems vulnerable to cyber-attacks, as demonstrated by Tam et al. (2021a) and Lund et al. (2018). These demonstrate that, if a cyber incident were to occur during operations, the crew would be expected to take an active role in responding to these incidents. A cyber incident is in this paper addressed as the consequence of an effective cyber risk. A cyber risk is a risk caused by a cyber threat and can be both malicious (adversary intended) and non-malicious (unintended or accidental). The risk, and thus the incident, does not relate to faults in cyber systems where cyber risk is not a contributing factor, such as fault in a cyber system (i.e. computers and network) caused by flooding or fire (Refsdal et al. 2015, page 33).

The maritime sector is however lagging behind other sectors, like aviation, in terms of cyber risk management (Hopcraft and Martin 2018), as well as cyber security training (Stoker et al. 2022). In 2017, the International Maritime Organisation (IMO) released Resolution MSC.428(98), which obligates organisations to consider cyber risk management within their safety management systems (SMS). The SMS is a requirement of the International Safety Management (ISM) Code (IMO 2017b). As part of the ISM Code requirements, companies are expected to provide training for their crews to ensure that they are equipped with the knowledge and skills to manage safety risks effectively (IMO 2018). However, cyber security is not explicitly mentioned in the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) (IMO 2016). STCW sets out the international baseline curriculum for maritime ship crew, through the use of standardised competencies every seafarer must demonstrate before obtaining certificates. Thus, there is currently no standardised skill or knowledge requirements relating to cyber risk management (Heering et al. 2021).

As IMO (2017b) urges shipping organisations to be resilient towards cyber risks, maritime cyber resilience originates as one of the components of maritime cyber risk management. Evolving is a central part of maritime cyber resilience (Erstad et al. 2021), and therefore maritime cyber resilience training will be a vital component in enhancing overall maritime cyber risk management knowledge. To ensure that crews are well prepared to handle cyber incidents, there is a need to enhance training, communication, and coordination to be considerate of these digital threats (Hopcraft 2021; Erstad et al. 2022a; Larsen et al. 2022).

This paper will apply a human-centred design (HCD) approach to the design of maritime cyber resilience training, by demonstrating how to develop and conduct a maritime cyber incident scenario as a training tool. The output is primarily intended for Maritime Training and Education Institutions (METI), but maritime

organisations could utilise the process for developing their own company-specific training. Demonstrating how companies can tackle the complex challenge of upskilling crews to respond to operational cyber incidents will enhance the cyber resilience skills of the people who work in the maritime sector, increasing overall security. Personnel equipped with maritime cyber resilience skills will also be empowered to influence maritime cyber risk management more proactively.

Originating in the design of interactive computer systems (ISO 2019), HCD places user needs, abilities, and purposes at the centre of the design process (Vu and Lützhöft 2020). Therefore, through the application of an HCD approach, this paper argues that METI and maritime industry companies can design and implement maritime cyber resilience training with their learners that is accurate, realistic, and relevant to ensure its effectiveness and usefulness in the real world. To be realistic and impactful, the tasks and social factors in the training must be technically and factually correct considering social and simulator fidelity (Wahl 2020), in order to present a true-to-life example that is relevant and useful to the nautical operational processes of the personnel receiving the training.

To better understand how adopting an HCD approach could facilitate an improvement in the accuracy, realism, and relevance of training, the remainder of this paper will do the following. Firstly, this paper will briefly ground this work within the current learning approaches adopted by the maritime sector, before discussing how the sector is currently addressing cyber risk management training. The paper will further introduce the HCD approach and how this could be implemented by an organisation to aid in the design of training. The paper will demonstrate the methodology required to develop a training example that is accurate, realistic, and relevant to a particular organisation. Finally, the paper will offer conclusions on the benefits, and potential drawbacks, of utilising an HCD approach when considering cyber risk management training.

2 Maritime learning and cyber training

As the foundation of this paper is within the aspect of learning and training, it is important to investigate learning theories adopted within the maritime sector. As Oommen (2020) argues, people learn via different methods. Looking at the maritime sector specifically, the applied methods rely on practical application. A fundamental component of STCW is sea-going service, by which a cadet must acquire a minimum number of months of service aboard a vessel to be certified. As part of that sea service, cadets muster on board with a set of knowledge and skills, facilitated by their training institution. The cadet then takes part in the everyday life alongside long-serving seafarers, learning on the job from those around them how to apply their knowledge practically to daily tasks and operations. The cadets are corrected when doing something wrong, or inappropriate, as such actions could have an impact on the safety of the ship and crew.

This approach to learning aligns well with both the constructivist and connectivist learning approaches. Connectivism focuses on the individual learner who forms knowledge within a network of nodes. A node can be any source of information,

including a computer, a human, or an organisation. The learner then connects the information gained from these various sources, placing it into the context of their environment. This particular approach allows the learner to experience knowledge from a variety of perspectives and sources, helping them to deepen their understanding (Siemens 2004). In constructivism, the learner takes an active approach to their learning and is encouraged to complete their learning alone by solving real work problems. The teacher, in this context the experienced seafarer, encourages the learner to reflect on the process and assists the learner to close any gaps between their knowledge and its practical application (Oommen 2020). While ‘teacher’ is a common term for teaching studies, the remainder of this paper will use the term ‘instructor’, as it fits the practical, maritime training terminology better. In addition, the student will be addressed as a learner, as the remainder of the paper address both professional learners in the industry seeking increased competence and cadet learners undertaking nautical studies.

These two learning approaches are important when considering maritime cyber risk management. Maritime cyber risk management is an interdisciplinary subject, consisting of aspects such as maritime cyber resilience, safety, and security, so learners need to develop skills to work together and respond collaboratively. ‘Maritime cyber resilience’ will be addressed in Section 3.1, and considering maritime cyber resilience training, the learning approaches constructivism and connectivism complement each other. Constructivism says that learners construct knowledge using their experiences and pre-existing knowledge, rather than just passively taking in information (UoB 2022). Connectivism, as illustrated by Siemens (2004), is well suited for blended learning, and focuses on learners connecting different information sources, ideas, and concepts (Goldie 2016). In maritime cyber risk management, being able to gather information from various sources, analyse, and then synthesise it is a vital skill when dealing with cyber incidents. Thus, maritime cyber resilience training is important for seafarers, as it exposes them to the different sources of data, and skills needed to respond to a cyber incident.

A combined approach of constructivism and connectivism will be beneficial in the development training for maritime cyber resilience, as there is still a lack of real-world examples of safety-critical cyber incidents. For example, one of the most notable cyber-attacks affecting the maritime industry, the NotPetya incident at Maersk in 2017, did not directly affect ship’s systems. However, the incident destroyed over 55,000 computers and 7000 servers used for business operations (Ashford 2019), illustrating that if this had propagated to on board ships, it could have caused serious consequences for the crew needing to maintain the safety of the vessel. In addition, these onshore personnel did need to communicate with their crews effectively due to the disruption caused by NotPetya.

A learning environment within the maritime sector where these two teaching methods can be effectively used is the maritime training simulator utilised in nautical sciences education, hereafter addressed as ‘maritime simulator’. Training utilising maritime simulators is a vital part of cadet education. Considering a typical maritime training scenario as described by Sellberg et al. (2021), learners would construct their learning together with an instructor, connecting this knowledge with other various sources, including their peers. The instructor would typically expose

the learners to a navigational problem, and the learners must collectively learn and construct a response using their experiences, considering both their triumphs and failures. This setting utilises the instructor, the other learners, whiteboards, projectors, documentation, and simulations to allow the learner to connect this information to form a coherent understanding of the topic at hand. The learner can then utilise the already gained knowledge (e.g. ship knowledge, nautical operations, safety management, crisis handling) and connect those nodes of newly acquired knowledge such as known cyber risks, as well as simulated and theoretically discussed consequences of cyber-attack scenarios. Thus, it can be claimed that both constructivism and connectivism are already used in traditional maritime training and will therefore benefit maritime cyber resilience training. In light of the previous, the learners should ask the question: How can my previous knowledge and additional resources help me in overcoming a cyber incident (connectivism) and how can I use this 'real world' problem to understand how I can best prepare if such or similar events were to happen (constructivism)?

2.1 Related work

Scanlan et al. (2022) highlight that the educational needs in the maritime industry are shifting. Sailing and operating a ship have always been related to safety, and today safety can be affected by cyber risks. However, cyber risk management is not explicitly mentioned within the STCW, but it is only inferred (Hopcraft 2021). Training which is not mandatory for keeping sea service certificates up-to-date is normally not prioritised by the maritime industry, as the industry is profit driven and cost sensitive, and traditionally reluctant to invest in courses not required by regulations (Erstad et al. 2022a). As such, METI and designers of maritime training programs should be aware of these new risks and tailor programs to the needs of the specific operation. Well-designed training, which is perceived as enhancing safety, will have a positive influence on a person's willingness to engage and overall performance (Nazir et al. 2015). Raising general awareness of maritime cyber security would help reduce the risk (Tam and Jones 2019; Akpan et al. 2022; Ben Farah et al. 2022). As such, the sector is becoming increasingly aware of the need to include cyber risk management training within academia which also serve seafarer schedules. In addition, the IMO has released guidelines that point out that personnel at all levels of an organisation should have an appropriate level of cyber risk awareness (IMO 2017a).

A training concept introducing maritime cyber risk management is the MariMOOC (Scanlan et al. 2022), which is short for Maritime Massively Open Online Course. The MariMOOC concept is a free, individual, training course available online 24/7. Using an open-source concept benefits the theoretical fundamental knowledge for cyber risk management in an efficient and structured way. However, it does not necessarily fully encompass the constructivist and connectivist approaches within the sector and does not allow for the practical application of problem-solving in teams, seen by other teaching methods. As this is delivered as individual

self-directed online learning, it does not foster team dynamics or give practical ways to practice communication.

Scanlan et al. (2022) argue that to engage stakeholders within maritime cyber risk management, training organisations could revisit the concepts of crew resources management (CRM). Originating from the aviation sector, CRM is already implemented in the maritime sector in both the bridge and engine departments and could be developed further to consider cyber as a context (Scanlan et al. 2022). Studies, like Raimondi et al. (2022) and (de La Vallée et al. 2022), describe training for enhancing the maritime cyber security capabilities for Security Operation Centres (SOC). Both SOC papers utilise the concept of cyber ranges in a maritime context and include practical elements. However, the scenarios are only targeted towards technically oriented SOC operators, and not operational and management personnel. Raimondi et al. (2022) emphasise that SOC operators must learn soft skills in order to relate key information back to the ship crew, pointing again to the importance of effective communication. Canepa et al. (2021) also argue that training is not only important for the user but also for other members of the extended technical teams. Considering maritime cyber resilience training, it should not focus solely on the seafarer, but other stakeholders should also be included, as will be further elaborated in Section 3.

Considering non-maritime, traditional cyber security training, it can vary from a simple tabletop discussion to detailed, live, full-scale technical cyber contests (Lund 2022). The length of the different forms of training can vary from single-day exercises to complex scenarios which last for days. Lund (2022) highlights that most cyber security exercises utilise the concept of cyber ranges. A cyber range is an infrastructure which utilises virtualization technology to create emulated networks, which are used both for training and development (Lund 2022; Vykopal et al. 2017). By utilising a cyber range, the facilitators can create an environment where an adversary actor (i.e. a hacker) is supposed to attack the victims' systems (i.e. the organisation under attack). The victims are also usually the main audience for the exercise (Lund 2022). Stoker et al. (2022) argue that the maritime industry can benefit from implementing non-maritime cyber security specialists. Training by using cyber ranges is beneficial for technical staff in an organisation, with in-depth knowledge of the cyber risks and the systems under study. It would seem unreasonable to put a deck officer and a ship engineer in traditional cyber ranges, as they most likely do not have the prerequisite knowledge to operate the systems, nor fight against cyberattacks. On the same argument, it would be unreasonable to put SOC staff in a maritime simulator to perform nautical operations, as they do not possess the prerequisite knowledge. However, as this paper will argue, engaging with these different perspectives within training enhances its effectiveness, whilst ensuring its realism, relevance, and accuracy.

As this paper moves forward to present an HCD methodology for designing training, it is important to remember the foundational aspects of maritime training. Firstly, the training must be focused on the safety and security of the ship and the crew. Secondly, training must provide some way for learners to put theory into practice. Thirdly, training must be considerate of the new dynamic risks that seafarers face.

3 Human-centred design

Human-centred design is a design philosophy (Norman 2013) that became increasingly popular in the 1980s (Vu and Lützhöft 2020). Due to increasing use and popularity over the years, HCD has now been adopted as an internationally recognised standard. To this end, the HCD process applied in this project is based on the ISO standard “Ergonomics of human-system interaction – Human-centred design for interactive systems” and is primarily focused on producing recommendations for activities related to designing interactive systems for computer-based systems (ISO 2019). HCD aids system designers to produce a solution to a user problem. The adoption of an HCD approach is not widely taken within the maritime sector as it is a very time-consuming process. However, as Vu and Lützhöft (2020) argue, the benefits of this approach outweigh the challenges. For instance, Porathe (2016) highlights the benefits of using HCD to develop prototype tools for bridge equipment. Further to this, Abey Siriwardhane et al. (2016) proposed a framework for facilitating an HCD approach into maritime engineering education, to ensure that engineers consider human factors at an earlier stage in the ship-building process. The IMO has implemented a ‘Guideline on Software Quality Assurance and Human-Centred Design (HCD) for e-Navigation’ (IMO 2015), thus formally accepting and establishing the link between HCD, human factors, and technology. Therefore, it is feasible to implement the HCD process when designing maritime cyber risk resilience training.

The goal of HCD is to provide the designer of a system with recommendations on activities to produce usable solutions, intended to fit the user requirements. In order to achieve that the training is human-centred, the next sections will demonstrate the use of theory in practice. Figure 1 below illustrates the HCD process on a holistic

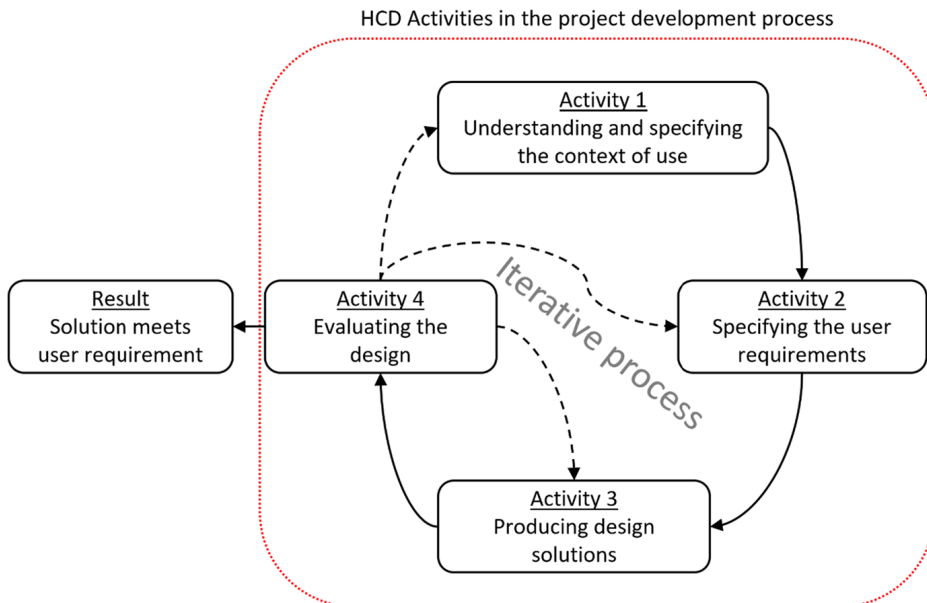


Fig. 1 The human-centred design process, adapted from (ISO 2019)

level and is adapted from the HCD standard (ISO 2019). HCD focuses on four different main activities in a project cycle. The activities relate to the respective HCD chapters. For example, the first activity relates to the definition of the users, the goal and task for the users, the characteristics of users, as well as the environment.

The authors argue that there are two levels to adopting the HCD method to design and develop training. The first, the macro-level, focuses on using the HCD principles to design a holistic solution to the identified problem. An example of this type of macro-level solution would be a complete cyber risk management training course. The second level of application would be at the micro-level, whereby the large problem is broken down with smaller (micro) solutions that, when combined, form the macro solution. For example, theory sessions, simulator exercises, and handouts would all be micro-solutions that together form part of the macro-training course.

This approach to the development of training is supported by Canepa et al. (2021), who argue that the development of a training framework for cyber security issues is necessary for the maritime industry. To aid in the development of these frameworks, Bacasdoon and Bolmsten (2022) conceptualised a model to evaluate METI educational approach, and contribution, to cyber security education. One aim of the framework is to aid METI in developing cyber security courses by developing an understanding of how micro-level solutions like learning activities and tools all contribute to the development and retention of skills.

It is important to note that solutions which are right for one METI or organisation might not fit another. The maritime industry is very diverse, different METI focus on different subsectors of the maritime industry, like passenger transport or offshore operations. Therefore, the learners and problems will differ, requiring different solutions. That is not to say that some of the micro-level solutions will not be similar, or the same, but the overall macro-solution of a training course may make use of different elements. The application of the HCD approach allows METI to understand their users and their specific problems to ensure that their solutions, both macro and micro, are relevant, realistic, and accurate.

3.1 Understanding and specifying the context of use

The first activity is defining the users, their characteristics, goals, and tasks, as well as the environment they operate within. Once this has been achieved, this can inform the context of the problem at hand and introduce a range of possible solutions to overcome it. This could be considered a macro-level activity within the HCD, whereby the designers of solutions are trying to gain a high-level understanding of why they are developing cyber risk management training.

In general, a ship's business model is based on making a profit from sailing and performing the intended operation for the ship. Therefore, ship safety, i.e., its ability to complete operations effectively, is considered a main goal for all stakeholders involved. As discussed above, Resolution MSC.428(98) urges the shipping industry to implement practices and procedures in an attempt to become operationally resilient toward cyber risks. Thus, maritime cyber resilience training is expected to have

a positive effect on maritime cyber risk capabilities, allowing the ship to advance towards its main goal of continued safe operations.

The maritime transportation system is complex, consisting of many different types of ships, operations, and stakeholders (Kessler and Shepard 2020). Erstad et al. (2021) describe the navigator at the sharp end of a nautical operation, where the navigator is seen as an asset to bring order to a cyber risk situation on a ship's bridge. However, all nautical operations rely on other vital roles on board, such as engineers and electricians. In addition, there is a full, shore-based support system, consisting of the ship owner, the insurance company, the class society, the ship equipment vendors, and national maritime authorities, amongst others. Therefore, in response to a cyber incident, it is important to consider these perspectives (ISO 2019), and how these actions could impact the response of the crew, and in particular the navigator, on board. The 'user' in this paper is thus the learner within the maritime industry, which can be a professional worker, a maritime cadet undertaking education or a simulator instructor who is responsible for facilitating training. Seeking additional knowledge considering maritime cyber resilience is what unifies the learners to be defined as the users.

As well as engaging directly with the organisations involved in the operations, attention should be paid to the current academic research relevant to the users and problem. In relation to maritime cyber risks, there are a number of papers that proposed maritime cyber incident scenarios (e.g. Tam et al. 2021a; Lund et al. 2018; Jo et al. 2022; Kessler and Shepard 2020; Meland et al. 2021). These are noteworthy scenarios, but are not intended for training purposes. Thus, whilst the research will ensure the accuracy of the developed solution, these findings need to be related to the specific user context to ensure that they are also relevant.

With this understanding of the users and their specific characteristics, it is important to consider the solutions that will best solve the problem at hand. Due to the complexity and diversity of responding stakeholders to a maritime risk incident, the development of training should be developed by a team with diverse expertise covering all areas of maritime operations, including cyber risk management, maritime training, ship management, maritime logistics, operational safety, and organisational economic stability. Maritime cyber risk management will vary somewhat from different aspects in an organisation, depending on the factors for upholding normal operations, as some stakeholders of the organisation may value the confidentiality of information as more important than the availability of a system. As maritime cyber resilience emphasises the ability to anticipate, withstand, recover, and evolve from a cyber threat in the minimum amount of time (Erstad et al. 2021), it would serve as a unifying concept, contributing to maritime cyber risk management knowledge.

As discussed in Section 2, maritime training is underpinned by the practical application of knowledge and skills. Connectivism begins with the individual who feeds knowledge into organisations and institutions and receives knowledge back, in a network of knowledge development (Siemens 2004). Maritime simulators offer a safe environment in which users are able to integrate their knowledge into the risk scenario response, where mistakes do not have significant impacts. Whilst not an exact replacement for time on board a ship during actual operations, training in maritime simulators has been a central strategy for increasing the practical problem-solving

competencies of future seafarers (Hontvedt and Arnseth 2013; Sellberg et al. 2018). METI today often utilise multiple high-fidelity maritime simulator setups, in addition to a briefing/debriefing room (Sellberg et al. 2018). This method allows for both theory and practical-based training to occur simultaneously, enhancing the reflective and constructive work of the learners (Sellberg et al. 2021). In a literature review by Chowdhury and Gkioulos (2021a), Chowdhury argues for the use of simulations in cyber security training, in particular team-based training, which is commonplace in critical infrastructure protection (i.e. aviation, energy, and nuclear). Therefore, the goal of the training scenarios, developed through an HCD approach, is to facilitate learning across the different groups (ship crew and shoreside support personnel) in ways that enhance the understanding and encourage a unified response as a way to overcome some of the perceived cyber risks.

There are several other arguments as to why training in simulators is a good solution to maritime cyber risk management training. Firstly, it is not possible for ships to dedicate the time and resources to perform extensive cyber training on board. Therefore, through the use of simulator exercises over a couple of hours, it allows organisations to potentially fit a large amount of content into achievable segments. Secondly, it would not be deemed safe to allow a live demonstration of a cyber incident on board. Such a demonstration could put the ship, crew, and systems on board at risk.

3.2 Specifying the user requirements

With this understanding of the users, their environment and characteristics, the problem, and potential solution, the second activity involves defining the specific user requirements, in order to propose more specific solutions to the problem at hand. The needs of both the user and other stakeholders should be emphasised (ISO 2019), meaning that as many perspectives should be included as feasible. To learn what the specific user requirements are, one can gather information in various ways, depending on the scope and size of the project including interviews, focus groups, field studies, simulations, and surveys, amongst others (Porathe 2016).

To demonstrate this step, the authors conducted interviews with navigators and ship owner representatives. The interviews aimed to understand how navigators interpret cyber threats and the effect this has on the maritime ecosystem from a navigator's perspective (Erstad et al. 2022a). The interviews revealed several key themes, such as the need for specific cyber threat training and the communication and coordination challenges between seafarers and shore personnel in response to incidents. The authors also raised the concern that there is little consensus amongst navigators on what a maritime cyber threat is, how it should be handled, and its potential consequences. What is more, the maritime industry often handles problems pragmatically and has a tradition of implementing unwritten rules, whereby seafarers cope with situations as they emerge and solve problems in their own way (Erstad et al. 2022a; Madsen et al. 2022). An approach is now being applied to cyber risk issues. Thus, the provision of maritime cyber resilience

training that illustrates different cyber risk scenarios and consequences could help develop a more informed approach to maritime cyber risk management.

As argued in the first activity of the HCD, maritime simulators are a safe environment where learners can develop skills and engage with numerous stakeholders holistically in scenarios that are relevant, realistic, and accurate for their defined problems. From the completed discussions, there is a lack of training, in particular simulator scenarios, which can be used to aid the sector in coping with cyber risks. This was seen as a difficult challenge to overcome as seafarers and maritime stakeholders, whilst holding expertise in maritime operations and risk management, lack the in-depth knowledge of cyber risks to integrate this effectively. As highlighted in Section 2.1, those with specific cyber risk knowledge lack the maritime-specific knowledge required to design accurate, realistic, and relevant training scenarios. To overcome this challenge, and further aid the definition of user requirements, more data collection was required. In this instance, the authors held a workshop, aimed at bringing both relevant maritime and cyber security stakeholders together to define scenarios that were accurate, realistic, and relevant for the particular organisation from both an operational and technical perspective (Erstad et al. 2022b). To help facilitate cross-discipline understanding, different interactive activities were performed to demonstrate both operational and technical capabilities. For example, several short 5–10 min simulator demonstrations were played out to help spark the imagination of the possibilities when using a maritime simulator within a cyber context.

It is also important to identify and specify trade-offs within this activity, in an attempt to map out potential conflicts between user requirements (ISO 2019). For example, there is a difference between how new navigators and experienced navigators interpret risks and if the risks are even feasible or realistic (Erstad et al. 2022a). Thus, scenarios must be tailored to the experiences of the intended learners. However, as cyber is still not part of STCW, the difference in risk perception is not as pronounced, potentially allowing the development of a ‘one-size-fits-all’ scenario, which itself could lead to challenges in creation. Wahl (2020) highlights the possibility of making participants take an active role in the scenario by altering the roles they play in a simulator scenario, which can be a solution to such a trade-off. For example, experienced mariners can play the role of shoreside personnel, whilst other stakeholders can play the role of the ship’s crew on board. This allows all participants to understand the operational requirements, and cyber risk management processes from different perspectives, facilitating a better understanding of cyber risk management and incident response. Identifying such trade-offs may be hard to do in advance, which again talks in favour of developing a flexible plan for maritime cyber resilience training, which will be discussed in the next section.

Another challenge is that current simulators are not fully equipped to simulate a cyber risk scenario in its entirety, but are still able to mimic the consequences realistically. For example, a cyber risk towards the electronic chart and display information system (ECDIS) could be a malware attack making the system crash. Whilst the simulator cannot mimic the whole attack chain, the trade-off is that it can mimic the consequences (i.e. loss of a navigational aid) in a realistic and relevant scenario for the users, without any safety risks to the ship or its crew and system. This allows

participants to focus less on the technical details of a cyber-attack and more on the operational impact.

3.3 Producing solutions

The third activity aims to propose and produce the actual solutions for the problem, based on findings from the previous activities. The previous activities have primarily focused on understanding the high-level requirements of the user and the solutions the organisation is creating. This phase aims at taking this macro understanding and applying that to the development of micro-level solutions. In the context of maritime cyber resilience training, the organisation now understands their intended audience (the user) and the different appropriate solutions that might exist (classroom activities, table-top, simulator exercises, posters, etc.) and are now at the point of creating those solutions.

This paper has argued that simulation is a valuable tool when adopting a connectivist and constructivist approach to both cyber awareness, and maritime training. However, some challenges need to be addressed when adopting these particular approaches, challenges that should be considered part of the HCD process. It has been argued that constructivism is a culture and not a fragmented collection of practices (Windschitl 1999), whereby it must like any culture be integrated and accepted as the norm within the work environment. Thus, during the early stages of the HCD, consideration must be given to how each training artefact, like simulator exercises, might need other artefacts and conceptual foundations to allow for the most effective use of the exercise (Watson 2001).

There are other logistical challenges that must be overcome, particularly when designing these practical sessions to ensure the full constructivist and collectivist potential is reached. These include understanding the new demands on both the instructor and learners (Windschitl 1999). For example, these approaches assume that the learners have a set of pre-existing knowledge and experiences, and a willingness to share them. If neither occurs, it could hamper the effectiveness of the training. Furthermore, due to the fluid and interactive nature of these sessions, made more so by the practical and semi-autonomous nature of simulator exercises, the instructor may find it challenging to control the exercise and discussion, again potentially hampering the learning outcomes of the exercise.

In the context of the examples outlined above, maritime simulator training is chosen as the solution under study for this paper. This phase would be about understanding how to best utilise the capabilities of the simulator, whilst reducing or accepting the limitations. For example, Wahl (2020) points out four recommendations for the development of simulator-based training. First, the simulator technology is essential, but it is not always necessary to have a true physical copy of a ship's bridge, as other elements, like the ship type, operation, and operational environment, all play a role in achieving realistic, relevant, and accurate scenarios. This mentality of only needing exercises to be realistic and relevant enough for the audience is supported by Hontvedt and Arnseth (2013). This leads to the second element, where real events and daily work practices are included, whereby there are enough elements within the

scenario that make them relevant to the learner whilst allowing them to apply their pre-existing knowledge and experience of the particular operation. The third factor argues for users to share stories and feedback with each other in order to improve the learning quality. This factor can be enhanced through the suggested role and hierarchy swapping, as it allows users to experience different perspectives and feed their experiences back into the group. The fourth consideration is the role of the instructor. The scenario should be designed in such a way as to aid the instructor in facilitating interaction between the learners to create life-like collaborative activities (Wahl 2020).

The instructor is the most important asset in the simulator scenario (Sellberg and Wiig 2020), and as the responsible facilitator of the scenario, the instructor must go beyond being only a system operator (Wahl 2020). The instructor should enable interaction between the learners and the systems, making the scenario as realistic as possible. A cyberattack can have an impact on several different aspects, such as operational safety, company confidential information, environmental safety, financial stability, and reputational factors. However, finding an instructor that has a good knowledge of both maritime supply chains and the relevant cyber risks might be challenging.

There are two critical phases within a simulation scenario, namely, the briefing before and the debriefing after completion (Sellberg et al. 2018). During the briefing, users should be provided with contextual detail like the roles and responsibilities they will be fulfilling, as well as technical details of the systems they are using and the information which will be available. Some details about what is to be expected might be provided. However, cyber incident scenarios may unfold dynamically and in an unknown manner. Therefore, the instructor should not be unrealistically expecting the standard maritime incident response to be effective. The instructor should encourage learners during the briefing that there is no single correct response to the coming scenario. Thus, learners should expect to use their experiences and pre-existing knowledge to develop a response that is most appropriate to the unfolding situation.

During the debrief, the instructor again plays a vital role, whereby they use the debriefing as a forum where the learners get a chance to reflect and discuss the scenario, as well as their own and their peers' actions. Wahl et al. (2020) support this emphasis on joint reflection. Sellberg and Wiig (2020) argue that a good method to utilise during debriefing is playback. This allows the users and the instructor to watch a recording of the exercise from a third-person perspective. Coupling this playback with examples from real events, or in this case, examples from cyber incident research will allow users to connect the dots between their own actions and the actions of others. Playback also allows the identification of potential mistakes, and where other pros and cons of other possible actions can be debated.

The proposed micro-level solution should be selected for its ability to facilitate the enhancement of maritime cyber resilience skills for team-based learning. Drawing on similar fields of research, Wahl et al. (2020) have investigated how simulators are an effective solution to the development of resilience skills for Dynamic Positioning Operators (DPO). The study '...indicate[s] three resilience skills that are essential to DPOs, and that can be trained in simulators; (1)

the ability to recognise anomalies and solve problems in a flexible manner, (2) the ability to define limits of action through shared knowledge with peers, and (3) the ability to operate the system with confidence' (Wahl et al. 2020, page 9). These resilience skills would be very beneficial when considering maritime cyber resilience training and should be thoroughly addressed by the instructor. Considering the third resilience skill mentioned, the authors would argue to operate the maritime cyber risk management system, rather than the technical ship system itself. Wahl et al. (2020) findings correlate and can be connected with the maritime cyber resilience goals 'anticipate', 'withstand', 'recover', and 'evolve' from a cyber threat situation in the minimum amount of time (Erstad et al. 2021). However, resilience skills are not developed by simulator training alone, and a broader approach embracing more actors (stakeholders), more technology (instructor stations and learner stations of simulator), and more platforms ('ship owner incident response office' in the instructor/briefing room) should be included (Wahl et al. 2020). The authors argue for the resilience skills of 'flexibility', 'efficiency', 'communication', and 'coordination', as well as the ability to learn, are important to address in maritime cyber resilience training. For example, during a real-life cyber incident, the navigators on board a bridge need to communicate and coordinate with shoreside support in a flexible manner, in order to overcome cyber incidents, as they do not have in-depth knowledge of such incidents. Learning will be of importance, as it is for every new risk emerging in any industry.

One of the potential drawbacks of using simulators as a solution, as highlighted by Nazir et al. (2015), is the fact that there is often a gap between the needs of the industry and the actual training of the operators, a gap that is only exacerbated by the rapid increase of digital technology being integrated into maritime operations. Discussions from the workshops held as an earlier part of the HCD supported the literature arguing that there is a lack of simulated abnormalities and accidents, except for vulnerabilities in electronic vessel positioning fixing, which leads to a lack of realism and accuracy within these scenarios. Regardless of the chosen solution, the limitations must be considered and factored in. One possible workaround would be addressing these limitations in another solution, for example, demonstrating the technical elements of a cyber incident theoretically or in a cyber range and then demonstrating the physical consequences in the maritime simulator. Considering cyber ranges and maritime simulators, an interesting concept of the future would be to combine the two by integrating cyber range software and capabilities into maritime simulators, as suggested by Tam et al. (2021b). In many ways, maritime simulators satisfy the definition of a cyber-range, given the amount of simulation and emulation used. However, maritime simulators are yet to properly consider the cyber context.

Therefore, when developing the solutions, consideration must be given to both the available capabilities and limitations of the chosen method. By an organisation completing detailed work during the earlier phases of the HCD process, it will allow the development of better solutions that are considerate of the users, the problem, and the solution.

3.4 Evaluating the design

Evaluation is a vital process within the HCD and should be implemented early as an iterative activity performed throughout the whole design process. Evaluation of an HCD solution can be achieved by several methods, such as user-based testing, inspection-based testing, and long-term monitoring (ISO 2019).

User-based testing can be undertaken at any stage in the design (ISO 2019). A form for user-based testing is prototype testing, where users are exposed to simple simulated cyber scenarios, like those in the workshop, and are then asked if it was a relevant, realistic, and accurate solution. Feedback from the discussions is then used to validate the chosen solution, both as a standalone element and as a single part of a large solution like a training course. The feedback also allows changes to be made to the solution to ensure that it remains as relevant, realistic, and accurate as possible.

Considering inspection-based testing, HCD urges that it should be performed by usability experts who base their judgement on prior experience (ISO 2019). At this stage, thorough testing with usability experts has not been performed, but it will be a prerequisite to invite evaluators with relevant competence to attend pilot scenarios. The stakeholders attending the previous HCD process should be invited to participate in the practical undertaking of the pilot scenarios proposed. Still, there has been a preliminary document review of the process by these experts, which serves as an early-stage inspection-based test. As maritime cyber risk management still is a novel research field, the authors would also argue for transparency in the developing process of training methods, such as is one purpose of this paper.

The third and final type of evaluation is long-term monitoring. This type of monitoring could be best achieved through learner assessment and feedback (ISO 2019). The implementation of a long-term evaluation scheme that assesses learner skill acquisition and long-term retention can help to evaluate the effectiveness of its training solutions. Direct learner feedback following the completion of the training would also provide an ongoing source of evaluation data to ensure that the training remains accurate, relevant, and realistic to the users as their roles, operations and risks change over time. In terms of such long-term user-based testing amongst the actual participants of such a training scenario, IMO (2012) provides 'Course Feedback Form' templates, which can form the basis for participant evaluative feedback for training.

Assessment of learning is necessary and should touch upon what the learner should know, what the learner should be able to do, and how the learner feels or modifies attitudes (IMO 2012). Even though maritime cyber resilience is a different field of research than traditional maritime training, findings in Sellberg et al. (2018) can be seen in parallel to findings in Chowdhury and Gkioulos (2021b), whereby there is an emphasis on the need for cyber security skills appropriate for different organisational roles. These include technical, soft, implementation, and management skills. These kinds of skills will be relevant both to seafarers and ship owner management. Sellberg et al. (2018) also conclude that there are emerging challenges in the field of assessment of maritime simulations because of emerging technologies. The development of cyberspace on board ships can create such a challenge. These

mentioned skills also correlate with the maritime cyber resilience skills, mentioned previously in the paper.

The IMO recognise that no organisation within the maritime sector is the same (IMO 2017a), and thus cyber risk management will differ across the sector. What might be a thorough cyber risk assessment for one ship, might not fit another. It is reasonable to believe that the same will apply to the assessment of the cyber resilience of learners. As the simulator exercises should be specifically tailored to the individual learners of the specific course, a standard generalised form of assessment covering the whole of the maritime sector might be hard to achieve, especially since the field of research is still new and unfolding. On the other hand, after performing the HCD process, the organisation developing training would have a thorough insight into what is important for the specific organisation, and therefore should be able to develop tailored assessments based on the process easily. For the solution presented in this paper, the authors would argue for a qualitative approach, as it can be ad-hoc altered to the learner's needs and focus on the resilience skills mentioned above.

It would be reasonable to assume that if the assessment of the learners receives a high score (quantitative or qualitative), either by a knowledge or skill test, or interviews/conversations, the user-based testing feedback mentioned in the evaluation part of HCD would also be deemed positive. In terms of usability (ISO 2019), the aspects of effectiveness, efficiency and satisfaction are important. The instructor needs to highlight the HCD-related questions to the learners, in order to maintain the focus on the user.

4 An HCD approach to developing and conducting a maritime cyber resilience simulator scenario

This section will provide a demonstration of how an HCD approach can be implemented in the development of a cyber resilience training exercise. The following sections will outline an overview of the intended learners, instructor, and the problem space, before presenting a detailed description of a scenario. A simulator exercise is the chosen solution as it provides the most effective and appropriate way for the organisation in question to develop cyber resilience skills. Depending on who is developing the training, it is not always appropriate to utilise simulators. As one of the organisations engaging with the authors is a METI, it allows the use of maritime simulators. Lacking simulators themselves, or engagement with a METI, other maritime organisations can still be able to employ an HCD approach to develop other effective internal training solutions, such as table-top scenarios.

Both the engaging METI and organisations in the HCD process focus mostly on offshore operations in the North Sea, which includes both traditional maritime sector perspectives and oil and gas sector perspectives. What is more, the offshore oil and gas sectors are also part of Norwegian critical infrastructure, and the sector is heavily driven by safety and security. Therefore, to ensure the relevance of the scenario with the users, it was prudent to set the scenario within an offshore operational environment.

Based on the initial phase of the HCD process, one distinct problem was identified, which is the challenge of understanding, teamwork, and communication in relation to cyber risk scenarios. Therefore, the chosen simulation scenario is needed to facilitate the development of such understanding and team cooperation. To facilitate this, the chosen operational context, whilst realistic, was also simple to enable inference of pre-existing knowledge and skills. Furthermore, the simplistic nature of a scenario allows other, non-mariner, stakeholders to be part of the scenario and play the role of surveillance and monitoring.

The system chosen for the scenario was the ballast water handling systems or ballast water management systems (BWS). Most commercial ocean-going vessels use BWS in daily operations. BWS utilises pumps and separate water storage compartments, to ensure that the ship remains stable despite a variety of factors (Rajaram et al. 2022), including cargo distribution. In 2019, the car carrier *Golden Ray* capsized due to the chief officer entering the wrong ballast calculations (NTSB 2021), demonstrating the risk of incorrect operation of the system. In the IMO's cyber risk management guidelines, 'cargo systems' are identified as vulnerable systems (IMO 2017a). As part of a ship's cargo system, BIMCO specifically names the BWS as a critical, and vulnerable, cyber system (BIMCO 2020). Due to the control, and interface elements of the BWS their operation can be compromised by malware delivered either via USB or a phishing email (Rajaram et al. 2022). There have been reports that some malicious actors at a nation-state level are investigating ways in which these vulnerabilities can be used to cause an incident (Haynes 2021). Due to the BWS being common on many ships and being identified as vulnerable by both the literature, as well as exploratory discussions with stakeholders, it was selected as the target system for the scenario.

To ensure the continued accuracy and realism of the scenario, the technical details of attacking the BWS need to be understood and the consequences implemented. It is not within the scope of this paper to provide technical details on the actual attack. However, it is important to note that the BWS software normally runs on a Microsoft Windows PC. As the lifespan of a ship can vary from 20 to 50 years, the operating system versions on the on board computers may be outdated. Older and unpatched versions of Windows might be vulnerable to known cyber exploits such as *Eternal Blue* and *Eternal Romance*, which were utilised by the NotPetya attack to spread the infection mentioned earlier (Fayi 2018). Furthermore, mechanical control of valves and pumps in BWS systems is usually carried out by Programmable Logical Controllers (PLC), a component which also has known vulnerabilities (Milinković and Lazić 2012). When a sophisticated attack towards BWS is executed, it can give the attacker remote access to the system to view and edit files. Additionally, BWS may also be vulnerable to denial-of-service attacks which can cause the system with the BWS software to crash and be unavailable inhibiting the operator from making verified changes.

Other factors for the scenario need to be considered, for example, weather. Calm weather was chosen for the scenario, as this might be the first encounter with a cyber simulator scenario for some of the learners. The instructor should be careful not to make the scenario too difficult the first time, as the focus is towards team communication, and not ship handling. The instructor also needs to bear in mind that not all

learners have nautical education or are trained in harsh weather conditions, as the scenario should fit a wide scope of participants.

4.1 Description of scenario

To ensure maximum efficiency of scenario design, the chosen scenario described below has various variables that can be decided by the instructor prior to the session starting. These variables include vessel type, location, stakeholder engagement, and malicious actor profile, amongst others. As a result of the earlier phases of the HCD Process, the defined scenario focuses on the cyber vulnerabilities of BWS for a vessel that operates in the North Sea. The vessel can be a multipurpose subsea vessel or an offshore supply vessel, depending on the instructor's expertise and available simulator model. The adverse actor in the scenario can be either a nation-state or a criminal organisation. As a sophisticated attack towards BWS requires a high level of resources to deploy, a lesser organisation, or individual, would likely be unable to deploy it alone. The choice of a malicious actor will affect the motivation of the attack. For a nation-state, it could be demonstrating cyber capabilities, or for a criminal organisation, it could be simply monetary reasons. A part of the training discussion will be to ensure the learners understand the different motivations of malicious actors and how this could change the outcome, for example, criminal groups may attempt to extort a ransom.

There will potentially be many stakeholders in such a scenario, depending on the number of participants. The rig, the ship, the ship owner company, the rig owner company, and all shoreside support systems can all be involved and will be affected differently in terms of consequences. If a ship does not have control over the vessel systems inside the safety zone of the oil rig, the emergency alarm should go off, and even the coast guard and national authorities would be involved.

Therefore, the learners should play the role of the ship's crew, shoreside support and other maritime stakeholders. As a recommended minimum, there should at least be two learners on the ship's bridge (captain and officer of the watch (OOW)) and at least two learners in the ship owner's office. Such a composition of the teams will ensure that at least some of the learners in both teams are actually part of that team in real operations, ensuring that the response remains accurate and realistic. Optimally, there should also be learners to play roles such as the oil rig, the national coast guard, and other relevant maritime stakeholders mentioned earlier. However, if lacking the individuals, and expertise to play these roles, the instructor will need to ensure they introduce these perspectives into the session. This highlights why the instructor is such an important role in the simulator scenario.

As part of the scenario, and separate from the simulator, the team that forms the fictitious ship owner's office will need to enact the organisation's emergency response team and monitor the situation from the instructor room. Then, there is a clear line of communication (voice) with the instructor. There is also a need for dedicated communication channels (intercoms, VHF, mobile phone) to the bridge team.

The duration of a simulator exercise will vary with the scope of the scenario. IMO Model Course 6.10 describes several example scenarios for simulator exercises,

varying from one and a half hours (handover exercise) to up to three hours (specific skill training exercise) (IMO 2012). Following the earlier consultations in the HCD process and realising that the resources prioritising cyber training are limited, the simulator exercise was limited to 45 min. This duration allows an appropriate length of time for the attack to be initiated and for participants to respond. However, this timing will differ depending on the requirements of the organisation and the scenario.

To ensure maximum time efficiency, and to ensure the scenario was appropriate to the problem, the authors created a high-level overview of the exercise where the accuracy, relevance and realism were verified by the engaging organisation. Figure 2 provides a high-level overview of the phases of the training session, with the suggested maximum duration from Briefing to Debrief being around an hour and a half.

4.1.1 Pre-scenario preparation

Considering the overarching story for the scenario, the ship owner’s company receives an email earlier on the same day as the scenario is set. The instructor must generate an email to display to the participants in the briefing of the scenario. The email informs that if the adverse actors are not paid an unreasonable ransom to an anonymous account (e.g. bitcoin-account) within an unrealistic short time frame, *something* will happen to one of their ships. The email must also strictly instruct that if the malicious actors notice any system owned by the ship owner being taken offline or shut down, then they will trigger the attack. Participants are then notified that the ship owner’s company has contacted their IT (Information Technology) vendor. The vendor has responded saying that there has been no notification indicating abnormalities within any of the assets they oversee and that everything is functioning as expected.

The instructor also needs to create the simulation exercise to be used. For this, the vessel itself is discharging fuel to an oil rig via a hose connection. This close-to-rig operation makes the situation complex and risky. During this operation,

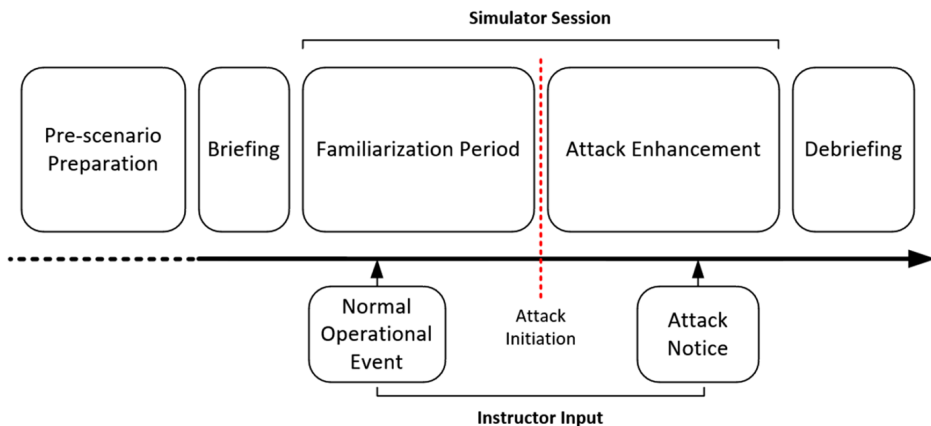


Fig. 2 Timeline of the scenario. Source: Authors

the vessel uses its dynamical positioning (DP) system, meaning the vessel is in a fixed position and not moving. The reason for using DP within the scenario is that the ship handling skills are not the purpose of the training and some participants will not have navigational experience. This gives all participants the opportunity to surveillance and monitor the ship and the situation and communicate with the other participants, rather than focus on ship manoeuvring.

It is also important to ensure the accuracy of the scenario prior to its development. Therefore, after previous consultations, it was determined that the scenario should not result in capsizing. This is because if a capsizing were to occur, the focus for the participants can alter more towards other aspects rather than the cyber incident. Also, if the ship capsizes, it could give a feeling of 'helplessness' to the participants, which is not the intent of the scenario. It is important to notice that not all ships can capsize due to an attack on the BWS; however, ships should not under any circumstance list uncontrollably inside an oil rig safety zone.

4.1.2 Briefing

During the briefing, the learning objectives, which are important for a scenario, should be made clear to the learners (IMO 2012). Emphasis on enhanced teamwork, communication, coordination and cyber risk management knowledge is important. In addition, the instructor should introduce the current operational environment and the vessel itself. This includes the details on the use of DP, and the expected actions of the crew (i.e. not worry about navigation).

4.1.3 Familiarisation

Familiarisation is a vital part of simulator training, and the participants should be familiarised with the simulator, the equipment and its limitations prior to the start of the scenario proper (IMO 2012). Standalone familiarisation training would be optimal. However, this is not always possible for intensive training scenarios, as time is a limiting factor. Therefore, it should be planned for a familiarisation period in the scenario itself, to introduce the participants to the environment and the operational controls which may differ from what they usually use. A way to do this is by the use of handover checklists or familiarisation checklists. Common for nautical operations is the use of handover when a new OOW is taking command of the vessel, which means that the OOW going off watch informs the relieving OOW about the status of the operation, vessel, and environment. The instructor would play the role of the OOW handover. A checklist also ensures that the participants know that the equipment they are using is functioning, e.g. an operational check of all communication equipment to be used. Establishing dedicated means of communication is very important for the scenario, as communication is

a key factor in crisis handling. This period should be limited to 10 min to allow enough time for the scenario proper to begin.

4.1.4 Normal operation event

In order to keep the crew active, the instructor should initiate a 'normal' event. This can be a radio check from the crane on the rig, providing general information on the status of the operation. The normal event should not be intended to worsen the situation for the bridge personnel, but rather focus on reducing stress and breaking radio silence.

4.1.5 Attack initiation

As the attack is initiated, the ship starts to list slowly to port. As a BWS computer is not standard equipment on all maritime simulators, the attack can be merely simulated by making the ship list. This can be performed by adding *external factors* on the ship, meaning that the simulator software simulates a heavy load on board, without the load being visible to the participants. A BWS computer might also be created as a simple mock-up, with a tank overview indicating that water is being filled on the tanks; however, this is not critical for the scenario.

4.1.6 Attack enhancement

The crew must be given the opportunity to notice and handle the situation together with shoreside support. The ship should not list 20 degrees to port instantly, but slowly and sequentially, for example, in short increments with a pause at 5-degree increments, thus allowing 20–30 min for the participants to respond to the developing scenario.

In these situations, it would be natural for the bridge crew to call the engine control room and to ask if they are the ones doing pump operation without noticing the bridge. If not, the instructor should call the bridge, as the chief engineer, to ask why they are doing BWS operation, without notifying the engine control room. An important part of the exercise is that no one has control over what is happening with the BWS system, and there are no corrective measures.

After 20–25 min of scenario time, the ship owner's company receives a new email, which says that the hackers now have demonstrated their powers and they could not see any payment on their account. The email informs the ship owner that they need to pay double the ransom stated in the first email, or *something* will happen to another random ship. Enhancing the scenario in this way will mean that the shoreside team will be put under pressure to respond, whilst considering the wider operational issues of the scenario.

4.1.7 Attack notice

If the participants themselves do not notice the ship listing, then the instructor should provide a small prompt to the participants so that they notice the incident, allowing them to have some time to respond within the scenario time limit.

4.1.8 Debrief

Considering the debrief, the instructor must facilitate productive and constructive discussions with the participants by taking an active role in the conversation. The scenario has no right or wrong outcome, as there is not much the crew can do in practice. Thus, the instructor should focus on communication, coordination, and understanding of maritime cyber risks. Due to the enhancement of the scenario to suggest that other ships might be affected, this brings in other elements to discussions, for instance, cyber risk scenarios are not always standalone events with consequences limited to one system, or piece of infrastructure. Motivations and consequences of the attack are also important, for example, in such a situation as this where the organisation must assume that the attacker has complete control to remotely access and monitor the BWS. Therefore, the crew had asked the engineer to shut down a pump manually, which could have triggered a further attack on another asset. Finally, the instructor should log the debriefing to facilitate for development of assessment methods, as mentioned earlier.

5 Conclusion

This paper has investigated how an HCD process can be applied to the development of maritime cyber resilience training. The HCD process is underpinned by the need to identify users, the goals, the environment, and a problem which needs a solution. For this paper, the problem was identified as a lack of cyber resilience training to respond to the increasing cyber risk within the maritime industry. This ‘need’ for training is discussed considering primarily the individual crew members actively serving on board ships, but also takes a more holistic approach by including a wider number of maritime stakeholders. The users were identified as the ones who need to respond to cyber-related incidents, which included experienced seafarers on board, academy cadets as well as other maritime stakeholders. The overall goal of adopting an HCD approach in this way is to develop training which enhances the safe operation of ships within the cyber risk landscape of the organisation.

Through the practical application of the HCD process, the authors outlined one possible solution that can form part of maritime cyber resilience training, team training in maritime simulators. By actively engaging with the end user during the development process, as prescribed by the HCD process, it ensures the developed maritime cyber resilience training is realistic, relevant, and accurate for the learners, their operations, and risks. Furthermore, the application of the HCD process demonstrates how this training can be tailored to focus more on team training aspects,

rather than specific technical skills, thus allowing learners to collectively construct learning and connect the crew with other maritime stakeholders in a practical way, which is the norm within the sector.

The justification for applying the HCD approach to maritime cyber resilience training is grounded in the use of the constructivism and connectivism learning approaches. As argued in Section 2, constructivism and connectivism are implicitly used in maritime simulator training. With maritime cyber resilience still a novel field of research, the teaching of those skills is yet to be fully realised within the maritime sector. Therefore, it is not unreasonable to argue that adopting well-known, and used, approaches in the delivery of this content will improve its effectiveness. To the best of the authors' knowledge, the combination of HCD, connectivism, and constructivism is a new and unexplored approach in maritime cyber resilience research. Both the authors and the readers of this paper need to be conscious of the implication this may have, as well as the potential challenges that follow with using these approaches, which are described throughout the paper.

The authors, therefore, argue that the application of the HCD process in the development of maritime cyber resilience training, whilst time-consuming, is an effective, efficient, and satisfactory methodology. Future work would look to applying the HCD approach in the development of a holistic, macro-level maritime cyber risk management training framework that uses simulations in unison with other solutions like posters, emails, newsletters, and online learning.

Acknowledgements The authors would also like to thank Arnt-Håkon Barmen, Terje Slinning, Marie Haugli-Sandvik, and Andreas Nygard Madsen at NTNU in Ålesund, as well as Island Offshore AS and all the colleagues of Cyber-SHIP lab, for help developing the idea, scenarios, and overcoming simulator challenges.

Funding Open access funding provided by NTNU Norwegian University of Science and Technology (incl St. Olavs Hospital - Trondheim University Hospital) This paper is partly funded by the research efforts under MarCy and Cyber-MAR. Maritime Cyber Resilience (MarCy) has received funding from the Research Council of Norway, with project number 295077. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.

Declarations

Disclaimer Content reflects only the authors' view, and neither the Research Council of Norway nor the European Commission, nor any project partner is responsible for any use that may be made of the information it contains.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

- Abey Siriwardhane A, Lützhöft M, Petersen ES, Enshaei H (2016) Human-centred design knowledge into maritime engineering education; theoretical framework. *Australas J Eng Educ* 21:49–60. <https://doi.org/10.1080/22054952.2017.1287038>
- Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M (2022) Cybersecurity challenges in the maritime sector. *Network* 2:123–138. <https://doi.org/10.3390/network2010009>
- Ashford W (2019) NotPetya offers industry-wide lessons, says Maersk's tech chief [Online]. *ComputerWeekly.com*: ComputerWeekly.com. Available: <https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief>. Accessed 23 Nov 2022
- Bacasdoon J, Bolmsten J (2022) A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches. *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation* 16:319–334. <https://www.transnav.eu/>
- Ben Farah MA, Ukwandu E, Hindy H, Brosset D, Bures M, Andonovic I, Bellekens X (2022) Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information* 13:22. <https://doi.org/10.3390/info13010022>
- BIMCO (2020) The Guidelines on Cyber Security onboard Ships. BIMCO (ed) Version 4.0
- Canepa M, Ballini F, Dalaklis D, Vakili S (2021) Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. *Proceedings of INTED2021 Conference*. 9th. <https://doi.org/10.21125/inted.2021.0726>
- Chowdhury N, Gkioulos V (2021) Cyber security training for critical infrastructure protection: a literature review. *Comp Sci Rev* 40:100361. <https://doi.org/10.1016/j.cosrev.2021.100361>
- Chowdhury N, Gkioulos V (2021b) Key competencies for critical infrastructure cyber-security: a systematic literature review. *Inf Comp Secur*. <https://doi.org/10.1108/ICS-07-2020-0121>
- De la Vallée P, Iosifidis G, Rossi A, Dri M, Mees W (2022) Sector-specific training - a federated maritime scenario. Cham: Springer International Publishing, pp 21–35. https://doi.org/10.1007/978-3-031-20215-5_3
- Erstad E, Ostnes R, Lund MS (2021) An operational approach to maritime cyber resilience. *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation* 15:27–34. <https://www.transnav.eu/>
- Erstad E, Lund MS, Ostnes R (2022a) Navigating through cyber threats, a maritime navigator's experience. <https://doi.org/10.54941/ahfe1002205>
- Erstad E, Larsen MH, Lund MS, Ostnes R (2022b). Maritime Cyber Simulator Scenario Workshop report. <https://ntnuopen.ntnu.no/ntnu-xmloi/handle/11250/3037765>. Accessed 12 Oct 2022
- Fayi SYA (2018) What Petya/NotPetya ransomware is and what its remediations are. *Information technology-new generations*. Springer. https://doi.org/10.1007/978-3-319-77028-4_15
- Goldie JGS (2016) Connectivism: a knowledge learning theory for the digital age? *Med Teach* 38:1064–1069. <https://doi.org/10.3109/0142159x.2016.1173661>
- Haynes D (2021) Iran's secret cyber files. *Sky News* [Online]. Available: <https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871>. Accessed 10 Dec 2022
- Heering D, Maennel O, Venables A (2021) Shortcomings in cybersecurity education for seafarers. *Developments in Maritime Technology and Engineering*. CRC Press. <https://doi.org/10.1201/9781003216582-06>
- Hontvedt M, Arnseth HC (2013) On the bridge to learn: analysing the social organization of nautical instruction in a ship simulator. *Int J Comput-Support Collab Learn* 8:89–112. <https://doi.org/10.1007/s11412-013-9166-3>
- Hopcraft R (2021) Developing maritime digital competencies. *IEEE Comm Stand Mag* 5:12–18. <https://doi.org/10.1109/mcomstd.101.2000073>
- Hopcraft R, Martin KM (2018) Effective maritime cybersecurity regulation—the case for a cyber code. *J Indian Ocean Reg* 14:354–366. <https://doi.org/10.1080/19480881.2018.1519056>
- IMO, I. M. O. (2012) Model Course 6.10 Train the simulator trainer and assessor. London: International Maritime Organization
- IMO, I. M. O. (2015) MSC.1/Circ.1512. Guideline on Software Assurance and Human-Centred Design for e-Navigation

- IMO, I. M. O. (2016) International convention on standards of training, certification and watchkeeping for seafarers (STCW). *International Maritime Organisation, London, UK*.
- IMO, I. M. O. (2017a) MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management.
- IMO, I. M. O. (2017b) Resolution MSC.428(98) - Maritime cyber risk management in safety management systems.
- IMO, I. M. O. (2018) International safety management code: with guidelines for its implementation. London, International Maritime Organization
- ISO, I. O. F. S. (2019) 9241–210: 2019 Ergonomics of human-system interaction. Part 210: Human-Centred Design for Interactive Systems. iso.org: International Organization for Standardization
- Jo Y, Choi O, You J, Cha Y, Lee DH (2022) Cyberattack models for ship equipment based on the MITRE ATT&CK framework. *Sensors* 22:1860. <https://doi.org/10.3390/s22051860>
- Kessler GC, Shepard SD (2020) *Maritime cybersecurity: a guide for leaders and managers*. Daytona Beach, Kessler & Shepard
- Larsen MH, Lund MS, Bjørneseth FB (2022) A model of factors influencing deck officers' cyber risk perception in offshore operations. *Marit Transp Res* 3:100065. <https://doi.org/10.1016/j.martra.2022.100065>
- Lund MS, Hareide OS, Jøsok Ø (2018) An attack on an integrated navigation system. *Sjøkrigsskolen*. <https://doi.org/10.21339/2464-353x.3.2.149>
- Lund MS (2022) Øving på cybersikkerheit: Ein casestudie av ei cybersikkerheitsøving. *Scand J Mil Stud* 5(1):244–256. <https://doi.org/10.31374/sjms.119>
- Madsen AN, Aarset MV, Alsos OA (2022) Safe and efficient maneuvering of a maritime autonomous surface ship (MASS) during encounters at sea: a novel approach. *Mar Transp Res* 3:100077. <https://doi.org/10.1016/j.martra.2022.100077>
- Meland P, Bernsmed K, Wille E, Rødseth Ø, Nesheim D (2021) A retrospective analysis of maritime cyber security incidents. *TransNav, The International Journal on Marine Navigation and Safety of Sea Transportation*. <https://www.transnav.eu/>
- Milinković SA, Lazić LR (2012) Industrial PLC security issues. 2012 20th Telecommunications Forum (TELFOR). *IEEE*, 1536–1539. <https://doi.org/10.1109/TELFOR.2012.6419513>
- Nazir S, Øvergård KI, Yang Z (2015) Towards effective training for process and maritime industries. *Procedia Manufacturing* 3:1519–1526. <https://doi.org/10.1016/j.promfg.2015.07.409>
- Norman D (2013) *The design of everyday things: revised and, expanded*. Basic books
- NTSB, N. T. S. B. (2021) Capsizing of roll-on/roll-off vehicle carrier golden ray, marine accident report. In: BOARD, N. T. S. (ed) *National Transportation Safety Board National Transportation Safety Board*. <https://www.nts.gov/investigations/Pages/DCA19FM048.aspx>. Accessed 10 Dec 2022
- Oommen PG (2020) Learning theories – taking a critical look at current learning theories and the ideas proposed by their authors. *Asian J Res Educ Soc Sci* 27–32%V 2
- Porathe T (2016) Human-centred design in the maritime domain. DS 85–1: Proceedings of NordDesign 2016, Volume 1, Trondheim, Norway, 10th–12th August 2016, 175–184
- Raimondi M, Longo G, Merlo A, Armando A, Russo E (2022) Training the maritime security operations centre teams. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). *IEEE*, 388–393. <https://doi.org/10.1109/csr54599.2022.9850324>
- Rajaram P, Priyanga R, Goh Voon Wei M, Zhou J (2022) Guidelines for cyber risk management in shipboard operational technology systems. *iTrust Centre for Research in Cyber Security: Singapore University of Technology and Design*. <https://doi.org/10.1088/1742-6596/2311/1/012002>
- Refsdal A, Solhaug B, Stølen K (2015) *Cyber-risk management*. Cyber-Risk Management. Springer. https://doi.org/10.1007/978-3-319-23570-7_5
- Scanlan J, Hopcraft R, Cowburn R, Trovåg JM, Lützhöft M (2022) Maritime education for a digital industry. *Necesse* 7:75
- Sellberg C, Wiig AC (2020) Telling stories from the sea: facilitating professional learning in maritime post-simulation debriefings. *Vocat Learn* 13:527–550. <https://doi.org/10.1007/s12186-020-09250-4>
- Sellberg C, Lindmark O, Rystedt H (2018) Learning to navigate: the centrality of instructions and assessments for developing students' professional competencies in simulator-based training. *WMU J Marit Aff* 17:249–265. <https://doi.org/10.1007/s13437-018-0139-2>
- Sellberg C, Lindwall O, Rystedt H (2021) The demonstration of reflection-in-action in maritime training. *Reflective Pract* 22:319–330. <https://doi.org/10.1080/14623943.2021.1879771>
- Siemens G (2004) *Connectivism: a learning theory for the digital age*. elearnspace

- Stoker G, Greer J, Clark U, Chiego C (2022) Considering maritime cybersecurity at a non-maritime education and training institution. *Proceedings of the EDSIG Conference* ISSN. 4901
- Tam K, Jones K (2019) Situational awareness: examining factors that affect cyber-risks in the maritime sector. <https://doi.org/10.22619/ijcsa.2019.100125>
- Tam K, Hopcraft R, Moara-Nkwe K, Misas JP, Andrews W, Harish AV, Giménez P, Crichton T, Jones K (2021a) Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. <https://doi.org/10.4236/jtts.2022.121001>
- Tam K, Moara-Nkwe K, Jones KD (2021b) The use of cyber ranges in the maritime context: assessing maritime-cyber risks, raising awareness, and providing training. *Mar Technol Res* 3:16–30. <https://doi.org/10.33175/mtr.2021.241410>
- UOB, U. O. B. (2022) Constructivism [Online]. <https://www.buffalo.edu/catt/develop/theory/constructivism.html>: Univeristy of Buffalo. Available: <https://www.buffalo.edu/catt/develop/theory/constructivism.html>. Accessed 10 Dec 2022
- Vu V, Lützhöft M (2020) Human-centred design application in the maritime industry challenges and opportunities. In: Rina, T. R. I. O. N. A. (ed) *Human Factors*. London. <https://doi.org/10.3940/rina.hf.2020.03>
- Vykopal J, Vizváry M, Oslejsek R, Celeda P, Tovarnak D (2017) Lessons learned from complex hands-on defence exercises in a cyber range. 2017 IEEE Frontiers in Education Conference (FIE). IEEE, 1–8. <https://doi.org/10.1109/fie.2017.8190713>
- Wahl AM (2020) Expanding the concept of simulator fidelity: the use of technology and collaborative activities in training maritime officers. *Cogn Technol Work* 22:209–222. <https://doi.org/10.1007/s10111-019-00549-4>
- Wahl A, Kongsvik T, Antonsen S (2020) Balancing Safety I and Safety II: learning to manage performance variability at sea using simulator-based training. *Reliab Eng Syst Saf* 195. <https://doi.org/10.1016/j.res.2019.106698>
- Watson J (2001) Social constructivism in the classroom. *Support Learn* 16:140–147. <https://doi.org/10.1111/1467-9604.00206>
- Windschitl M (1999) The challenges of sustaining a constructivist classroom culture. *The Phi Delta Kappan* 80:751–755

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Paper IV

CERP: A maritime cyber risk decision making tool

CERP: A Maritime Cyber Risk Decision Making Tool

E. Erstad¹, R. Hopcraft², J.D. Palbar² & K. Tam²

¹ Norwegian University of Science and Technology, Ålesund, Norway

² University of Plymouth, Plymouth, United Kingdom

ABSTRACT: An increase in the complexity of systems onboard ships in the last decade has seen a rise in the number of reported maritime cyber-attacks. To tackle this rising risk the International Maritime Organization published high-level requirements for cyber risk management in 2017. These requirements obligate organisations to establish procedures, like incident response plans, to manage cyber-incidents. However, there is currently no standardised framework for this implementation. This paper proposes a Cyber Emergency Response Procedure (CERP), that provides a framework for organisations to better facilitate their crew's response to a cyber-incident that is considerate of their operational environment. Based on an operations flowchart, the CERP provides a step-by-step procedure that guides a crew's decision-making process in the face of a cyber-incident. This high-level framework provides a blueprint for organisations to develop their own cyber-incident response procedures that are considerate of operational constraints, existing incident procedures and the complexity of modern maritime systems.

1 INTRODUCTION

Considering the global maritime cyber risk landscape, the likelihood of maritime digital systems becoming the target of a cyber-incident has increased in recent years [1]. Research indicates that critical onboard systems are susceptible to compromise by both accidental actions and deliberate interference [2]. There are currently several approaches to managing these threats. Firstly, the UN Specialised Agency the International Maritime Organization (IMO) has provided high-level requirements and recommendations for cyber security on board ships [3, 4]. Secondly, one of the largest global shipping associations BIMCO has provided a maritime cyber risk management-specific framework for preparing against the cyber threat on an organisational level [5]. Thirdly, the International Association of Classification Societies (IACS), has recently published two new

Unified Requirements (UR) considering cyber resilience for ships, namely "E26 Cyber resilience of ships" and "E27 Cyber resilience of on-board systems and equipment". As IACS consist of the largest class societies in the world, covering a majority of the world's fleet, these URs will have a worldwide impact [6]. However, with these requirements only being implemented on new builds from 1st January 2024, the realisation of these impacts will be a long time coming.

All the above documentation is designed to aid shipowner companies in the management of the risks they face due to connected technology. However, on board ships, the cyber risks are still being handled pragmatically and by improvisation, as seafarers currently have little to no formalized education about the cyber risks they face [7]. Thus, there is a need for operational tools which can be used by the crew in

response to cyber incidents that are considerate of the organisational management processes. It is therefore vital for management to provide procedures that allow the crew to be able to recognise, respond and recover effectively from a cyber incident, whether the incident is deliberate or accidental.

Developed through engagement with a large offshore operator and a national coastal administration, this paper proposes a maritime cyber risk decision-making tool, the Cyber Emergency Response Procedure (CERP). Based on an operational flowchart, the CERP intends to serve three purposes. Firstly, it provides a blueprint that allows organisations to include cyber incident response within their standard incident response procedures. Allowing the development of policies and procedures that are considerate of processes and practices already in place. Secondly, it provides a high-level decision-making tool that guides crew through the response to a cyber incident. This tool guides the crew through the initial identification of a cyber incident, and managing its symptoms and outcomes using standard documentation found on board. Thirdly, the CERP sets out to demonstrate the need for, and procedure for attaining, external support in the face of a cyber-incident the crew cannot handle independently.

The rest of the paper is as follows. Section 2 will explore the current approach to current maritime incident response and cyber incident response, justifying the use of a flowchart like the one presented in this paper. Section 3 will present the CERP and demonstrate its implementation through the use of examples. Section 4 will explore the future work that would be required to effectively implement the CERP into maritime operations. Section 5 will conclude by arguing that the CERP is a vital first step on a longer road to effective emergency response to maritime cyber incidents.

2 MARITIME AND CYBER INCIDENT RESPONSE

The response to maritime incidents is heavily driven by regulatory bodies and international requirements. As such, this section will start by introducing the current maritime incident response and some of the tools, like checklists, that have been standardised in an attempt to aid that response. The section will also investigate several of the key cybersecurity standards that provide some insight into the development of an appropriate cyber incident response. Finally, the section will explore how the sector is currently coping with maritime cyber risk and lay the foundations of how the work of this paper can enhance that response.

2.1 Maritime incident response

The current response to a maritime risk event is illustrated in Figure 1, whereby in the event of an incident the primary objective is to ensure the safety of the vessel and crew through the use of incident procedures. If completed correctly this should lead to the safe conclusion of the incident, whereby operations will continue as normal, or in a reduced mode. For simplicity, this paper will adopt the

following definitions. Returning to normal operations means that the incident has not limited the operation of the vessel and no further action would be required. Reduced mode covers all other outcomes including the need to gain outside assistance in order to return to normal operations.

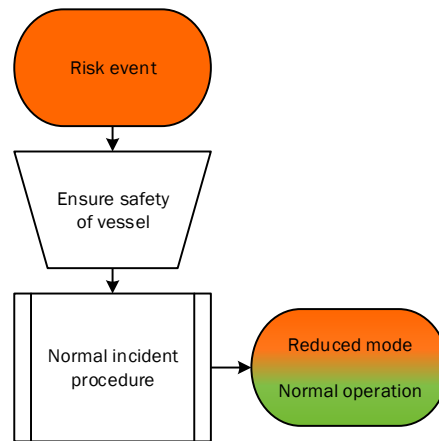


Figure 1. Traditional incident management

As the UN regulator charged with governing the maritime sector, the IMO has developed a variety of regulatory frameworks to improve the safety and security of the sector [8]. The framework most relevant to this article is the International Safety Management (ISM) Code [9], which is mandated under Chapter IX of the International Convention for the Safety of Life at Sea (SOLAS) [10]. The primary aim of the ISM Code is to guarantee, preserve and embed maritime safety and pollution prevention into everyday maritime operations [11]. One particular requirement of the ISM Code obligates companies, and their vessels, to implement, and maintain, a Safety Management System (SMS). Failure to implement an SMS will result in the vessel being unable to obtain its Safety Management Certificate (SMC) and subsequent Document of Compliance (DoC), hindering its ability to operate.

A compliant SMS provides crew with measures to respond at any time to accidents, hazards, and emergency situations, such as fire, grounding, and collision. Through the use of risk assessments, these measures are adapted by each company to be considerate of operational constraints and organisational structure. As part of this process, companies should identify response procedures to emergency situations, and establish drills and exercises to practice them [9]. For the offshore operator the authors engaged with, these drills were on a trimonthly basis and were complementary to other safety drills, like fire or evacuation.

Part of the response procedures and plans include the use of checklists that detail the process through which the expected, and essential, actions should be taken to manage the incident [12]. For example, see Figure 2 which details the contents of the checklist action plan that is to be used in response to a suspected ransomware attack.

Cyber Security - IT Action Plan		
Title Cyber Security - Ransomware		
Description A ransomware attack is easy to recognize, as it holds important files or data hostage. This means that your files will become inaccessible. For example, if you try to open a word document, it will ask for an encryption key, but you must pay the ransom in order to get it. In most cases there is a pop-up window, advising you about the infection and how to pay the ransom		
Immediate action plan		
Action	Complete	Comments
Turn off equipment to minimize the spread of the infection through the network	Yes	<input type="checkbox"/>
	No	<input type="checkbox"/>
	N/A	<input type="checkbox"/>
Immediately power off an disconnect affected systems from the onboard network until further investigation	Yes	<input type="checkbox"/>
	No	<input type="checkbox"/>
	N/A	<input type="checkbox"/>
Contact ICT Department for further investigation, coordination and support	Yes	<input type="checkbox"/>
	No	<input type="checkbox"/>
	N/A	<input type="checkbox"/>

Figure 2. Example maritime checklist

As the example illustrates, each checklist is designed for a specific incident, in this case, that is ransomware, but others include sensor failures or fire. The checklist provides a brief description of the risk to outline the parameters that this checklist is appropriate for. The final, and most important element is the action plan, which provides clear steps that the crew should take in response to the incident. These actions should be developed in collaboration with both crew and onshore management to ensure the response is both appropriate to the operations and considerate of the existing organisational policies and procedures.

2.2 Cyber incident response

Cyber security and information security have gone hand-in-hand for many years. To this end, there are a number of key documents, both regulations and standards, that have been published to provide insight into improving the cyber security of digital systems. The ISO 27000 series, consisting of multiple standards, are one of the most iconic within the domain. The introductory ISO 27000 provides the high-level terms of reference for the security management of any system that collects, processes, stores and transmits information [13]. ISO 27001 provides the requirements for establishing, implementing, maintaining, and improving such information security management systems. These requirements include the establishment and practice of procedures that allow for a quick, effective, and orderly response to information security incidents [14]. In section 5.24, ISO 27002 provides more details on the development of incident plans. The standard argues that organisations should establish plans that are considerate of the organisation's specific risks, capability for detection and response, as well as ensuring appropriate training is identified, and delivered to those expected to respond [15].

Arguably the ISO 27000 series focuses on Information Technology (IT) systems and not the Operational Technology (OT) systems commonly found onboard ships. However, many of these OT systems are underpinned by IT systems and require accurate and reliable data (i.e., information) to operate effectively. Therefore, high-level security

requirements, like response plans, are easily transferable between the IT and OT space. Whilst standards are useful for providing guidance for the development of incident response practices, they are only voluntary requirements.

In 2016, the European Commission published the Network and Information Security (NIS) Directive (EU Directive 2016/1148), which lays down requirements that certain organisations within the European Union must adhere to in order to raise the level of security of network and information systems [16]. At the start of 2023, the EU Commission published NIS2 which will replace the original NIS Directive when it enters into force in 2024 [17]. Within NIS2, there are clear requirements for organisations defined as either "essential" or "important" to have cyber incident response plans. These plans themselves must include reporting mechanisms of incidents to the national authorities. Again, highlighting how cyber response procedures do not only require the involvement of the operator but often include the involvement of external stakeholders.

The above documents, whilst reiterating the importance of having cyber incident response plans do not provide clear details on what these plans should include aside from the potential need to report. The National Institute for Standards and Technology (NIST) Cybersecurity Framework [18], whilst again having an IT focus, does provide some details on what these plans should contain with the "Respond" function. Several activities are particularly relevant to the context of this paper. Firstly, personnel should know their role and the order of operations in response to an incident. Therefore, the availability of checklists detailing procedures is a useful tool. There should also be coordination between stakeholders, both internally and externally, to ensure an effective response.

2.3 Maritime cyber incident response

The maritime industry has for a long time been vulnerable to cyber security risks, and over the last few years regulations and requirements have been implemented to reduce these risks. Whilst this resolution marks the formal need for organisations to consider cyber risk, arguably others had been pushing this approach for many years prior. For example, in 2011 the European Union Agency for Cybersecurity (ENISA) published one of the earliest reports highlighting the sector's cyber security risks and the need for plans to be developed [19]. In 2016, the maritime cyber security discussion intensified with a plethora of documents calling for more action were published. Firstly, classification society DNV published their Recommended Practice "Cyber security resilience management for ships and mobile offshore units in operation" [20]. Secondly, IACS published "IACS-166 Recommendation on Cyber Resilience" [21]. Thirdly, BIMCO published the first version of the "Guidelines on Cyber Security Onboard Ships" [22]. Such were the popularity of these documents they have all since been updated, with the BIMCO guidelines now on their fourth edition [5].

Following increasing pressure for action from its membership, the IMO published "MSC-FAL.1/Circ.3 –

Guidelines on maritime cyber risk management" [3], which provides high-level recommendations on maritime cyber risk management. The following year, after intense discussion the IMO ratified MSC.428(98), making cyber risk management a mandatory element within a ship's SMS [4]. This requirement meant that from 1st January 2021 in order to obtain their DoC, shipowners were required to consider their cyber risks within their SMS and subsequently develop plans and procedures to manage those risks.

Both these IMO documents argue that the sector should consider "industry best practice" when addressing cyber risk. Thus, the IMO recommends operators consider the NIST Cybersecurity Framework, the ISO 27000 series and the BIMCO guidelines as a way to inform their practices. In light of the entry into force of Resolution MSC428(98), the ISO has released ISO 23806:2022, which focuses on cyber safety for ships and marine technology [23]. Again, like the other documents, there are few details in the specifics of cyber incident response. However, the standard does present a high-level cyber safety risk assessment that allows the company to determine the specific risks that they face and mitigate against those.

Some states, like the USA, have produced documentation outlining their expectations for ships that are compliant with Resolution MSC.428(98). Produced by the US Coast Guard (USCG), a Work Instruction (WI) entitled "Vessel Cyber Risk Management" (CVC-WI027) stipulates the expectation that all companies should maintain a Vessel Security Plan alongside the SMS, both of which should include cyber risk [24]. These plans should include a training element to ensure crew are able to respond effectively to a cyber incident. The WI also provides some details on what that response should look like, including the need to request assistance from Coast Guard Cyber Protection Team and Port State Control Officer when appropriate.

The previously listed documents focus on developing cyber incident response plans for ships that are currently operating. As mentioned in Section 1, IACS has been proactively developing new cyber risk management requirements for new builds post-2024. Both UR E26 (cyber resilience of ships) and UR E27 (cyber resilience of ships equipment) stipulate that all new builds classified by an IACS member should have an incident response plan [25, 26]. These plans should "...contain documentation of predetermined set of instructions to detect, respond to, and limit consequences of incidents..." [25, page 18]. As per UR E27, these plans should be developed considering the vessel's operational requirements as well as key information available from the manufacturer.

Therefore, whilst maritime cyber incident response forms part of the mandated requirements for ships, there is still little information available as to what these plans should include. What is clear, is that failure to comply with the development of cyber response instructions, and drills to test them, could lead to non-compliance which would have a negative impact on the operation of the vessel. To ensure compatibility with current practices these new plans should resemble the existing documentation for

incident response. Thus, these plans and instructions should take the form of checklists and flowcharts which support the decision-making process of crew during incidents.

3 A CYBER INCIDENT DECISION SUPPORT TOOL

The previous sections have discussed there is little work currently being done in applying the response to cyber incidents to maritime operations. Therefore, the core aim of this paper is to introduce a maritime cyber incident response framework that can aid organisations in the development of their own response plans that are considerate of the company-specific nuances of their operations, systems, and crews.

In keeping with the traditional methods as these represent both best practice, and the most effective methods of responding to maritime incidents, the authors considered the development of a checklist that would provide details on the handling of a cyber incident. However, following discussions with a variety of stakeholders, including a large offshore operator and coastal administration, it was decided that in isolation these checklists would be of limited benefit. What was clear from these discussions was that crews and organisations, while capable of creating and completing checklists, do not fully understand the correct procedure for dealing with cyber incidents at large. Thus, the authors decided to develop a cyber risk decision support tool that fulfils the three purposes listed in Section 1:

1. Act as a blueprint for organisations to include cyber incident response within their existing response procedures;
2. Provide high-level decision support to crews responding to a cyber incident;
3. Demonstrate the role that external support will play within cyber incident response.

The decided format for this support tool, mimicking the norm within the sector, is a flowchart identified as the CERP (Cyber Emergency Response Procedure). As argued by [27], flowcharts provide a visual representation of the procedures allowing crew to address risks rationally and systematically.

3.1 *Cyber Emergency Response Procedure (CERP) flowchart*

By introducing the maritime cyber risk decision support framework in this way, the authors emphasize that the handling of cyber risk shall not be prioritized before safety critical incident processes. Aligned with the requirements of Resolution MSC.428(98) [4] cyber risks should simply be included in the existing incident handling procedures, as any other risk, such as fire or flooding. The safety of the vessel, crew, and the environment are, as always, the priority.

Remembering Figure 1 that presented a simplified emergency response procedure on board. Figure 3 takes this one step further and illustrates how the crew should initiate the CERP if there is a "cyber" element to the incident. In some situations,

particularly time-critical incidents, it may not be possible to initiate the CERP immediately. Therefore, the crew's first step should be to ensure the safety of the ship, crew, and environment before attempting to initiate the CERP. For example, consider the following ransomware scenario.

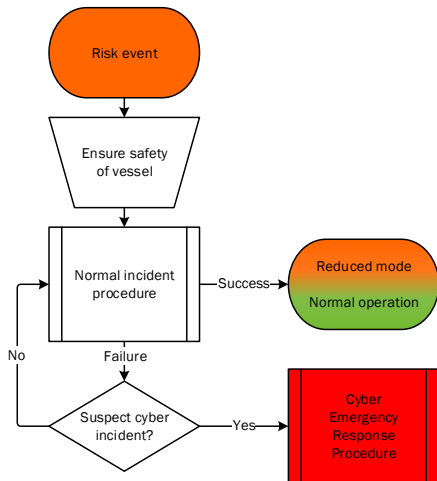


Figure 3. Traditional incident response expansion to include cyber incident response.

A vessel is currently underway and suddenly all the bridge equipment screens display an image saying all their systems are encrypted until a ransom has been paid. The crew realise that this means that they have now effectively lost control of the steering and propulsion systems of the vessel. The crews' response to this scenario, whilst clearly a cyber incident, has two different potential routes depending on the current operational environment. If this scenario were to occur whilst the vessel was transiting open seas then, as long as there is no immediate risk to the crew, ship or environment, the crew could initiate the CERP. However, in the same scenario but the vessel is now transiting a busy Traffic Separation Scheme (TSS), the crew would need to ensure the safety of their ship and crew as well as others before initiating the CERP. In this case, it would be to manually take control of the vessel and remove themselves from danger, and eventually alert vessels in the vicinity following their standard incident procedures. For example, by the use of lights, horn, Automated Identification System, Global Maritime Distress and Safety System (GMDSS) and a PAN-PAN broadcast via VHF (i.e., initiating PAN PAN procedure by voice via VHF). Once the ship and crew are safe then the CERP can be initiated.

The flowchart itself is developed considering ISO 5907-1985 [28], which provides standardised symbols and definitions for flowcharts. Whilst the standard does not fit the author's purpose directly, the paper has adopted the approach under the description of a "Program Flowchart", whereby it details the procedural sequence of operations within a program. Whilst this type of flowchart is best suited for a computer program, in a simplified format it can appropriately be used to visualise the procedure a human operator can follow within their own system of working.

Figure 4 illustrates the CERP developed by the authors and verified with experts within the maritime sector. The CERP has 4 distinct phases, which also relate to specific divisions on board and ashore. The first labelled Operational Team is the initial phase of the CERP. The operational crew, bridge, or engine room have already determined that there is a potential cyber incident occurring and that the safety of the vessel is currently not at risk. Within this initial phase, crew would be expected to identify the risk (M1), this might be as simple as identifying the potential system(s) at fault, or potential causes for the consequences presented within the incident. Once the system(s) at risk have been identified then the crew need to determine whether they can mitigate the risks, by either using a manual/alternative measure (M2) or isolating the system (M3). It is not essential that both are achieved, but it could help reduce the risk of the incident spreading to other systems. Companies would need to provide procedures for how to achieve manual operation and isolation of systems, with acceptable alternatives listed.

The second phase labelled as the Onboard Technical Response, is the onboard crew's initial attempts to manage and mitigate the cyber incident. Once the crew have identified the systems at fault, they should be following prepared checklists and procedures in troubleshooting the affected devices (Doc1). In some cases, this will work, and the ship can return to normal operations (T2). However, if the crew consider there is a possibility that the problem is propagated to other systems, they should restart the CERP for that particular system. This should continue until crew have exhausted all possible solutions.

Once this exhaustion has occurred onboard, the crew should determine that contacting the Shoreside Support Team for technical support is the next option (D4). These teams will contain a greater expertise in cyber incident handling or have access to this expertise (contact with manufacturer support). In some cases, this shoreside team may be able to solve the incident remotely (T3), or by providing instructions to the crew, who will either succeed (T2) or fail. On failure, it may be determined that the only possible solution would be to initiate the company's repair and replacement procedures (P2). In these situations, the Master must consider the integrity of the DoC. For example, if the ship only navigates using an Electronic Chart Display and Information System (ECDIS) and does not have updated paper charts, then the vessel could be deemed un-seaworthy and must, in the worst case, seek emergency harbour to rectify deficiencies in the DoC.

There are two important points of note that the crew should be aware of during the implementation of the CERP. Firstly, if the situation of either the ship's operational environment or incident changes, then the crew should reassess the safety of the ship and determine whether preventative measures need to be taken immediately before proceeding with the CERP. Secondly, the three termination points (T2, T3 and T4) are labelled as reduced mode/normal operations. This is because there will be situations whereby the risk has been mitigated enough to an acceptable level that operations can continue, just at a reduced level.

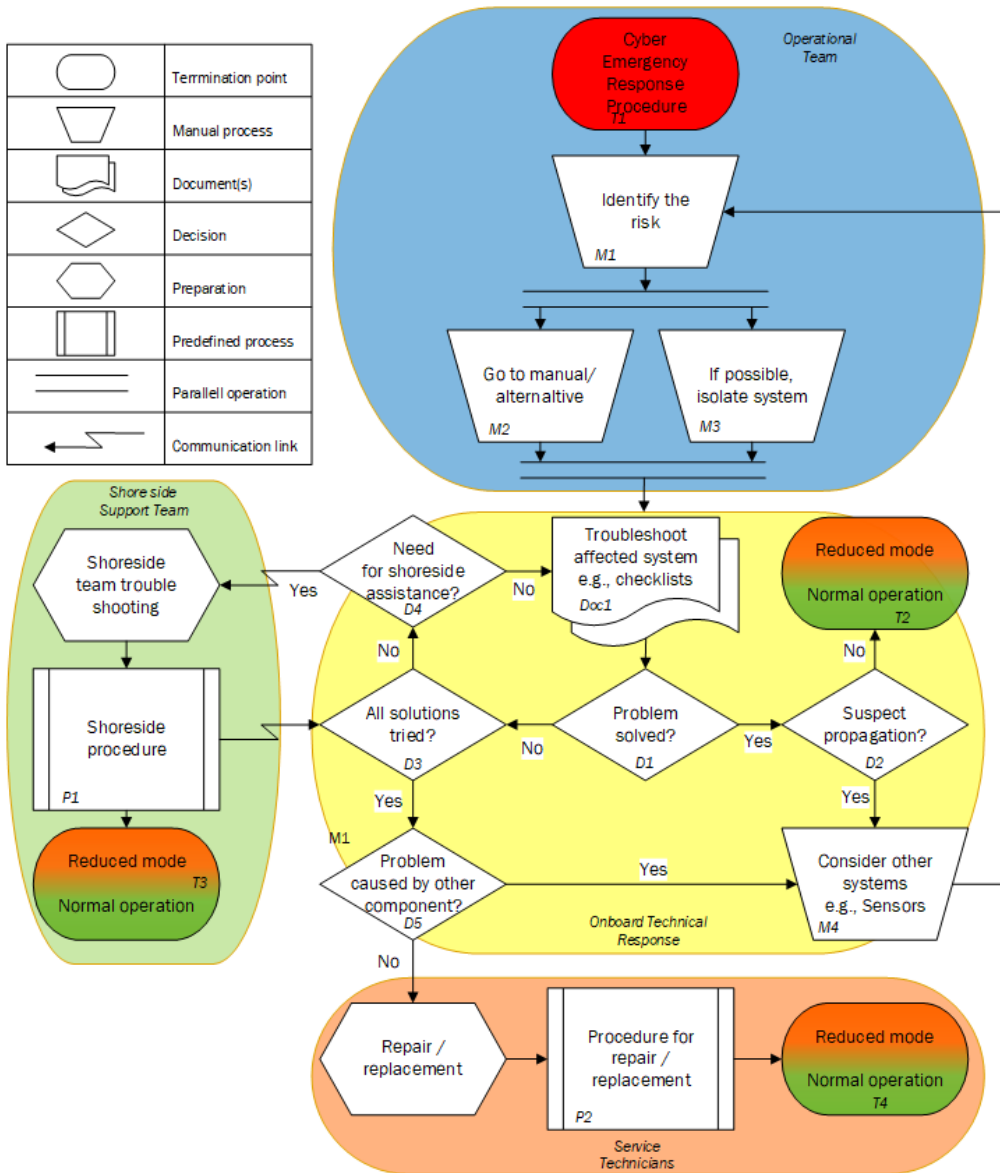


Figure 4. Flowchart for the Cyber Emergency Response Procedure (CERP)

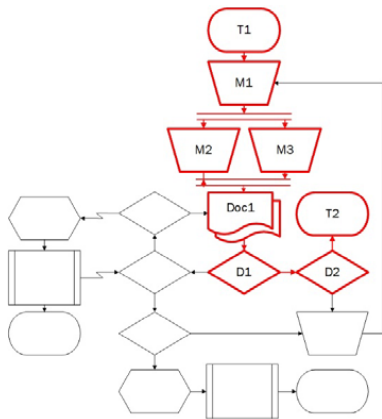
3.2 The CERP in practice

This section will present three scenarios that demonstrate how the CERP can be utilised by companies and crews to respond to cyber emergencies. The scenarios are written to be generic in order for the reader to adjust each scenario to their own experiences and operations. For instance, the bridge scenario could target the Multi-Function Displays (MFD) or the Dynamic Positioning (DP) systems. Each scenario will illustrate the route through the CERP that the crew will take (with manual actions notated by M#) to reach each of the termination points (T2, T3 and T4).

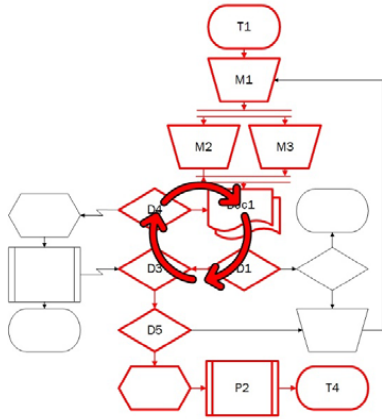
3.2.1 Compromised non-essential device

During normal operations, a computer suddenly displays a ransomware message, and the crew member is unable to access any files on the device. The crew member immediately notifies the Master of the problem. Using the CERP, the Master determines there is no direct impact on safety and instructs the crewmember to remove the network (ethernet) cable to isolate the device (M3). As per the documentation (Doc1), the Master notifies the engineer on board responsible for IT systems of the problem who then takes responsibility for troubleshooting and reporting back to the Master. Having already isolated the device, the engineer reboots the device from a backup and the computer is no longer infected (D1). The

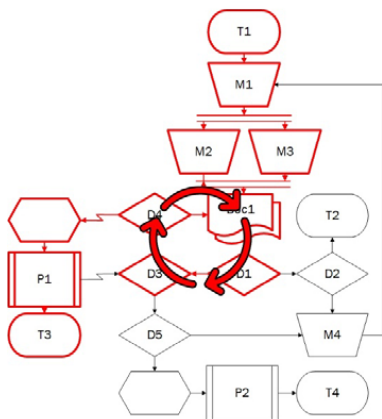
Master confirms with the rest of the crew that no other devices seem to be impacted, so assumes the ransomware has not propagated (D2). Allowing the vessel to continue normal operations (T2).



a



b



c

Figure 5. Implementation of CERP (a: Section 3.2.1, b: Section 3.2.2, c: Section 3.2.3)

3.2.2 Faulty GNSS sensor

During normal operations, the crew are actively using the ECDIS for navigation and determines that the observed position is not corresponding to the other position-fixing methods (i.e., visual and radar). The officer of the watch notifies the Master of his concerns. The Master determines that whilst there is no risk to the safety of the ship, ECDIS is a critical system so corrective action is required. As it is not possible to isolate the ECDIS, the Master instructs crew to use other position-fixing methods and posts an extra lookout as an alternative to the device whilst it is being troubleshooted (M2). The crew then follow the troubleshooting checklists for ECDIS (Doc1). After several unsuccessful attempts, the crew cannot solve the problem (D3) and determined another device might be at fault (D5). Crew determine that it is a Global Navigation Satellite System (GNSS) sensor causing the issue (M4), so begin the CERP for that device. After unsuccessful attempts to troubleshoot the GNSS sensor (Doc1), the Master instructs the crew to use the backup sensor and with support from shore initiates the decommission and replacement procedures for the faulty GNSS sensor (P2), allowing the ship to continue operations at in a reduced mode (T2).

3.2.3 Engine control room (ECR) systems

When entering the Engine Control Room (ECR) the Chief engineer notices an E-cigarette plugged into a USB port of the control panel. Unsure if the device has transferred malware onto the control systems, the Chief Engineer immediately notifies the Master of the situation. The Master determines that all systems are fully operational so deems it not appropriate to take alternative measures or isolate a system (M2, M3). The engineer considers the appropriate checklists (Doc1) which involves the notification of the shoreside team (D4). The shoreside team implements their own procedures for remotely accessing the ECR systems and running their own security checks (P1). They determine that the systems have not been compromised, so instruct the vessel to continue operations as normal (T3).

3.3 Roles and responsibilities

As per the requirements of a ship's SMS, all crew should be aware of their responsibilities when responding to an incident [9]. Furthermore, as this paper has argued the response to a cyber-incident might require the involvement of shoreside personnel. Therefore, all personnel, both on board and ashore need to be aware of their responsibilities to ensure the most effective response to an incident whilst maintaining the highest level of safety.

3.3.1 Service technicians

The management level onboard a ship, primarily the Master and Chief Engineer, hold the highest level of responsibility for responding to incidents. While both must work seamlessly in response to a cyber incident, both have slightly different roles to play. The Master's primary role is to ensure the continued

safety of the vessel and its crew with an operational focus. It is the Master who completes the mental risk assessment to determine if the ship is in a safe enough position and/or state to initiate the CERP, or if other action is required prior to initiation. The Chief Engineer, on the other hand, whilst still having a responsibility for ensuring safety, will primarily be focused on providing technical support during an incident and completing mental risk assessments regarding the criticality of systems.

In both instances the management level on board will primarily fulfil a coordination role, pulling on their substantive experiences and training to direct other crew members in their response. They would also be the ones responsible for contacting shoreside assistance, as required. These personnel would also be expected to synthesise the information from all sources across the ship and ashore and disseminate that back to others in the form of instructions or information.

3.3.2 *Technical team on board*

The technical team would be those personnel who have clearly defined areas of responsibility which play a critical role in the safe operation of a vessel. These personnel include navigation officers and members of the engine department. These personnel hold several critical roles in the response to cyber incidents. Firstly, as they are the operators of the technical equipment (hands-on), they are likely to be the first to detect a problem. The second responsibility they have is to ensure they communicate this problem to the management level, along with any other operational information that could influence the response. The third and final role that these personnel will fulfil is the implementation of the response. Take the example in Section 3.2.2, the technical operator would be expected to implement the troubleshooting documents when instructed by the management level and report back on its success.

3.3.3 *Shoreside assistance*

With the complexity of many maritime systems and the plethora of attack vectors, it would be surprising if the crew on board the vessel were able to respond to all cyber incidents independently. Therefore, shoreside assistance should be available when needed.

3.3.3.1 *Company support team*

Operators should recognise that whilst capable of responding to many incidents, the crew are operational experts, not technical experts. Whilst many operators have a team, commonly termed "IT Support", they may lack the operational knowledge and skills like communication, required to respond to incidents on a moving vessel [29]. Therefore, operators should ensure a shoreside team that has the correct operational and technological knowledge and skills is able to provide support to the crew when needed. This team will have their own set of procedures for responding to a cyber incident. These procedures may include the remote access and maintenance of a system or the communication of

more detailed, and technical, instructions back to the vessel for the crew to implement.

3.3.3.2 *Service technicians*

The second part of the shoreside assistance includes service technicians, either from 3rd party service providers employed by the operator to maintain the vessel systems, or members of the technical support teams from the original equipment manufacturers. Again, operators should recognise that their technical staff may require the assistance of those more intimately aware of the systems to enable an effective response. Operators have the responsibility to ensure that, when involving external support, information is passed to these teams so that they can provide a response which is considerate of the current operational requirements of the vessel. The external technicians have a responsibility to comprehend this information and utilise the knowledge within their own organisations to facilitate an effective response to an incident.

3.3.3.3 *Other shoreside assistance*

Whilst outside of the scope of this paper, it is also important to highlight that there might be other stakeholders who would be involved in the response to a cyber incident onboard. This could include entities like the coastguard, military (or equivalency), or other operators involved in the rescue and recovery of the vessel. All these entities have different roles to play, and operators should be aware of which situations would require their involvement and have procedures in place to initiate that involvement.

4 IMPLEMENTATION OF CERP INTO MARITIME OPERATIONS

The previous section illustrated the CERP and demonstrated how the CERP can function in a practical, shipboard environment, affected by a cyber incident. However, to include the CERP fully and safely into maritime operations, several aspects must be accounted for. The CERP must be tested and verified in order to prove the integrity of the flowchart, as well as supporting documentation and discussion of Cyber Emergency Response Teams (CERT) training must be considered.

4.1 *Testing and verification of CERP*

Two perspectives need to be considered for the testing and verification of the CERP. Firstly, there is the verification of the CERP itself. Secondly is the verification of the organisation's implementation of the CERP.

In terms of validating the overarching CERP framework, the authors presented the framework to experienced operators who provided feedback and comments. All of which have been implemented into the final design, ensuring it is accurate at an operational level. To further validate and test the framework more work must be done by putting the

CERP into practice either via workshops or simulation exercises with experienced crews. The use of these simulated exercises will determine whether the CERP is a useful decision-support tool for crew to understand their response. However, through the use of the three scenarios in Section 3.2, the authors can demonstrate how the CERP works in application, providing a soft verification of results. Once further validation has occurred it will allow the CERP to fully fulfil its core purposes.

For an organisation using the CERP as a blueprint for their own cyber incident response, it should be tested at all levels of maritime personnel (support, operational and management). To ensure effective preparation and response, both shoreside and shipside personnel should participate in joint training drills allowing technical and operational knowledge to be shared. These drills will also illustrate how decision-making processes may differ across the response team. Thus, informing the development of organisational policy. What is more, through these drills and practices the implemented CERP can be amended and adapted as required by the organisation. Coupling these results with a detailed cyber risk assessment methodology like the NIST Cybersecurity Framework will allow organisations to understand crucial systems, assets, threats and other possible mitigation measures.

Consequently, the utilization of this tool will guide the user through the collection of key information about the cyber incident, affected systems, and operational status. The application will be similar to the NIST Cybersecurity Framework [18], which is recommended by the IMO, as it provides companies with a methodology that allows them to identify crucial systems and assets, assess systems threats, and provide needed mitigation procedures. This information can then be used to inform the decision-making process of the crew in response to an incident, to either restore the system enabling a return to normal operation as soon as possible, or a safe enough temporarily reduced mode.

4.2 *Development of checklists*

As seen in Section 2.1 it is important for operators to follow industry guidelines as well as comply with regulatory requirements addressing cyber security [5]. One such requirement is the development of response plans. Whilst the CERP represents a part of that plan, this paper has also identified checklists as an essential cognitive aid that has many benefits to incident response. In safety-critical industries, checklists have been described as a 'fourth crew member' [30]. Thus, when designed correctly checklists help users recall critical steps, reduce the stress experienced during an incident, as well as maintain effective teamwork [31].

The BIMCO Cyber Workbook provides several examples of checklists which include guidance on the initial response, notification, and investigation of cyber incidents on board [32]. However, these are generic and should be used for reference by organisations as they develop their own which are considerate of their operation-specific risks, including the different IT and OT systems. This also includes

engaging with other key stakeholders like system operators or manufacturers.

It is also important to note that whilst checklists are useful, they do have limitations such as they set out explicitly the expected actions the crew should take. However, from discussions with industry, the authors noted that in response to real-world incidents crew often act independently. This deviation, whilst not exactly desirable, might in certain circumstances be the most appropriate response.

Therefore, to help ensure these checklists are appropriate they should be implemented during drills and practices. This has two benefits, like the CERP, firstly it allows the organisation to determine if changes are required, and secondly, it allows crews to become familiar with their contents [33]. What is more, practicing these checklists allows the practice itself to be reflected upon. As philosopher John Dewey argues, "We do not learn from experience... we learn from reflecting on experience" [34].

4.3 *Development of cyber response teams*

The roles and responsibilities of people engaging in cyber incident handling are of importance, as emphasised in Section 3.3. The paper has argued that to ensure effective incident response dedicated cyber response teams both onshore and onboard should be developed.

On the shoreside, the maritime industry is increasingly using Security Operation Centres (SOC) [35] which can benefit from implementing non-maritime cyber security specialists [36]. As mentioned in the USCG WI, the USCG have already implemented Cyber Protection Teams, which also support the maritime sector, not just land-based companies [24]. BIMCO has put the NIST framework into a maritime context and specified that a cyber emergency response team (CERT) should be available to provide timely support to the Designated Person Ashore (DPA) [5, page 53]. In IACS UR E26, a cyber emergency response team is not specifically mentioned. However, the document does require that companies implement procedures for managing cyber security incidents, and designate personnel with the appropriate training and experience to respond to such incidents [25].

Regarding ships, it is not unreasonable to argue that the lines of communication to shoreside support may be unavailable/compromised. Furthermore, with seafarers fulfilling the role of operator they are expected to bring order to an unnormal situation [37]. Therefore, the authors argue that there should be a dedicated CERT on board similar to the dedicated firefighter on board. This crew member should be provided with specific incident response training, which goes beyond cyber awareness. However, as a 2022 study found, there is a limited amount of formalized training considering cyber risk in the industry [7]. Thus, operators should develop training that provides key knowledge and skills regarding cyber response, that is considerate of the organisation's operations.

4.4 Training

As argued throughout this paper, certain skills are required to implement the CERP. As the CERP (Figure 4) illustrates there are four teams required for effective response. Each of these teams fulfils different roles within incident response therefore need different skills in order to handle cyber emergency situations. Thus, different training modules will need to be developed. As per roles and responsibilities, at the management level, the general responsibility relies on the Master's and Chief Engineer's operational experience and team management skills. Therefore, training must provide a detailed understanding of cyber risks, and mitigation measures to allow them to identify potential incidents and direct the appropriate resources in response. At an operational level, the onboard technical response team will need specific details regarding systems, their dependencies and troubleshooting methods. For the shoreside teams, this training should include the skills required to remotely implement measures or communicate those mitigations to the crew in the language they understand.

As argued drills and practices form a vital role in verifying and testing procedures, they also offer the opportunity for personnel to gain familiarization with the skills they need to deal with abnormal situations. Thus, these drills can provide a dual purpose in training, allowing personnel to not only implement response plans but also develop experiences which can help inform their decisions at a later date.

5 CONCLUSIONS

This paper has investigated traditional maritime incident handling, traditional cyber incident handling and maritime cyber security handling. Many of the approaches discussed argue for the need for cyber incident response plans but fail to provide clear details of what these should contain. In response, by analysing incident handling and taking a pragmatic approach in collaboration with maritime industry actors, the authors propose a maritime Cyber Emergency Response Procedure. As crew on board a ship is traditionally known to take a pragmatic approach to problem-solving, the flowchart provides the crew with a visual representation of a cyber problem-solving approach, than a text-based approach.

This flowchart serves three purposes. Firstly, the CERP acts as a blueprint for organisations to include cyber incident response within their existing response procedures. The proposed CERP is also considerate of the traditional incident response and builds upon and adapts best practices to include elements relevant to cyber incidents. Secondly, the CERP in its current format provides a high-level decision support tool for crews, providing enough details of what steps they should be taking to safely manage a cyber incident. These steps, again considerate of normal incident response procedures, include the involvement of shoreside support and the requirement to consider whether the incident has propagated to other systems. Thirdly, the CERP illustrates where external support from the shoreside might be needed in order to

respond appropriately. This support can come from the technical support teams, equipment manufacturers, or as in the USCG example, the state.

In conclusion, the maritime sector lacks a standardised approach to cyber incident response. By adapting current best practices, the CERP is a vital first step to addressing this issue. However, it is important to note that this is just the first step on a longer road to the effective emergency response to maritime cyber incidents. Further work will be needed to understand the CERP's implementation at an organisational level, as well as the training required to fulfil the roles and responsibilities it highlights. However, the CERP does represent a visual tool that will hopefully start much-needed discussions regarding maritime cyber emergency response.

ACKNOWLEDGEMENT

This paper is partly funded by the research efforts under MarCy and Cyber-MAR.

Maritime Cyber Resilience (MarCy) has received funding from the Research Council of Norway, with project number 295077. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389.

Content reflects only the authors' view, and neither the Research Council of Norway nor the European Commission, nor any project partner is responsible for any use that may be made of the information it contains.

The authors also want to thank the people at the Cyber-SHIP lab, Solstad Offshore ASA, and The Norwegian Coastal Administration for their engagement with this research.

REFERENCES

- [1] NORMA Cyber, "NORMA Cyber Annual Threat Assessment 2022," Norwegian Maritime Cyber Resilience Centre, normacyber.no, 2022. [Online]. Available: <https://www.normacyber.no/news/norma-annual-threat-assessment-2022>
- [2] K. Tam et al., "Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety," 2021, doi: <https://doi.org/10.4236/jtts.2022.121001>.
- [3] International Maritime Organization, MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management, 2017. [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx.
- [4] International Maritime Organization, Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, 2017. [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx. Accessed on: 22.02.2023.
- [5] The Guidelines on Cyber Security onboard Ships Version 4.0, BIMCO, 2020. [Online]. Available: <https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships>
- [6] IACS. "IACS adopts new requirements on cyber safety." IACS. <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/> (accessed 20 February, 2023).
- [7] E. Erstad, M. S. Lund, and R. Ostnes, "Navigating Through Cyber Threats, A Maritime Navigator's

- Experience," 2022, doi: <https://doi.org/10.54941/ahfe1002205>.
- [8] International Maritime Organization. "Maritime Safety." IMO. <https://www.imo.org/en/OurWork/Safety/Pages/default.aspx> (accessed 20 February, 2023).
- [9] International Maritime Organization, International safety management code: with guidelines for its implementation, 2018 edition.; Fifth edition. ed. (ISM-Code). London: International Maritime Organization, 2018.
- [10] International Maritime Organization, SOLAS, Consolidated Edition, 2020 (SOLAS). London: International Maritime Organization, 2020.
- [11] International Maritime Organization. "The International Safety Management (ISM) Code." IMO. <https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx> (accessed 23 February, 2023).
- [12] International Chamber of Shipping, Bridge Procedures Guide. Marisec, 2022.
- [13] ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, ISO, iso.org, 2020. [Online]. Available: <https://www.iso.org/standard/73906.html>
- [14] ISO/IEC 27001:2017 Information security, cybersecurity and privacy protection — Information security management systems — Requirements, ISO, iso.org, 2017. [Online]. Available: <https://www.iso.org/standard/82875.html>
- [15] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, ISO, iso.org, 2022. [Online]. Available: <https://www.iso.org/standard/75652.html>
- [16] Directive (EU) 2016/1148 European Union Parliament, Official Journal of the European Union, 2016. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>
- [17] DIRECTIVE (EU) 2022/2555, European Union Parliament, Official Journal of the European Union, 2022. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1677163438395&from=en>
- [18] Framework for improving critical infrastructure cybersecurity, N. I. o. S. a. T. NIST, 2018. [Online]. Available: <https://www.nist.gov/cyberframework/framework>
- [19] ENISA, "ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR," <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1>, 2011. [Online]. Available: <https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1>
- [20] Cyber security resilience management for ships and mobile offshore units in operation, DNV, standards.dnv.com, 2016. [Online]. Available: <https://standards.dnv.com/explorer/document/0ED73B3209DA42CDA6392BC3946585C9/4>
- [21] Rec 166 - Recommendation on Cyber Resilience, IACS, 2020. [Online]. Available: <http://www.iacs.org.uk/publications/recommendations/161-180/>
- [22] The Guidelines on Cyber Security onboard Ships Version 1.0, BIMCO, 2016. [Online]. Available: [https://www.bimco.org/about-us-and-our-](https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships)
- members/publications/the-guidelines-on-cyber-security-onboard-ships
- [23] ISO 23806:2022 Ships and marine technology — Cyber safety, ISO, iso.org, 2022. [Online]. Available: <https://www.iso.org/standard/77027.html>
- [24] Vessel Cyber Risk Management Work Instruction, United States Coast Guard, <https://www.dco.uscg.mil/>, 2020. [Online]. Available: <https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Commercial-Vessel-Compliance/CVCmms/>
- [25] IACS UR E26 Cyber resilience of ships, IACS, <https://iacs.org.uk/>, 2022. [Online]. Available: <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/>
- [26] IACS UR E27 Cyber resilience of ships equipment, IACS, <https://iacs.org.uk/>, 2022. [Online]. Available: <https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/>
- [27] T.-r. Qin, W.-j. Chen, and X.-k. Zeng, "Risk management modeling and its application in maritime safety," *Journal of Marine Science and Application*, vol. 7, no. 4, pp. 286-291, 2008.
- [28] ISO 5807:1985 Information processing — Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts, ISO, iso.org, 1985. [Online]. Available: <https://www.iso.org/standard/11955.html>
- [29] M. Raimondi, G. Longo, A. Merlo, A. Armando, and E. Russo, "Training the maritime security operations centre teams," in 2022 IEEE International Conference on Cyber Security and Resilience (CSR), 2022: IEEE, pp. 388-393, doi: <https://doi.org/10.1109/csr54599.2022.9850324>.
- [30] P. Greig, A. Maloney, and H. Higham, "Emergencies in general practice: could checklists support teams in stressful situations?," (in eng), *Br J Gen Pract*, vol. 70, no. 695, pp. 304-305, Jun 2020, doi: 10.3399/bjgp20X709373.
- [31] D. L. Hepner et al., "Operating room crisis checklists and emergency manuals," *Anesthesiology*, vol. 127, no. 2, pp. 384-392, 2017.
- [32] BIMCO, International Chamber of Shipping, and Witherby Publishing Group, *Cyber Security Workbook for On Board Ship Use - 4th Edition*, 2023. Livingston: Witherby Publishing Group, 2023.
- [33] F. S. Foundation. "FSF ALAR Briefing Note 1.5, Normal Checklists." SKYbrary Aviation Safety. <https://skybrary.aero/bookshelf/fsf-alar-briefing-note-15-normal-checklists> (accessed 21 February, 2023).
- [34] G. Di Stefano, F. Gino, G. Pisano, and B. R. Staats, "Learning by Thinking: How Reflection Can Spur Progress Along the Learning Curve," *Management Science*, Harvard Business School NOM Unit Working Paper No. 14-093, 2014, doi: <https://dx.doi.org/10.2139/ssrn.2414478>.
- [35] A. Nganga, M. Lützhöft, J. Scanlan, and S. Mallam, "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment," 2022.
- [36] G. Stoker, J. Greer, U. Clark, and C. Chiego, "Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution," in *Proceedings of the EDSIG Conference ISSN*, 2022, vol. 2473, p. 4901.
- [37] E. Erstad, R. Ostnes, and M. S. Lund, "An Operational Approach to Maritime Cyber Resilience," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, vol. 15, no. 1, pp. 27-34, 2021, doi: <https://doi.org/10.12716/1001.15.01.01>.

Workshop report

Maritime Cyber Resilience project

Maritime Cyber Simulator Scenario Workshop report

Erlend Erstad
Marie Haugli Larsen
Mass Soldal Lund
Runar Ostnes

NTNU in Ålesund, 11.02.22

Norwegian University of Science and Technology
Faculty of Engineering
Department of Ocean Operations and Civil Engineering

Document history:

11.02.22 Revision 1 First issue of document



Summary

The 7th of December 2021, the Maritime Cyber Resilience (MarCy) project held a Cyber Simulator Scenario workshop aiming to create a fundament for training to enhance operational maritime cyber resilience.

MarCy is a research project collaboration, between the academic partners Norwegian University for Science and Technology (NTNU), Norwegian Defence University College (NDUC), and the industry partners DNV, Norwegian Hull Club (NHC) and Kongsberg Defence & Aerospace (KDA).

The scope of the workshop was to invite maritime stakeholders and people in the maritime industry to discuss how and if simulator training should be part of cyber awareness training, and what simulator scenarios can be beneficial to implement in such training. The aim was to develop both operational level scenarios for the crew handling ships, and management level scenarios for the shipowners and maritime stakeholders. In addition to this, the workshop led to fruitful discussion how the maritime industry is dealing and coping with cyber threats, and what could be considered as beneficial for cyber training. Real life incidents and experiences was also shared among the participants.

The MarCy project partners and the authors of the report want to express their greatest gratitude for all the participants attending the workshop. The workshop could not have been completed without you. Due to the protection of the privacy for the attendants, no individual level information is given. See more in Section 2.

List of the organizations attending the workshop:

DNV	NTNU – SFI-Move project
Island Offshore	Royal Norwegian Naval Academy
Kongsberg Aerospace & Defence	The Norwegian Armed Forces Cyber Defence
Norwegian Defence University College	The Norwegian Armed Forces
Norwegian Hull Club	The Norwegian Coast Guard
NTNU – COAST project	The Norwegian Coastal Administration
NTNU in Ålesund	The Norwegian Society for Sea Rescue
NTNU in Gjøvik	

1 Introduction

The maritime industry is being digitalized and is constantly changing with new technology. This introduces new types of cyber threats towards navigational equipment which is essential for safe navigation. If a cyber threat occurs on board, the navigators and deck officers are expected to handle the situation, yet there is no standardized training on the topic. Cyber security is not even mentioned in the STCW-convention (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) which is the international baseline curriculum for maritime navigators.

The MarCy¹ project is a “Knowledge building Project for Industry” (KPI), funded by the Research Council of Norway, project number 295077. The MarCy project target cyber security challenges that are specific for maritime digital control systems and maritime operations. The primary objective of the MarCy project is to develop validated means for improving cyber resilience of maritime digital control systems and maritime operations. A part of this is to investigate and develop education and training programs to increase maritime navigators’ and operators’ awareness of, and resilience against, cyber risks. A vital part of nautical education is simulator training. The scope of this workshop was two-folded. The primary objective was to invite maritime stakeholders to take part in a discussion to map out potential cyber threat simulator scenarios to be implemented in maritime training and education, as well as discuss nearby topics, as relevance, plausibility, realism, and handling of the scenarios. The second purpose of the workshop was to collect data for a PhD project which is part of the MarCy project.

Section 1 introduces scope of the workshop as well as how the workshop was performed. Section 2 presents the identified cyber simulator scenarios. Section 3 presents a summary of the discussions of the workshop sessions. Section 4 concludes the workshop report and provides recommendation for future work.

1.1 Workshop information

In addition to facilitate for discussion, this workshop also intended to give the participants an insight into the equipment used in nautical education at NTNU in Ålesund. NTNU in Ålesund have modern, high-end, full mission bridge simulators, delivered by Kongsberg Digital, type K-SIM². The participants were briefed in the simulators before they were exposed to two cyber threat test-scenarios. The test-scenarios were intended for inspirational purpose only. The idea was to stimulate for creativity and engagement of the participants, making them more willing to share ideas and thoughts later in the workshop discussion sessions. Below is a short description of the introduction scenarios.

¹ Read more on the Research Council of Norway website:
<https://prosjektbanken.forskingsradet.no/project/FORISS/295077?Kilde=FORISS&distribution=Ar&chart=bar&calcType=funding&Sprak=no&sortBy=date&sortOrder=desc&resultCount=30&offset=0&Fritekst=marcy>

² Read more on Kongsberg Website:
<https://www.kongsberg.com/no/digital/products/maritime-simulation/k-sim-navigation/>

Introduction to the simulators: All participants were given a tour of the simulator-park at NTNU Ålesund. This included the K-SIM Nautical Educational Simulators, K-SIM Research Simulator, and Offshore Simulator Centre (OSC) Research Simulators. All participants were then put in a Nautical Education and Training Simulator for briefing, prior to the introduction scenarios. The briefing was simple, the different components on the simulator bridge were demonstrated to the participants and the simulation were located in the port of Ålesund. This helped the participants to easily explore the capabilities and limitations of the simulators.

First scenario: The first scenario took place onboard a High-Speed Craft bound from Ålesund to Hareid, which is a real-life voyage for freight of passengers. The participants entered the bridge when it was about 10 minutes remaining of the voyage bound to Hareid. When entering port of Hareid very dense fog occurred, and it should be hard to navigate visually past the narrow molo in the entry point of the port. The vessels radar and ECIDS should not indicate any alarms but were set up with a 160-metre antenna offset, providing a false picture of position for the participants. This means, if the participants would have sailed solely using radar and/or ECDIS, they would have crashed into the molo, if they did not proceed with very low speed.

Second scenario: The second scenario also took place onboard a high-speed craft bound from Ålesund to Hareid. This scenario took place in Breisundet, just west of Ålesund. In Breisundet, a military convoy was coming from west, heading into the Hessafjord, all with active AIS and good radar reflectivity, even though they were hard to see due to dense fog. When sailing south towards Hareid, the participants needed to give way for the convoy, forcing them on a collision course with a frigate with no AIS and no visible radar target. The intended thought was that the radar has been intentionally jammed, making the participant unable to view some targets. This could result in a severe collision or near collision with the frigate.

1.2 Privacy of attendants

This workshop was partly audio recorded. Due to the protection of the privacy for the attendants there will not be mentioned any names or personal information which can be traced back to the individual in this report. The participating organizations will therefore be mentioned and appreciated. The participants in the workshop had given written consent to participate, and the workshop was approved by NSD³, Notification Form 422483. Further information regarding the tape recording of the discussions will be presented in section 3.

For more information, please contact Erlend Erstad, +47 995 00 777 / erlend.erstad@ntnu.no.

³ More information: www.NSD.no

2 Cyber simulator scenarios

This section documents scenarios identified during the workshop. The intention was to define cyber threat scenarios for operational level and management level operators in the maritime industry, which can be trained for in a safe simulator environment. However, the scenario findings are not divided into operational level and management level scenarios, as the scenarios were found to fit both operational and management level, depending on the context of the to-be-developed scenarios. For example, a plausible ransomware scenario will affect both the crew on board and the shipowner, but it will initiate more action on one part, depending on the setting of the scenario. This section is meant to give inspiration to development of cyber threat simulator scenarios, and not to be considered as a product ready to be deployed in a simulator scenario. By operational level scenarios are meant scenarios which are relevant for crew on board a ship bridge. Management level scenarios are more relevant for other maritime stakeholders, such as shipowners, insurance companies and class societies. Below is a list and explanation of the scenario findings:

- Unintentional cyber threat-scenario
 - Remote access is being mentioned as an emerging issue. Uncontrolled remote handling of the maritime digital control systems from shore can cause severe problems for ships. Service providers can potentially connect to the wrong equipment or even wrong ship, when performing intended maintenance. The participants talked about situations where remote maintenance failed and created a possible dangerous situation. Workshop participants discussed experiences with remote operators shutting down generators and other critical ship equipment on an unaware ship in operation. The intention was to perform service on the equipment on an other ship, but the remote operator connected to the wrong vessel-system.
- Intentional adverse actor cyber threat-scenario
 - Adverse actors can have interest in controlling the maritime digital control systems, using it as leverage for ransom. Possible attack surfaces could be malicious USB-flash drives, unsafe mobile phone charging in the affected equipment, or unsafe internet connection. More and more vessels are somehow connected to the internet, and the internet link may not always be safe. These kinds of scenarios can relate directly to a traditional ransomware scenario but targeted against ship critical infrastructure. Possible scenarios and affected equipment can be:
 - Ballast water treatment system – A cruise ship which gets 15 degrees list to either side will have troubles deploying their lifeboats. This potential attack can be a Remote Access Trojan-attack (RAT).
 - Forced blackout of generators – Adverse actor actively shutting down the generators or machine control systems of a ship in a dangerous situation, for example close to rig or in narrow waters. This potential attack can be a Denial-of-Service attack (DoS).
 - Steering gear equipment – Altering the steering gear in a dangerous situation, for example in port or a dense traffic area. “Ever Given”-

- incident is indicated to be a potential cyber threat scenario. This can be both RAT and DoS.
- Dynamic Positioning (DP) System – Same as the two previous mentioned but affecting the DP system. Could be very critical in close to rig operations. Can be both RAT and DoS.
 - Electronic Chart Display and Information System (ECDIS) and RADAR attack – Alterations, manipulations, and/or DoS of the ECDIS or radar could lead to dangerous situation for the vessel. Can be both RAT and DoS.
 - “Kidnapped cargo”-situation – If a hacker can control maritime digital control systems, a potential situation is the hacker taking control of the vessel cargo. Some ships are carrying freezer containers, which is dependent on constant low temperature, or else the value of the cargo will be damaged. The container systems on board ships are also highly electronical systems today, which means the wrong cargo can go to the wrong destination, if the malicious actor finds a way to do it. This scenario can also relate to tank operations, where a potential adverse actor takes control of the digital control system operating valves and pumps for tankers.
- Manipulating critical onboard sensors and equipment
 - Global Navigation Satellite Systems (GNSS) are today important for the safe navigation of vessels, and high precision of positioning of vessels. GNSS provides signals which can automate most of the navigational tasks a navigator needs to do today. Alterations of such signals could have impact on the control systems used by navigators on a ships bridge.
 - Jammed GNSS signal – The equipment used for navigation is deprived from receiving input from GNSS, and the navigators must utilize more manual modes of navigation. This is reported to be part of real-life incidents, collision of vessels in a situation with lost GNSS signals. GNSS jammers can also be installed in cars or trucks for blocking the authorities’ surveillance of the vehicles, which again can affect ferries. Roads and ship fairways are often in the same areas.
 - Spoofed GNSS signal – An adverse actor maliciously manipulating the GNSS signals to send a ship on a course the navigator did not intend to sail, while displaying erroneous position information. This can also have impact on other systems, such as integrated navigation systems, as technologies and equipment on board ships are increasingly interconnected. If the steering gear control system is controlled by Track Pilot mode (i.e., the ship follows a pre-determined route), and the altering of course is controlled by the ECDIS, which again receives GNSS-input, the consequences can be fatal, in for example narrow waters.
 - Automatic Identification System (AIS) are used to identify vessels, displaying information of position, course of vessel, speed, size, etc. Maliciously altering

the AIS information can have impact on the safety of ships traffic, as it is common to rely on the information provided by AIS.

- Nation state attacks could alter the position of vessels, falsely displaying a ships position in hostile waters, while the ship is not actually there. This kind of attack relate closely to spoofing attacks, where the adverse actor alters the position input to the AIS.
 - AIS also shows information of what kind of cargo is carried. Some nation states could alter the cargo information to “Nuclear”, which is prohibited to carry in some territorial waters. This will initiate an investigation and ship can be subject to unjustified and unwanted ransacking.
- Port stay vulnerabilities
 - This is not directly a scenario but can provide the fundament for a scenario setting or context to a scenario. Port stay is associated with more risk than sailing on the ocean. This is because there is often an uncontrolled flow of service technicians, port authorities, crew for mobilizing the vessel, salesmen, etc. Both physical and digital access to the ship is more accessible than on open waters, and even though there are strict port regulations, malicious actors can use port stays as entry points and attack vectors. Port stays are often also a time with increased internet activity and connectivity, which can cause a potential attack surface for attackers.

3 Workshop discussions

This chapter presents a summary of what was discussed in the different workshop sessions. The participants were divided into three groups for the discussion sessions. Two groups talked in Norwegian and one in English. Each session was moderated by one of the authors of this document, and tape recorded with consent from the participants. After the workshop the tape recordings were transcribed for analysis purposes. The tape recordings were stored on a local tape-recording device, and the transcriptions stored locally.

The aim of the discussions was two folded. The participants were primarily asked to identify possible scenarios for cyber threat situations, but the intention was also to discuss around the handling of these potential situation, their origin, and the potential outcomes. It was also found that the groups discussed more around the topics than first anticipated. The scenarios mentioned in the previous section will not be repeated in this section.

3.1 The discussions

The participants agreed that there should be a difference when facilitating for simulator scenarios to nautical students, compared to experienced navigators. For training scenarios in the nautical education, the observant students will most probably detect errors at once because the scenarios are concentrated and the students actively surveillance the systems, due to the simulator situation they are used to find themselves in. The students will always expect something to happen. For example, GPS-failures will be easily detected, as the students are paying utmost attention to the position and utilizing visual/radar navigation,

as they know they are being observed and evaluated. Simulator training for the nautical students may also be hard to generalize to the common navigator around the world. The NTNU nautical training centre is a very high-end simulator centre, which may not be the case for simulator centres in other parts of the world. The educational system around the world is very diverse, so are the different vessels sailing the oceans.

The participants discussed that small disturbances are the hardest ones to detect. If your vessel jumps from the North Sea to the shores of Canada within a second, you can easily assume something is wrong, for example erroneous position input. The level of alertness will vary during the voyage for navigators. Navigators will most probably be more alert sailing near the coast, than open waters. The participants discussed that humans are only able to hold a sufficient level of alert for 30 minutes in a task, i.e., humans cannot focus on one task for more than 30 minutes, before the level of alertness disintegrates. A question raised in the discussion was if the common navigator is as attentive as the students in a simulator situation. Simulator scenarios are compressed and synthesized situations of what can occur in the real world, however, when sailing a vessel, it can be hours, days, or weeks of sailing before the ship encounters a situation, considering for example overseas voyages. It is seen as unreasonable to expect the navigators to always be agents monitoring the navigation systems sufficiently, especially considering 6- and 12-hour shifts. The instruments navigators are using are working well most of the time. The participants believe it will be hard to detect anomalies in systems that are showing correct information/status 99-100% of the time. The participants do not think the seafarers are expecting something to happen to a more or less stable system, when the ship is not in a critical situation.

A navigator cannot learn all aspects of cyber threats. Therefore, the participants believe the focus of training should be towards situational awareness of cyber-attacks. Making the navigators take a step back and reflect if a cyber-attack is the potential fault in a system is seen as a key factor for success. By exposing navigators to possible cyber threats in simulators, the navigators' troubleshooting-mindset could be altered to also consider possible cyber-attacks/threats. When troubleshooting problems on board ships, cyber threats are not the first thing which comes to mind. In short, the navigators are supposed to look for a ghost they never have seen before. Regarding cyber awareness, both simple scenarios and "James Bond"-like-scenarios are needed, as the participants do believe it is only a matter of time before "James Bond"-scenarios could be realistic.

For seafarers, it can be hard to convert cyber security theory into practice, as the seafarers' interest for cyber security are on a generally low level. The participants believe that for a cyber incident to be relevant for crisis management on board, the cyber incidents need to result in larger and more destructive accidents, such as grounding or collision. Therefore, a cyber crisis will also be treated as a "traditional" crisis. If trained for in a simulator environment, this type of accidents can stimulate to cyber security awareness, as the consequences of a fault will be visualized.

The participants highlight that asking the right questions is important in traditional preparedness scenarios. What is the situation and what to the shipowner do? Do they have the resources, the right persons, the right procedures? The key is to create awareness and

understanding of the situation. Regarding maritime cyber resilience, the seafarers should be trained in the most common cyber-attacks to build experience and a mental library of possible situations. Going from a novice to an expert takes time and experience. The participants also highlight that an expert in navigation can be a novice in cyber security, and vice versa.

A triangular approach to threats is suggested, where technical equipment, competence, and culture are considered. These factors need to correlate, and one should not exceed the other. Simulator scenarios need to be classified to pinpoint the purpose of the scenarios. The scenarios can range from tabletop scenarios to full scale preparedness onboard or onshore scenarios. When designing simulator scenarios, it could be beneficial to have a different approach when considering highly experienced seafarers and novice seafarers. Highly experienced seafarers might not take a “James Bond”-scenario seriously, as the consequences is too farfetched and unrealistic for their understanding of reality. They will not consider such scenarios to be likely for their ship and operation. Scenarios designed for highly experienced seafarers should have a solid foundation in reality, to get the seafarers interest and attention. The scenarios should also be relevant for the ship, as the experienced seafarers have in-depth ship knowledge. In contrast, the students may be more open for “James Bond”-scenarios, as they have not yet developed the same kind of in-depth knowledge. They will tend to trust the simulator instructor more than their own experience, which will often be opposite for the experienced seafarers. The training could also benefit from being gradually incorporated. Some examples are drawn to the companies who send “friendly” malicious emails to their employees and gives a warning if the employee have clicked on a potential malicious link.

The participants who have previously participated in cyber crisis preparedness exercises urges the importance of debriefing with cyber security experts after such an exercise. In one mentioned cyber preparedness exercise where the ballast water management system of a vessel was compromised and hijacked by hackers, the dedicated cyber crisis response company had a walkthrough with the navigators after the exercise. The intention of this was to explain how the attack was even possible. This was seen as an eye-opener and clearly beneficial to the participants in the cyber preparedness exercise. The most vital part of the simulators scenarios is the people in the scenario. This adds an important dimension which is needed to get a fruitful test of the preparedness of the company.

Participants from the naval defence sector highlights that they do not treat “cyber” as a separate focus area, but rather as an addition to traditional problem solving. Cyber is balanced across the whole industry, similar as safety and security is implemented in an organisations procedures and operation. Today, leaders must have a better understanding of the system the organisation is using. It is no longer acceptable for a leader to mean that cyber security is someone else’s problem. A leader in the armed forces need to take more responsibility towards cyber security. If they cannot adapt to these kinds of requirements, the leaders will be asked to reconsider their role. This issue can be challenging for many leaders, as leaders in any organisation will normally be expected to consider operations and matters on a management level, not a detailed, operational level. This is now changing for cyber threats and may also be a momentum for civilian organisations to consider.

4 Conclusion

This workshop report has summarized the findings of a cyber security simulator workshop. Cyber security cases undertaken in simulator scenarios were in unison seen as beneficial for the maritime industry. Mariners are familiar with simulator training, and if done right, one could get the attention of both novices and expert mariners. Design of scenarios should be tailored to the intended people undertaking the scenario. The participants were eager to share what they found important and realistic to consider when designing scenarios. Organisations could benefit of implementing cyber security in the organisation as a whole, and this could also be the case for education. Cyber security should be an integral plan of business strategies and educational plans, to create foundation for inherent cyber resilience in the maritime industry.

Future work will be to implement the findings from this workshop report in the development of maritime cyber resilience training. This implementation will aim at developing both shipowner and ship crew specific training, as well as simulator training in the M.Sc. course “Maritim Digital Sikkerhet” within the M.Sc. degree program “Management of Demanding Marine Operations” at NTNU in Ålesund.

Annex II – Additional SLR information

Several criteria were set for the literature review. There was a limitation on when the papers searched for should be published, and to get updated research information the years from 2000 – 2023 were chosen. The reason for this was to capture as much of the literature as possible, but also to cover if any research on the topic existed on maritime cyber resilience before 2010, as Bolbot indicates that there is no research at that time. The literature review should consider both conference papers and journal articles, as the maritime cyber resilience is a growing field of research, as well as the papers should be in English. The databases were chosen as maritime cyber resilience is an interdisciplinary field of research, and the databases comprises both maritime studies, engineering, and social sciences, and/or a combination. For searching for literature, the relevant databases need to be chosen. Bolbot et al. (2022) provides a literature review of the status of development and research directions in maritime cyber security and emphasise that maritime cyber resilience research needs to be expanded. Bolbot relied on Scopus as a sole source and suggest doing a more specified literature review as well as using non-Scopus databases. Hence the literature review in this thesis includes more search engines. Bolbot also Thus, the chosen databases were Scopus, SpringerLink, Web of Science, EBSCO and Compendex. The database was reviewed and found through NTNU library service, Oria, which also means that the university had the necessary access and admissions necessary for a literature review. The search strings needed to be adjusted to each database and is as described below. The date of search was the 27th of June 2023.

All results from searching the literature were logged in an Excel file, structured where each database was logged in a separate sheet with its respective papers. The total number of findings was 1379.

The results of the searching phase were stored in an Excel file, and first duplicate titles was removed. The number then decreased to 1187. For each phase of the literature review, a new Excel file was duplicated from the previous one, to keep track and log of the process and uphold transparency. The documents containing the raw data is available for the reader upon request to the author of this thesis.

Practical screening is about including literature for the review and figuring out if the paper is applicable for the literature review or not (Okoli & Schabram, 2010). This was performed by first reading and assessing the titles, before reading the abstracts, to understand what articles to include further in the literature review. In case of any doubt of relevance to the literature review, the paper was included for the next phase, quality appraisal. It was a low threshold to be included as a result of the practical screening.

The research question for the literature review was a guiding light in the process and the specified criteria for inclusion/exclusion were follows:

1. English language
2. Open-access – available
3. Journal or conference paper – peer reviewed
4. Relevant to maritime cyber resilience/security/risk/safety or similar terms, such as maritime information security, and/or maritime cyber-attacks/incident/crisis/situations affecting operational situation of the vessel.
5. Relevant to ship handling or maritime navigator training.
6. Relevant and focusing on the operational aspect, not only on technical aspects/security measures.

7. Paper only relevant for unmanned autonomous ships, not considering human operation/involvement was excluded.
8. Paper only relevant for port and port operations was excluded.
9. Papers related to legal aspects, economics, or insurance aspects was excluded.
10. Literature reviews was excluded.
11. Paper written by the author of this thesis was excluded.
12. Titles which indicate a collection of conference papers, editorial or commentary was excluded.

The quality appraisal phase should assess the quality of the papers resulting from the practical screening (Okoli & Schabram, 2010). As stated in the previous sub-section, none of the paper written for this thesis is considered in the literature review. However, as the research area of maritime cyber resilience is as narrow as it is, the working definition described in Erstad et al. (2021) will be used for guidance, as there still not is found a pin-point definition of “maritime cyber resilience”. The aim of this thesis is to enhance maritime cyber resilience, and the reviewed paper should have some form of relevance to the aspect. This means that the papers for review must:

1. Must have relevance for conventional navigational operation of vessels.
2. Must consider aspects of maritime cyber resilience, including but not limited to:
 - Operational handling of cyber situations (anticipate, withstand and recover)
 - Training/educating to overcome cyber situations (evolve)

According to methodological quality appraisal suggested by (Okoli & Schabram, 2010), if any of the papers found in the previous practical screening does not answer “yes” any of the two criteria stated above (including the aspects mentioned in the practical screening process), the paper is not considered further.

For the data extraction, the paper was listed with what the research question and goal of the paper was, before it was categorized in how it relates to the working definition of “maritime cyber resilience”. Everything was logged in a separate Excel sheet.

To ease the process and to get more specified information, “maritime cyber resilience” has been divided into the following themes:

- prior cyber incident / training and educating (anticipate and evolving)
- during cyber incident / incident handling (withstand and recover)

Annex III – Interview guide

The interview guide was originally in Norwegian, transcribed to English for the thesis.

Theme	Suggested questions
Information prior the interview	<ul style="list-style-type: none"> • Purpose and the project • Explain duty of confidentiality and anonymity • Ask if anything is unclear and permission to start audio recording
Personalia	<ul style="list-style-type: none"> • Education • Experience – Type ship • Current employment
Own experience considering cyber incidents	<ul style="list-style-type: none"> • How do you consider the term “cyber threat” towards your ship? • Have you been exposed for a cyber-attack/incident? • To what extent? • If no: Have you heard of anyone else been exposed for a cyber-attack/incident?
Education	<ul style="list-style-type: none"> • Training in education • Simulator scenario in education • Training as professional • If no: What is missing? • If yes: what was good/bad/more/less with the training?
Procedures and policy	<ul style="list-style-type: none"> • For awareness? • For handling? • Other methods? • Responsible for cyber security onboard and on shore
Exercises	<ul style="list-style-type: none"> • Do you have exercises for cyber-attacks/incidents?
Handling of cyber-attacks	<ul style="list-style-type: none"> • What would be a plausible cyber-attack against your/other ship? • What would you do if you were victim to a cyber-attack (provide examples for ECDIS or ransomware)? • Could you imagine a situation you couldn't handle? Especially PNT (position, navigation, timing) • Do you have any opinion about what it takes to enhance operational resilience against cyber-attacks against ships?
Summary	<ul style="list-style-type: none"> • Considering what we have talked about, is it anything you find extra interesting? • Why is this important? • What could/should be done? • Summarize my understanding of the conversation as a whole. • Do you want to add anything?



Table 5 - Interview guide - translated from Norwegian to English

Annex IV – Course feedback scheme

Below is an extract of the feedback for the simulator exercises. The whole feedback report is available on request to the author.

Jobber du nå, eller har jobbet tidligere, som dekksoffiser?

Number of submissions: 17




Submissions	Count	% of submissions	
Ja	7	41.2%	 41.2%
Nei	10	58.8%	 58.8%

Nåværende stilling (frivillig å svare på)

- Los
- Systemansvarlig Vedlikehold/PMS
- seniorrådgiver
- Supervisor
- Vessel manager
- Administrasjon
- Maritim Operativ leder
- Daglig leder
- IT Leder
- Sikkerhetsrådgiver






Synes du at du lærte mye av simulatorøvingene?

Number of submissions: 17

Submissions	Count	% of submissions	
1 Slett ikke	0	0%	0%
2	0	0%	0%
3	1	5.9%	 5.9%
4	7	41.2%	 41.2%
5 Absolutt	9	52.9%	 52.9%
Vet ikke	0	0%	0%




Synes du simulatorøvingene var relevante for ditt arbeid?

Number of submissions: 17

Submissions	Count	% of submissions	
1 Slett ikke	0	0%	0%
2	1	5.9%	 5.9%
3	5	29.4%	 29.4%
4	4	23.5%	 23.5%
5 Absolutt	6	35.3%	 35.3%
Vet ikke	1	5.9%	 5.9%

I hvilken grad oppfylte kurset behovet ditt for kompetanseheving innen maritim digital sikkerhet?

Number of submissions: 17

Submissions	Count	% of submissions	
1 I liten grad	0	0%	0%
2	0	0%	0%
3	0	0%	0%
4	8	47.1%	 47.1%
5 I stor grad	8	47.1%	 47.1%
Vet ikke	1	5.9%	 5.9%

Annex VI – NSD forms



[Notification form](#) / [Håndtering av dataangrep mot skip](#) / Assessment

Assessment of processing of personal data

Reference number

364232

Assessment type

Standard

Date

01.09.2020

Title

Håndtering av dataangrep mot skip

Institution responsible for the project

Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Project leader

Erlend Erstad

Project period

07.09.2020 - 31.01.2021

Categories of personal data

General

Legal basis

Consent (General Data Protection Regulation art. 6 nr. 1 a)

The processing of personal data is lawful, so long as it is carried out as stated in the notification form. The legal basis is valid until 31.01.2021.

[Notification Form](#)

Comment

Det er vår vurdering at behandlingen av personopplysninger i prosjektet vil være i samsvar med personvernlovgivningen så fremt den gjennomføres i tråd med det som er dokumentert i meldeskjemaet med vedlegg den 01.09.20. Behandlingen kan starte.

MELD VESENTLIGE ENDRINGER

Dersom det skjer vesentlige endringer i behandlingen av personopplysninger, kan det være nødvendig å melde dette til NSD ved å oppdatere meldeskjemaet. Før du melder inn en endring, oppfordrer vi deg til å lese om hvilke type endringer det er nødvendig å melde:

https://nsd.no/personvernombud/meld_prosjekt/meld_endringer.html

Du må vente på svar fra NSD før endringen gjennomføres.

TYPE OPPLYSNINGER OG VARIGHET

Prosjektet vil behandle alminnelige kategorier av personopplysninger frem til 31.01.2021.

LOVLIG GRUNNLAG

Prosjektet vil innhente samtykke fra de registrerte til behandlingen av personopplysninger. Vår vurdering er at prosjektet legger opp til et samtykke i samsvar med kravene i art. 4 og 7, ved at det er en frivillig, spesifikk, informert og utvetydig bekreftelse som kan dokumenteres, og som den registrerte kan trekke tilbake. Lovlig grunnlag for behandlingen vil dermed være den registrertes samtykke, jf. personvernforordningen art. 6 nr. 1 bokstav a.

PERSONVERNPRINSIPPER

NSD vurderer at den planlagte behandlingen av personopplysninger vil følge prinsippene i personvernforordningen om:

- lovlighet, rettferdighet og åpenhet (art. 5.1 a), ved at de registrerte får tilfredsstillende informasjon om og samtykker til behandlingen
- formålsbegrensning (art. 5.1 b), ved at personopplysninger samles inn for spesifikke, uttrykkelig angitte og berettigede formål, og ikke behandles til nye, uforenlige formål
- dataminimering (art. 5.1 c), ved at det kun behandles opplysninger som er adekvate, relevante og nødvendige for formålet med prosjektet
- lagringsbegrensning (art. 5.1 e), ved at personopplysningene ikke lagres lengre enn nødvendig for å oppfylle formålet

DE REGISTRERTES RETTIGHETER

Så lenge de registrerte kan identifiseres i datamaterialet vil de ha følgende rettigheter: åpenhet (art. 12), informasjon (art. 13), innsyn (art. 15), retting (art. 16), sletting (art. 17), begrensning (art. 18), underretning (art. 19), dataportabilitet (art. 20).

NSD vurderer at informasjonen om behandlingen som de registrerte vil motta oppfyller lovens krav til form og innhold, jf. art. 12.1 og art. 13.

Vi minner om at hvis en registrert tar kontakt om sine rettigheter, har behandlingsansvarlig institusjon plikt til å svare innen en måned.

FØLG DIN INSTITUSJONS RETNINGSLINJER

NSD legger til grunn at behandlingen oppfyller kravene i personvernforordningen om riktighet (art. 5.1 d), integritet og konfidensialitet (art. 5.1. f) og sikkerhet (art. 32).

For å forsikre dere om at kravene oppfylles, må dere følge interne retningslinjer og/eller rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET

NSD vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til med prosjektet!

Tlf. Personverntjenester: 55 58 21 17 (tast 1)



[Notification form](#) / [Håndtering av datatrusler mot skip](#) / Assessment

Assessment of processing of personal data

Reference number

422483

Assessment type

Standard

Date

08.09.2023

Title

Håndtering av datatrusler mot skip

Institution responsible for the project

Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Project leader

Erlend Erstad

Project period

03.05.2021 - 31.01.2024

Categories of personal data

General

Legal basis

Consent (General Data Protection Regulation art. 6 nr. 1 a)

The processing of personal data is lawful, so long as it is carried out as stated in the notification form. The legal basis is valid until 31.01.2024.

[Notification Form](#) [↗](#)

Comment

Behandling av personopplysninger er utvidet til 31.01.2024. Vi vurderer at behandling fortsatt er lovlig, under forutsetning om at utvalget ditt får ny informasjon, her også informasjon om endret varighet.

Mer at vi legger til grunn at du har kontaktinformasjon til utvalget ditt og vil gi dem ny informasjon. Hvis ikke dette er tilfellet, må du sende melding til oss i meldeskjemaet slikt at vi kan foreta en mer inngående vurdering av om behandlingen fortsatt vil være lovlig.

Lykke til videre med prosjektet!

ISBN 978-82-326-7812-9 (printed ver.)
ISBN 978-82-326-7811-2 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)



NTNU

Norwegian University of
Science and Technology