Doctoral theses at NTNU, 2024:46

Marie Haugli-Sandvik

Cyber Risk Perception in Offshore Operations

An Exploratory Study of Deck Officers' Perceptions of Cyber Risks in Norwegian Shipping Companies

Doctoral thesis

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

NTNU
Norwegian University of Science and Technology

Marie Haugli-Sandvik

Cyber Risk Perception in Offshore Operations

An Exploratory Study of Deck Officers' Perceptions of Cyber Risks in Norwegian Shipping Companies

Thesis for the Degree of Philosophiae Doctor

Trondheim, January 2024

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

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of Science and Technology

Thesis for the Degree of Philosophiae Doctor

Faculty of Engineering
Department of Ocean Operations and Civil Engineering

ISBN 978-82-326-7694-1 (printed ver.)
ISBN 978-82-326-7693-4 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

Doctoral theses at NTNU, 2024:46

Printed by NTNU Grafisk senter

Statement of Authorship

I, Marie Haugli-Sandvik, hereby declare that this thesis, entitled “Cyber Risk Perception in Offshore Operations: An Exploratory Study of Deck Officers’ Perceptions of Cyber Risks in Norwegian Shipping Companies”, is entirely my own. The work of others and any additional sources of information have been duly cited.

I confirm that:

- The research presented and reported in this thesis is original and has been conducted by me, unless otherwise acknowledged.
- No portion of the work referred to in this thesis has been submitted in support of an application for another degree or qualification to this or any other university or institution.
- I have clearly acknowledged the work and contributions of others and have adhered to all guidelines and principles of academic honesty and integrity.
- All data, findings, and interpretations presented in this thesis are true to the best of my knowledge.
- Any views expressed in the thesis are my own and do not represent the views of the university.

Ålesund, January 2024

Marie Haugli-Sandvik (sign.)

Abstract

The digital evolution of the maritime industry has given rise to new cybersecurity challenges and increased cyber risks for shipping companies and their vessels. At sea, losses from cyber-attacks are not just monetary but can include human lives and damage to the environment. Deck officers are part of the frontline mitigating and handling cyber risks on vessels, and understanding how they perceive such risks is crucial for developing targeted cyber risk management strategies and enhancing vessel security and safety. The overall objective of this thesis was to explore deck officers' perceptions of cyber risks in offshore operations.

This research project was grounded in risk perception theories from the psychology field and utilised a mixed methods exploratory sequential design. The approach ensured that each research phase in this thesis informed the subsequent one, providing a comprehensive understanding of factors influencing deck officers' cyber risk perceptions within the context of Norwegian shipping companies.

The research was conducted in four subsequent phases. The first phase involved a systematic literature review, which aimed to capture the current state of research on cyber risk perception and present an approach for investigating factors influencing people's perception of cyber risks using psychological models. The review identified 24 dimensions of cyber risk perception, demonstrated how these dimensions could be applied in a maritime context, and highlighted research gaps in the existing literature.

Informed by the literature review, the second phase employed in-depth interviews to explore deck officers' perceptions of cyber risks in offshore operations. A contextual model was developed with thick descriptions of dimensions influencing these perceptions. Key findings included the deck officers' perceived distance from cyber risks, their inherent trust in cyber-physical systems, more restricted work flexibility because of digitalisation, and their dependence on others for cyber defence.

Building on insights from the qualitative phase, the third research phase utilised a self-administrative questionnaire to investigate factors shaping deck officers' cyber risk perceptions towards information technology (IT) and operational technology (OT) systems. Variables such as perceived benefit, trust, cybersecurity training, and prior experiences with cyber-attacks were analysed, revealing distinct risk perceptions towards IT versus OT systems.

The synthesis in the fourth phase, comprising this thesis, led to the development of a characteristics model that serves as a roadmap for obtaining contextual knowledge that is essential for developing targeted cyber risk management strategies. The model illustrates how the working environment on offshore vessels (the context), combined with deck officers' personal experiences and biases (the risk perceiver), the intangible nature of cyber risks (the risks), and the on-board system categories (IT and OT), forms distinct perceptions of cyber risks. As the maritime industry becomes increasingly interconnected and reliant on digital systems, understanding how cyber risk perceptions are shaped among operational decision-makers is crucial. This research provides foundational insights that can guide future efforts to enhance maritime cybersecurity practices.

Acknowledgements

First and foremost, I would like to express my gratitude to my supervisors, Frøy Birte Bjørneseth, Mass Soldal Lund, and Sokratis Katsikas. Your guidance, feedback, and support have been instrumental throughout this project. Furthermore, I owe a sincere thank you to all the participants of my studies. Without their time, insights, and willingness to share, this thesis would not have been possible. Additionally, a special acknowledgment goes to my colleague, Erlend Erstad; our discussions and collaborations over the years have been invaluable and greatly appreciated.

To my family, your support has been the foundation of this work. A special note of thanks goes to my husband, Hans Kato. Your endless understanding and patience have been instrumental to this achievement. Last, but not least, I thank my feline companion, Laban, whose purring company at my home office, especially during the COVID-19 pandemic, brought smiles and warmth to the sometimes dauting process of thesis writing.

Abbreviations

AHTS	Anchor Handling Tug Supply Vessel
BIMCO	Baltic and International Maritime Council
COVID-19	Coronavirus disease 2019
CSV	Construction Support Vessel
ECDIS	Electronic Chart Display System
ENISA	European Union Agency for Cybersecurity
FPSO	Floating and Production Storage and Offloading Vessel
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
ICT	Information and Communication Technology
IMO	International Maritime Organization
IoT	Internet of Things
IT	Information Technology
KA-SAT	Geostationary telecommunications satellite owned by Viasat
MaCRA	Maritime Cyber Risk Analysis model
MITRE ATT&ACK	MITRE Adversarial Tactics, Techniques, and Common Knowledge
MSC	Mediterranean Shipping Company
NIST	National Institute of Standards and Technology
NORMA Cyber	The Norwegian Maritime Cyber Resilience Centre
OT	Operational Technology
POSEIDON framework	Procedures, operations and standards for the detection of integral events and the development of naval operating capacity
PSV	Platform Supply Vessel
STCW Convention	The International Convention on Training, Certification and Watchkeeping for Seafarers
UK	United Kingdom
USB	Universal Serial Bus

List of included papers

Paper 1

Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review

Authors: Marie Haugli Larsen* and Mass Soldal Lund

IEEE Access, Volume 9, October 2021, Pages: 144895–144906, DOI: 10.1109/ACCESS.2021.3122433

Paper 2

A Model of Factors Influencing Deck Officers' Cyber Risk Perception in Offshore Operations

Authors: Marie Haugli Larsen*, Mass Soldal Lund, and Frøy Birte Bjørneseth

Maritime Transport Research, Volume 3, June 2022, Article number 100065, DOI: 10.1016/j.martra.2022.100065

Paper 3

Maritime Decision-Makers and Cybersecurity: Deck Officers' Perception of Cyber Risks Towards IT and OT systems

Authors: Marie Haugli-Sandvik, Mass Soldal Lund, and Frøy Birte Bjørneseth

International Journal of Information Security, in press

*I changed my last name from Larsen to Haugli-Sandvik in October 2022.

Contents

List of figures

List of tables

PART I

1 Introduction

In the age of rapid digitalisation, the maritime industry is experiencing transformative shifts. The maritime domain consists of highly operational working environments, and the increase in connectivity and digitalisation creates both opportunities and challenges (Det Norske Veritas [DNV], 2023). Offshore operations, once primarily governed by human intuition and manual control, now largely depend on integrated, automated, and network-based systems. While offering operational efficiencies and new functionalities, this digital evolution has given rise to new cybersecurity challenges and increased cyber risks for shipping companies and their vessels (Chubb et al., 2022).

Recent incidents, such as the catastrophic cyber-attack on Maersk Shipping Company in 2017 and the malware-based cyber-attack on shipping giant Mediterranean Shipping Company (MSC) in 2020, highlight the potential consequences of these rising cyber risks (Kuhn, 2022). At sea, losses are not just monetary but can escalate to impact human lives and the environment and cause significant disruptions to the maritime transportation system (Ben Farah et al., 2022). As the International Maritime Organization (IMO) and other regulatory bodies emphasise, cyber risks are not merely technical challenges for information technology (IT) departments to handle (DNV, 2023; IMO, 2017). Cyber risk management encompasses understanding underlying processes that drives human behaviour and decision-making – areas that remain relatively unexplored in the context of maritime cybersecurity (Haugli-Sandvik et al., in press; Larsen & Lund, 2021).

It is crucial to understand how operational decision-makers, such as deck officers, perceive cyber risks to their vessels' technological systems. With their hands-on approach to vessel management, deck officers are part of the frontline mitigating and handling cyber risks, such as malware attacks on operational systems or targeted phishing attacks on crew members (Erstad et al., 2022). How the officers perceive cyber risk is important because it influences their individual behaviour, decision-making, and their acceptance of technologies, policies, and norms, which, in turn, have implications for risk exposure, risk communication, and risk management (Siegrist & Árvai, 2020). Consequently, it essential to investigate factors influencing these cognitive processes (Fan et al., 2023; Larsen et al., 2022).

Offshore operations, which encompass both IT and operational technology (OT) systems, are inevitably linked to deck officers, who manage these systems daily. However, little research dives into the cognitive processes influencing operational decision-makers actions in the face of cyber risks (Bolbot et al., 2022; Haugli-Sandvik et al., in press). Such an understanding is not only of academic interest; it has implications for shaping cyber risk communication, cybersecurity training, and holistic policies tailored to the maritime context. The focus of this thesis is to address this research gap by investigating deck officers' perceptions of cyber risks in offshore operations. Utilising a mixed-method exploratory sequential design, the study's main objective is explored through the following four subsequent phases: a systematic literature review, a qualitative study with in-depth interviews, a quantitative self-reporting questionnaire, and the synthesis of these phases, comprising this thesis. By grounding the research in the real-world experiences and perspectives of deck officers working within Norwegian offshore shipping companies, this thesis offers both theoretical insights and actionable recommendations that can guide the maritime industry in developing tailored cyber risk management strategies.

1.1 Objectives and research questions

The overall objective of this thesis is to explore the cyber risk perception of deck officers in offshore operations. The significance of this objective stems from a noticeable gap in the existing literature and the importance of considering human behaviour in maritime cybersecurity. While risk perception has been studied in various settings and contexts, the perception of cyber risks within offshore operations requires further exploration. This thesis addresses the overall research objective by mapping existing literature on cyber risk perception, developing a contextual model of factors influencing deck officers' perceptions of cyber risks, and measuring levels of perceived cyber risks to develop statistical models and test causal relationships.

To address these aims and provide a comprehensive understanding of deck officers' cyber risk perceptions, this study poses the following research questions:

RQ 1: What is state-of-the-art research within the field of cyber risk perception in general, and in the context of the maritime domain?

To establish a foundational understanding of cyber risk perception and map the current state of research, a systematic literature review was conducted. This research phase investigated relevant empirical studies and methods within cyber risk perception, facilitating the identification of existing research trends and providing the groundwork for subsequent research directions within the maritime context.

RQ 2: What factors can influence deck officers' perception of cyber risks in offshore operations, and how can these factors be described?

Upon gaining a clear picture of the status of research on maritime cyber risk perception, a qualitative study with in-depth interviews was conducted. The aim was to develop thick descriptions and a contextual model of the factors influencing deck officers' perceptions of cyber risks. This approach was used to provide descriptive categories grounded in data collected on participants' experiences and reflections to discover new themes and dimensions of cyber risk perception specific to offshore operations.

RQ 3: What level of cyber risk do deck officers perceive towards IT and OT systems, and is there a difference in how the independent variables of perceived benefit, trust, cybersecurity training, and experience with cyber-attacks predict the officers' cyber risk perception?

Drawing on insights gained in the qualitative phase, a quantitative study was conducted with hypotheses built upon the findings from the contextual model. A self-administered questionnaire was used to measure deck officers' levels of cyber risk perception in relation to vessel IT and OT systems. The objective was to develop statistical models that predict cyber risk perception levels based on previously identified independent variables.

1.2 Research scope

Central to this research is the exploration of factors influencing deck officers' perceptions of cyber risks in offshore operations, particularly within the context of Norwegian shipping companies. This research seeks to gain a broader understanding of the individual cognitive processes that shape these operational decision-makers perceptions, emphasising cyber risks for offshore vessels' systems and officers' experiences with such risks.

The decision to focus on deck officers working in Norwegian shipping companies was driven by several factors. Firstly, the Norwegian offshore sector is well-known for being technically

advanced and having a stringent regulatory environment (Huus & Paulsen, 2022), which makes it one of the most mature maritime contexts for investigating cyber risk perceptions. Secondly, deck officers were selected as the primary research population due to their responsibility for the safety and security of crew and vessels, making them the operational decision-makers on vessels. Finally, the research scope was intentionally narrowed down to deck officers to keep the study manageable, although engineers and other crew members also play a significant role in addressing cyber risks. While team dynamics on vessels are important, this thesis focus on individual experiences and perceptions of deck officers.

Even though traditional offshore vessels and their associated cyber risks remain central to the discussion, this research intentionally sidesteps the domains of ports and autonomous, or remotely, controlled vessels. This sidestep is due to the focus on deck officers' experiences and perceptions in offshore operations. The areas of ports and autonomous vessels have other operational distinctions and technological aspects. Moreover, it is crucial to note that the primary emphasis in this work is not the technical dimensions of cybersecurity but cognitive processes affecting human cyber risk perceptions. This thesis presents clear definitions of cyber risks and threats but intentionally avoids delving into specific cyber threats, since this would limit the scope of exploring deck officers' cyber risk perceptions and confine responses from the participants.

This thesis is theoretically anchored in the psychology approach in risk perception research. Central to this positioning are the psychometric paradigm, heuristics, and cognitive biases. These theories originally sought to elucidate human perception of physical risks, including incidents such as nuclear disasters, environmental catastrophes, and health hazards (Siegrist & Árvai, 2020), by emphasising the cognitive processes by which people interpret and understand the world. While this research provides illustrative examples for explaining the theoretical aspects in this thesis, the direct application of these frameworks to cyber risks necessitates nuance. Cyber risks, inherently intangible compared to their physical counterparts, may present different cognitive challenges and perceptions. This study acknowledges these potential distinctions. However, the underlying cognitive processes involved in risk perception are similar across different types of risks (Bada & Nurse, 2020), which means that the theoretical frameworks can still be useful for exploring deck officers' cyber risk perceptions.

1.3 Research strategy

The research trajectory was driven by the objective of exploring deck officers' cyber risk perceptions in depth. Accordingly, this research project adopted a mixed-methods approach with an exploratory sequential design. This implies that the studies were conducted in sequential phases, with insights from one phase informing the design and objectives of the subsequent phase (Creswell, 2022). A visualisation of this strategy is presented in Figure 1.

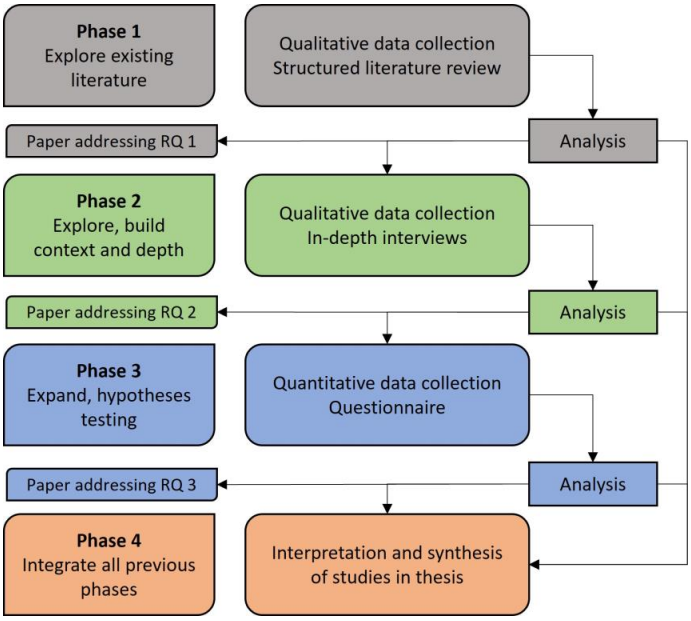


Figure 1: *Research strategy with sequential exploratory design*

The initial phase aimed to provide an overview of the status of maritime cyber risk perception research, including relevant studies within the psychometric paradigm and cognitive biases related to cyber risk perception in general and the maritime domain specifically. The identified research guided the second phase, which aimed to develop a contextual model and descriptions of factors influencing cyber risk perception. Subsequently, the third phase built on the qualitative insights to develop statistical models to predict cyber risk perception in relation to IT and OT systems. Finally, the fourth phase integrated the findings from all the previous stages, culminating in this thesis, which offers a holistic interpretation and analysis of the entire research trajectory.

1.4 Scientific and industrial contributions

This thesis offers valuable insights for both academia and the maritime industry, drawing on the discoveries of each individual paper and the overarching narrative they collectively form. Employing a mixed methods exploratory sequential design, this research pioneered a holistic understanding of deck officers' cyber risk perceptions in offshore operations. The research design allowed for sequential studies in which one phase informed the next, resulting in a depth and breadth not previously achieved in this context.

By delving into, and building on, established risk perception theories, the findings offer a descriptive model of dimensions influencing cyber risk perceptions. Statistical models that investigate causal relationships between influential factors are also presented to evince how various factors influence officers' perceptions of cyber risks and that these perceptions vary across system categories within the same context.

The focus on deck officers working in Norwegian shipping companies provides a regional lens on a topic of global relevance. A fundamental contribution of this thesis is the characteristics model, which emerges from the synthesis of the studies in this thesis. This model serves as a framework that encapsulates the factors influencing deck officers' cyber risk perceptions and emphasises characteristics of the context (offshore vessel working environment), the risk perceiver (deck officers), the risk (cyber risks), and the on-board systems (IT and OT systems). While the model offers insights specific to deck officers' perceptions in offshore operations, the high-level characteristics have a broader application since they are adaptable and can evolve alongside changes in individuals' risk perceptions. As such, the model can be explored across contexts and demographics.

Insights from this research have led to actionable recommendations for enhanced cyber risk management in the maritime domain. While these recommendations are crucial, the study's true contribution lies in the holistic understanding of maritime cyber risk perception that underpins these suggestions, which can guide maritime stakeholders in the development of tailored cybersecurity strategies.

1.5 Thesis impact

The research undertaken for this thesis has made a significant impact in several areas, with its key insights enriching maritime cybersecurity education. In particular, the research served as the foundation for a life-long-learning course in maritime cybersecurity, introduced at the Norwegian University of Science and Technology (NTNU) in Ålesund. According to the students' feedback, they have expressed satisfaction and heightened awareness of the importance of integrating cybersecurity into their maritime education programs. The findings have also broadened NTNU's curriculum, inspiring student projects at both the bachelor and master levels.

The findings and recommendations presented in this thesis have been disseminated through a variety of activities, including presentations at conferences targeting maritime industry professionals and policymakers and publications in international journals. The research has also heightened awareness within the maritime industry, thanks to workshops and presentations tailored to industry stakeholders such as shipping companies and regulatory bodies. Collaboration has flourished, with partnerships established both locally and internationally, spanning across continents from Estonia to Canada. Given the momentum and interest this work has generated, it is expected to set the direction for future research initiatives with a focus on human behaviour aspects in maritime cybersecurity.

1.6 Reflexivity and researcher positionality

Acknowledging the influence of a researcher's positionality in the research process is important (Creswell & Poth, 2018), and my diverse experiences significantly shape this study's perspectives. My academic journey began with a focus on psychology and sociology, leading to an interest in human cognition and how we interact with our surroundings. Despite these interests, I chose to pursue a career as a deck officer in the maritime industry.

My professional and educational background as a deck officer provided me with firsthand experience and understanding of the operational working environment in offshore operations. Our risk management was focused principally on assessing physical risks related to, for example, loading and offloading cargo, welding jobs, working in heights, weather limitations on equipment and vessel, and navigational challenges. This knowledge significantly influenced my approach to maritime cybersecurity.

I then stepped ashore to engage in a master's degree in the management of demanding marine operations, which strengthened my understanding of decision-making and risk management frameworks. My interdisciplinary background has resulted in an appreciation of pragmatic approaches to improving the human condition globally. I hold a firm belief that it is imperative to understand human behaviour when working towards enhancing maritime cybersecurity.

My experiences and beliefs have not only informed how I formulated my research questions but also guided my methodological choices and interpretations of the findings. While I have endeavoured to maintain a balanced and reflective stance, the interpretive nature of this study, particularly its qualitative aspects, is influenced by my individual perspective. However, by adopting a mixed-methods approach, I strived for a nuanced, comprehensive exploration of deck officers' cyber risk perceptions in offshore operations.

Multiple strategies have been adopted in this thesis to mitigate bias and enhance validity. Continuous reflection about how my background and beliefs might influence the interpretation of data was operationalised through maintaining a research diary and engaging in reflexivity sessions. These sessions involved critically examining my assumptions and their potential impact on interview question development and the thick descriptions in the contextual model. Peer feedback from fellow researchers and supervisors was instrumental in refining the data analysis and research process, leading to enhanced methodological rigour as detailed in Chapter Four (Creswell & Poth, 2018). This chapter underscores the systematic approach and transparency integral to this thesis. A mixed-methods approach was chosen to provide complementary data, offering both breadth and depth.

1.7 Thesis outline

The structure of this thesis is designed to provide clarity and a logical progression through the research process. Part I begins with an introduction that highlights the relevance of and motivation for this thesis. The following "Background" section offers contextual information about the particularities of the maritime industry, human factor research, and cybersecurity, which are essential for understanding the distinct challenges within the research context. Next, the "Theoretical foundation" section presents a review of theories underpinning the research and provides insight that enlightens the empirical findings. The "Methodological considerations" section outlines the research design and approach, discusses assumptions made

during the research process, and details the methods used for data collection. The heart of the thesis lies in the “Summary of findings and contributions” section, which summarises the scientific papers that form the thesis’s core and presents their key findings and contributions. Building on the results, the “Discussion” section contrasts the findings with the theoretical backdrop, offering a critical analysis and synthesis of the papers that make up the research in this thesis. The “Conclusion” section discusses the broader implications of the research and encapsulates its key takeaways, offering a holistic view of its significance.

The thesis culminates with Part II, which presents the scientific papers integral to this study. These papers form the foundational basis for the undertaken research and complement the information articulated in this thesis.

2 Background

Understanding the particularities within the maritime industry is important when considering research findings and theoretical implications. This section first briefly explains the maritime and offshore industry within this international sector and presents aspects of maritime human factors. It then explains maritime cybersecurity, IT and OT, as well as the human element in maritime cybersecurity before concluding with a presentation of related work.

2.1 The maritime and offshore industry

As part of the backbone of global transportation for centuries, the importance of the maritime industry to international commerce and the global economy cannot be overstated (Chubb et al., 2022). The primary service for moving goods throughout the world, this sector is integral to the transportation system and is considered part of countries' critical infrastructure. Kessler (2022) describes the maritime industry as a system of systems, in which each system is unique and has its own sub-systems. This thesis focuses on deck officers working on offshore vessels in Norwegian shipping companies, which are crucial to parts of the maritime transportation system. These vessels can be considered floating networks that must be interconnected; the deck officers are decision-makers operating these networks and systems, executing vessel operations, and maintaining system functionality and security (Erstad et al., 2022; Kessler & Shepard, 2022).

On-board offshore vessels there are typically four deck officers forming the bridge team (captain, chief mate, and two deck officers). The captain, who is the highest-ranked deck officer, holds the ultimate command and responsibility. Additionally, the deck officer on watch represents the captain and is responsible for operational safety in the absence of the captain on the vessel bridge. This team has responsibility for navigation, cargo handling and stowage, controlling the operation of the vessel, and caring for the persons on-board. The International Convention on Training, Certification and Watchkeeping for Seafarers (STCW Convention) provides international requirements for skills and training for officers, highlighting the importance of being able to operate the on-board technology to ensure safe navigation and vessel operations (STCW, 1978).

Offshore shipping companies typically provide vessels that support various phases of maritime oil and gas projects, from exploration and development to operation and decommissioning

(Kjerstad, 2017). In recent years, renewable energy has emerged as an alternative income source for this segment as the emphasis on green solutions and sustainability intensifies globally. All vessel activities related to supporting project phases within these areas are considered offshore operations in this thesis. Examples of such operations are transportation of containers and diesel to offshore installations, moving installations (e.g. oil rigs or wind turbines) from one location to another, laying pipelines, transportation of oil, and installation of subsea constructions. Commonly used ship types in these operations are seismic vessels, platform supply vessels (PSV), anchor handling tug supply vessels (AHTS), floating and production storage and offloading vessels (FPSO), shuttle tankers, and construction support vessels (CSV). These modern offshore vessels are usually technically advanced and require the deck officers to constantly update their knowledge and skills in handling the on-board systems. Furthermore, Norwegian shipping companies locate their vessels in various geographical locations, leading the deck officers to work in different parts the world (Kjerstad, 2017). The diversity of vessel locations and the reputation of good working conditions on offshore vessels in Norwegian shipping companies often results in bridge crews composed of officers from various countries.

2.2 Maritime human factors

To fully grasp the complexity of the environment deck officers work within, it is crucial to move beyond just understanding the structure of the offshore industry and the officers' responsibilities and work tasks. It is important to consider the insights gained from research on maritime human factors regarding the complex interplay between human operators and technological systems, which is essential context for understanding how cyber risks are perceived.

The history of maritime accidents has shown that safety and security is of utmost importance in the management and operation of vessels, and several studies have concluded that human factors contribute to errors and mistakes in this regard (Fan & Yang, 2023). Catastrophic events such as the sinking of the passenger ship Titanic (1912), the capsize of the passenger ferry Herald of Free Enterprise (1987), the major oil spill from the oil tanker Exxon Valdez (1989), and the shipwreck of Costa Concordia are all examples of accidents attributed human factors such as mental overload, fatigue, distraction, and situational awareness (Chauvin, 2011; Fan et

al., 2023). Such performance-shaping factors are considered aspects of the working environment and of human behaviour which influence system performance (Bridger, 2021, p. 17). One of the key aspects of understanding human factors is the notion of the fit between the person and their surrounding environment where the performance-shaping factors are not causes but always relevant. Within the maritime operational context, human factors are often associated with navigational factors, environmental factors, operational factors, and organisational factors (Grech et al., 2008).

James Reason's (1990) work on human error and safety is a crucial part of human factors research and emphasises that errors often result from a combination of latent failures at high levels in organisations and active failures at the individual level. This understanding of the human contribution to disasters has provided a theoretical backbone for analysis tools used to understand maritime accidents (Galieriková, 2019). Reason defines "unsafe acts" within active failures as errors or violations committed by individuals in the presence of a potential hazard (Reason, 1990, p. 206). Errors involve unaware deviation of action from intention (slips and lapses) and divergence from the intended plan to achieve a desired goal (mistakes). Violations can be routine, or exceptional, deliberate deviations from practices deemed necessary to maintain safety without prior intention to cause damage (Reason, 1990). Rapid digitalisation and increased automation of on-board systems may cause challenges in comprehending potential cyber risks, leading deck officers to commit unsafe acts (Fan & Yang, 2023).

Another important concept for explaining human behaviour and avoid human failure is situational awareness (SA), which can be understood as "the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future" (Endsley, 1988, p. 792). This definition divides achieving SA into three levels; (1) perception, (2) comprehension and (3) anticipation. This means that deck officers need to perceive the information elements in the environment (1), derive meaning from this perception (2), and then make a projection about the future based on the comprehension of the situation (3) before deciding upon actions to handle in the current situation (Sharma et al., 2019). Several studies have identified loss of SA as one individual factor that can be an immediate cause of maritime accidents (Fan et al., 2023; Hetherington et al., 2006). As human perception and experiences are crucial in building and maintaining SA

(Cordon et al., 2017), understanding factors influencing perceptions of cyber risks can be essential for enhancing SA on-board vessels.

Digitalisation and automation enhance the complexity of the on-board systems, making it harder for deck officers to achieve sufficient SA (Chan et al., 2022; Sharma et al., 2019). James Perrow's Normal Accident Theory (NAT) suggests that complex technological systems cannot be completely safe since they are characterised by tightly coupled components and interactive complexity (Spagnoletti & Za, 2022). Perrow (1999) states that complex interactions may be unfamiliar and unintended sequences of events leading to "normal accidents". These interactions are either not visible or not immediately comprehensible, making it difficult for the human operator to anticipate or perceive the risks of them happening (Perrow, 1999, p. 78).

The maritime human factor research presented in this section is mainly motivated by investigating major maritime accidents. There is limited research applying these frameworks to maritime cyber incidents (Afenyo & Caesar, 2023). Nevertheless, studies on human factors in cybersecurity highlight the potential of applying these perspectives to understand the intersection between humans, systems and organisations in cyber incidents such as the ransomware attack on Maersk Shipping in 2017 (Algarni et al., 2019; Backman, 2023).

2.3 Maritime cybersecurity

With the unique characteristics of the maritime industry and the humans working within it, handling cybersecurity on board vessels poses a significant and complex challenge (Schinas & Metzger, 2023). To fully comprehend the contextual studies presented in this thesis, it is important to understand definitions, cyber incidents, and technological systems involved in maritime cybersecurity. The upcoming sections will provide context and definitions of cybersecurity concepts before further delving into the human element of maritime cybersecurity.

As a reaction to increasing digitalisation and connectivity within the maritime domain, in 2017, the IMO released a statement about the urgent need to raise awareness about cyber risks and threats through efficient cyber risk management strategies. One of the goals of the IMO – the United Nations agency responsible for the safety and security of shipping – is to work towards an industry that is operationally resilient to cyber risks (IMO, 2019). The IMO published a resolution that by January 2021, an approved safety management system on-board vessels

should consider cyber risks, providing the first low-threshold guidelines on maritime cybersecurity (IMO, 2017; Mraković & Vojinović, 2019). Cyber risk management is considered the approach for coordinating activities to direct and control organisations in relation to cyber risks (Refsdal et al., 2015).

Two years after the IMO resolution, the world entered the COVID-19 pandemic, and the push for digitalisation in every sector, including maritime, intensified. Dealing with personnel restrictions and health protocols, shipping companies increasingly adopted digital solutions for their vessels to ensure business continuity. However, the rapid digital transformation introduced additional cybersecurity challenges, with systems hurriedly integrated in new ways, and work processes like maintenance and surveys transitioning to be conducted remotely (Kuhn et al., 2021).

As a result of these digital developments, humans at sea not only interact with the vessels' technology but are becoming potential targets. Therefore, just as we protect our technological systems from cyber risks, we must understand that humans are assets that need protection as well. To substantiate this, this thesis adopts the definition of von Solms and van Niekerk (2013) as an understanding of cybersecurity: "Cyber security can be defined as the protection of cyberspace itself, the electronic information, the Information and Communication Technologies (ICT) 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" (Von Solms & Van Niekerk, 2013, p. 101). This definition is wide enough to encompass both humans working on vessels and the on-board technology (OT and IT), which are essential in the maritime domain.

2.4 Maritime cyber risks and threats

While technological advancements have enhanced operational efficiency, they have also introduced new cyber risks. The term cyber risk is complex, and there are several definitions highlighting different dimensions of this term (Strupczewski, 2021). Refsdal et al. (2015, p. 33) define cyber risk as a risk that is caused by a cyber threat. The European Union Agency for Cybersecurity (ENISA) defines cyber threats as any circumstance or event with the potential to adversely impact an asset through unauthorised access, destruction, disclosure, modification of data, and/or denial of service (ENISA, 2023). Cyber threats present a diverse and complex

challenge and can be classified into two categories based on their origin and intent: malicious and non-malicious.

Malicious cyber threats are orchestrated by actors with a deliberate intent to harm, steal, or disrupt data, systems, or operations. Common methods employed by these actors include malware (malicious software designed to cause harm or exploit any network), phishing (attempts to obtain sensitive data by disguising oneself as a trustworthy actor), and distributed denial-of-service attacks (multiple systems flood a targeted system or resource, causing a denial of service to users (Refsdal et al., 2015). An example can be a nation-state actor utilising malware to compromise a vessel's ballast water systems. Such an attack might have severe ramifications, potentially destabilising the vessel's balance and leading to hazardous situations.

Non-malicious cyber threats are inadvertent threats devoid of any harmful intent and often stem from human mistakes, system malfunction, natural events, or programming errors (Eie, 2020; Refsdal et al., 2015). For example, a crew member unintentionally downloads an update containing a virus, leading to a malfunction in the vessel's Electronic Chart Display and Information System (ECDIS). This incident might lead to a delay in the vessel's departure from port and monetary losses.

Kuhn (2022) stresses that technological change and the flow of serious vulnerabilities make cyber incidents inevitable and that maritime organisations must consider the varied nature of cyber risks to improve their mitigation strategies. A cyber incident is considered an event that has been assessed as having an actual or potentially adverse effect on the security or performance of a system (ENISA, 2023). A cyber-attack is considered a cyber incident caused by a malicious cyber threat. Additionally, a cyber vulnerability is a weakness, flaw, or deficiency that can be exploited by a cyber threat (Refsdal et al., 2015). See the Baltic and International Maritime Council (BIMCO) et al. (2020, p. 3) for an overview of what characterises cyber incidents and vulnerabilities in the maritime industry.

To summarize, cyber risks involves a state of uncertainty that may involve loss, injury, catastrophe, or other undesirable outcomes (Kuhn, 2022). General cyber risks to vessels include, but are not limited to, physical damage (e.g. collision or grounding because of malware infections), interruption of operations (e.g. system breakdown or misplacement of cargo due to denial-of-service attacks), loss of hire (e.g. vessel not seaworthy because of a system

malfunction), data loss (e.g. loss of sensitive personal information from phishing attacks or company data loss from ransomware attacks; (Kuhn et al., 2021; Meland et al., 2021). Understanding these maritime cyber risks is challenging as they are complex, evolving, and asymmetrical (De Smidt & Botzen, 2018).

As the maritime industry has increasingly integrated digital technology into all aspects of vessel management, the industry's exposure to cyber risks has risen proportionally. Meland et al. (2021) conducted a review of maritime cyber incidents from 2010 to 2020 and present a list of the top ten cyber threats to the industry. The Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) also provides an overview of the status of state actors and cyber-attacks in their Annual Threat Assessment of 2023. The overview highlights the impact of the Ukraine War on the maritime sector, with physical and digital disruptions and sanctions. The report also provides examples of successful malware attacks on vessels, and an incident in which malware stemming from a USB-stick was found in the engine control room of an offshore supply vessel (NORMACyber, 2023).

Kuhn (2022) outlines cyber-attacks that occurred between 2019 and 2020, in which diverse tactics were deployed against maritime organisations and their vessels. Notable attacks include GNSS spoofing on the United Kingdom (UK) tanker Sterna Impero, consecutive ransomware attacks on the logistics giant Toll Group, a malware attack on shipping giant MSC, and cyber incidents at ports and major maritime institutions, including a significant incident with the IMO (Kuhn, 2022, p. 4). These events emphasise the potential consequences, both operational and economic, of cyber-attacks in the maritime sector. Responding to the increase in cyber risks, several frameworks and guidelines have emerged to help maritime organisations implement cyber risk management strategies and increase vessel security. One of these, "The Guidelines on Cyber Security Onboard Ships", in particular acknowledges the importance of protecting both OT and IT on board vessels (BIMCO et al., 2020).

2.5 IT and OT systems

Modern offshore vessels contain myriad technological systems that are digitally controlled and networked together through the Internet of Things (IoT), satellite communications, radio technologies, and cloud-based services. These systems range from navigation and propulsion to cargo handling and communications. Ben Farah et al. (2022) provide a comprehensive

overview of vessel components and possible cyber-attacks targeting inherent vulnerabilities within critical vessel systems; they highlight that increasing reliance on IoT and connectivity is motivating cyber criminality, such as phishing, ransomware attacks, and identity theft.

Vessels' systems can be categorised in different manners depending on their purpose and application. When considering maritime cybersecurity and cyber risks, it is common to categorise technological systems as OT or IT. The distinction between these categories lies in the system's primary focus and scope of influence. IT systems are predominantly focused on data management and administrative functions, while OT systems are designed to interact, monitor, and control physical assets and processes (Kessler & Shepard, 2022).

OT systems, as described in BIMCO et al. (2020, p. 7), comprise the hardware and software that directly monitor or control physical devices and processes to the extent that they are an integral part of the ship and must function independently of the on-board IT systems. Unlike IT systems, OT systems are dedicated to the real-time monitoring and control of equipment and tasks crucial for the vessel's physical operations. In this thesis, OT systems refer to all systems critical for the operation of vessels, including, but not limited to, navigational systems, engine controls, cargo-handling equipment, and safety mechanisms.

Several recent papers provide comprehensive overviews of vessel IT and OT architectures, together with records of inherent system vulnerabilities, possible cyber-attack vectors, and significant cyber-attacks within the maritime industry (Akpan et al., 2022; Ben Farah et al., 2022; Kuhn et al., 2021; Meland et al., 2021; Tam & Jones, 2019b). These studies all highlight the growing trend of integrating IT and OT systems, which adversely impacts vessel security. Coupled with limited maritime OT security expertise and the emergence of more advanced cyber-attack techniques, this trend heightens the probability of successful cyber-attacks on vessels (Chubb et al., 2022).

2.6 The human element in maritime cybersecurity

The maritime industry has developed an increased awareness of cyber risks, and shipping companies are recognising the importance of developing holistic cyber risk management strategies. This shift mirrors the understanding that cybersecurity is not merely a technical concern but an essential part of safe and efficient vessel operations (Schinas & Metzger, 2023). While having technology and protective measures in place is crucial, it is increasingly evident

that the human element plays an essential role in securing vessels. Deck officers helps bridge the gap between technology and effective cyber risk management as they are part of the frontline protecting the vessel's technical systems (Erstad et al., 2023; Larsen et al., 2022).

Despite the importance of humans in protecting these systems, the majority of cyber incidents are argued to occur due to human behaviour and actions. Often, the actions are unintentional, such as using weak passwords, accidentally downloading malicious software, or leaving systems unattended. However, there are instances in which intentional actions cause cyber-attacks, driven by motives such as blackmail, discontent, or espionage (Farahmand & Spafford, 2013). Nevertheless, understanding the underlying factors driving human behaviour may also lead to uncovering both latent and active failures within the maritime systems (Fan et al., 2023). Consequently, it is imperative to implement effective strategies to increase the crew's capability to manage all aspects of cyber risks to their vessels and working environment.

A prerequisite for developing and implementing successful cyber risk mitigation strategies is understanding the operational working environment of end users and their behaviour within this context (Bada & Nurse, 2020). Understanding end users' perceptions and tasks might provide necessary context to build efficient security mechanisms (Adams & Sasse, 1999). For instance, every offshore operation, whether relocating a drilling rig or surveying the seabed, has a unique set of challenges and risk factors. The tools, technologies, and procedures in place meet the specific demands of that segment's operations. Therefore, understanding this context is vital as mitigation strategies should be integrated seamlessly without restricting day-to-day operations. Understanding the deck officers' perceptions when interacting with the technological systems needed to perform the operations can also guide the development and implementation of targeted, user-friendly security measures and cyber risk communication strategies, leading to enhanced SA regarding cyber risks in vessel operations (Grech et al., 2008; Van Schaik et al., 2017).

Grasping human perceptual tendencies can provide indications of factors driving SA and decision-making related to cybersecurity. Humans' cognitive processes play a role in how cyber risks are addressed, which affect SA and decision-making at different levels. Therefore, factors such as cognitive biases, previous experience, training levels, and knowledge influence how cybersecurity measures are perceived and adopted by the crew (Roeser, 2012; Sjöberg, 2005). In summary, the operational setting and human perceptions play a defining role in cyber risk

mitigation on board vessels. Understanding what influences underlying cognitive processes, such as perception of cyber risks, will ensure that mitigation strategies are not just technically sound but also tailored to the operational decision-makers in offshore operations.

2.7 Related work

Unsurprisingly, research within the area of maritime cybersecurity has increased alongside the digitalisation of the industry. Bolbot et al. (2022) present a thorough literature review on the topic, providing an overview of identified research categories within maritime cybersecurity. Previous literature reviews within this research area have focused on overarching cybersecurity challenges, system vulnerabilities and cyber threats, relevant regulations and standards, the integration between IT and OT systems, and protective measures against cyber-attacks (Afenyo & Caesar, 2023; Ashraf et al., 2022; Ben Farah et al., 2022; Caprolu et al., 2020; Progoulakis et al., 2021; Schinas & Metzger, 2023). The next sections provide a brief introduction to research related to cyber risk assessments, cybersecurity frameworks, cybersecurity awareness and knowledge, cybersecurity training, and resilience within the maritime domain.

According to Bolbot et al. (2022), the most extensive body of work within the field of maritime cybersecurity comprises studies on methods for the risk identification, analysis, evaluation, and treatment of cyber-attack scenarios on vessels and vessel systems. Many of these studies have investigated methods for jointly implementing cybersecurity and safety risk analysis in the context of autonomous or remotely controlled vessels. For traditional vessels and maritime organisations, Tam and Jones (2019a) proposed a maritime cyber risk assessment framework (MaCRA – Maritime Cyber Risk Analysis model) to evaluate cyber risks in the face of various maritime cyber scenarios, encompassing any combination of ships, systems, environments, and attackers. Meland et al. (2022) developed a threat likelihood estimation approach that supports risk management in maritime systems when there is little or no historical data about past security incidents. Jo et al. (2022) introduced an analysis method based on the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework to identify cyber-attacks in ship systems. Martinez et al. (2024) review existing guidelines and frameworks for maritime cyber risk management before proposing the POSEIDON framework (procedures, operations and standards for the detection of integral events and the development of naval operating capacity).

Moreover, research has shown interest in cybersecurity regulatory frameworks and cyber risk management. Hopcraft and Martin (2018) argue for establishing a holistic cyber code to develop robust maritime cybersecurity regulations. Drazovich et al. (2021) present a systematic analysis of cybersecurity guidelines relevant to the maritime transportation system and identify shortcomings related to the comprehensiveness of each guideline in the industry. On a more positive note, Kechagias et al. (2022) conducted a case study showcasing a maritime company's successful approach to assessing and mitigating cyber risks by implementing procedures and policies for cyber risk management. Furthermore, the study of Kanwal et al. (2022) demonstrated that regulatory frameworks positively influence cybersecurity policies, which in turn positively affects vessel system readiness, monitoring, training and awareness.

Another category of emerging research is survey studies focusing on cybersecurity awareness and knowledge. In 2018, Lee and Wogan investigated cyber preparedness in maritime companies, showing that employees in larger companies are more experienced with data breaches and more confident in their preparation to defend against future attacks than employees in smaller companies. Knight and Sadok (2021) found that employees on cruise ships perceive cybersecurity to be important, but technical and organisational obstacles mean that their perceptions are not reflective of their security behaviour. This also aligns with findings in a study of Croatian seafarers, which argues for the importance of providing education and training to the staff to enhance vessel security (Pavlinović et al., 2022). Erstad et al. (2022) investigated how navigators experience maritime cyber threats and argue for using human-centred principles to design cyber awareness training and education.

Other studies have investigated how to develop suitable training frameworks for maritime cybersecurity. Hopcraft (2021) argues for the need to develop standardised digital competencies for all seafarers by utilising the well-established National Institute of Standards and Technology (NIST) Cybersecurity Framework. Kuhn et al. (2021) designed and tested a game-based cybersecurity exercise to train on incident response in the case of a cyber-attack on a maritime system. In a later study, Kuhn (2022) examined decision-making and support at the senior leadership level. Potamos et al. (2021) employed a maritime cyber range as a basis for developing cybersecurity training scenarios. Potamos et al. (2023) extended this work by building a curriculum for developing skills to handle ransomware attacks on vessels. Erstad et al. (2023) demonstrated the use of human-centred design when developing cyber resilience

training in maritime simulators. Oruc et al. (2024) proposes a cybersecurity training framework of eleven modules to improve cybersecurity knowledge, skills, and attitude of seafarers.

These studies show the growing significance of and attention to maritime cybersecurity. However, there is an overarching trend in research to focus on technical vulnerabilities, regulatory frameworks, and system-level risk assessments, with few studies centred on understanding the cognitive aspects of humans in maritime cybersecurity. While several studies touch upon cybersecurity awareness, SA, decision-making, and resilience, they often fall short of addressing the underlying cognitive processes that influence and drive human decision-making and behaviour. With this context in mind, the next section dives into the theoretical underpinnings of risk perception within the psychological approach, which is one of the cognitive processes known to shape and influence decision-making at various levels of society (Larsen et al., 2022; Short & Rosa, 2004).

3 Theoretical Foundations

This section provides an overview of the theoretical underpinnings within the psychological approach that guide this thesis's exploration of risk perception. Understanding risk perception requires a solid understanding of the chosen paradigm and its foundational concepts. This section first presents the conceptual foundation of risk and then the psychological approach. Next, it explores perceived benefits in the realm of revealed and expressed preferences, which leads to the psychometric paradigm. Lastly, it discusses trust as an influential factor in risk perception and concludes with a presentation of frequently used heuristics and biases within the risk domain. The section aims to offer robust theoretical anchoring to ensure that the empirical investigations and discussion are grounded in well-established academic paradigms and theories.

3.1 The conceptual foundation of risk

Risk research is a discipline with contributors from many areas of the natural and social sciences. This range can be seen as a reflection of a growing concern about risks in society, as modern social systems aim to reduce complexity and define criteria for effective risk management (Slovic, 1990; Vasvári, 2015). The responses to what criteria are appropriate and who should design these criteria depend on the underlying risk paradigms or theoretical frameworks adopted in the given context. For example, if risk is seen as objective and measured as the probability of an undesired event, resource allocation would be based on reducing the greatest risks first. In contrast, if risk is seen as a social construction, resource allocation and priorities should reflect social values and preferences (Renn, 1992, 2004). The case of nuclear power exemplifies this dichotomy. While statistically the risk of a nuclear disaster is rare, public fear of the consequences of a potential nuclear disaster makes it necessary to account for the social and psychological ramifications of such an event.

Given the influence of risk perspectives on the understanding of a particular problem, it is crucial to apply the appropriate risk concepts to match the required tools for proper risk management. Scholars have identified various risk categories tailored to specific contexts, and a prevalent categorisation divides risk into three overarching approaches: the scientific, the psychological, and the cultural (Möller, 2012).

The scientific approach enables a meticulous examination of risk by employing scientific methodologies, thereby facilitating systematic and replicable measurements of risk. Research employing this approach depends on statistical and probabilistic tools to describe risks, quantify uncertainties, and predict potential outcomes (Vasvári, 2015). Risk, viewed through the scientific approach, can be objectively analysed and managed based on quantifiable metrics. This approach is commonly used in research fields such as engineering, environmental sciences, epidemiology, and finance (Roeser, 2012).

In comparison to the scientific approach, which seeks to quantify risk through empirical data, the psychological approach considers people's perceptions of risk and places greater emphasis on individuals' subjective judgements (Spencer, 2016). This includes studying how individuals process information, their emotional reactions to potential hazards, and the biases and heuristics that influence their judgements (Tversky & Kahneman, 1974). Within this framework, even effect measures, probabilities, and aggregation methods are viewed as subjective. As a result, what emerges is a subjective expected value derived from perceived probabilities, as opposed to objective or absolute probabilities (Vasvári, 2015).

The third category, the cultural approach, emphasises the role of societal contexts in shaping perceptions of risk. Instead of relying on empirical data or individual psychology, this approach investigates how shared values, traditions, narratives, and societal norms influence collective interpretations and responses to potential hazards (Möller, 2012). In research fields such as anthropology, sociology, cultural studies, and communication studies, the cultural approach is prominently employed, reflecting the deep influence of societal norms and values on perceptions and behaviours.

Because this thesis's main objective is to explore individual perceptions of cyber risk within a specific context, the psychology approach to risk is applied. This choice is informed by the approach's fundamental emphasis on understanding individual cognition, emotion, and behaviour in relation to people's perceptions of risks (Slovic, 1987). However, it is essential to acknowledge the distinction between reality and possibility as a common element across all risk concepts. Renn (1992) articulated this notion by suggesting that the very term "risk" would be meaningless if the future were either predetermined or completely independent of human activities. Under such circumstances, there would be no need to anticipate future outcomes as negative consequences would be inevitable. This understanding remains applicable in the

context of cyber risks and denotes risk as the possibility that an undesirable state of reality may occur as a result of natural events or human activities (Renn, 1992, p. 55). With this as a foundation, the following theoretical discussion elaborates on risk perception theories within the psychology approach and how these apply to cyber risks.

3.2 The psychology approach to risk perception

Early psychological studies on risk perception comprised empirical investigations into probability assessments, utility assessments, and the mechanisms of decision-making (Slovic, 1987). The goal was to highlight structures and processes of individual risk perception, with a focus on the cognitive and affective aspects of perception processes. Here, the term perception is understood as the mental processes through which a person takes in, deals with, and assesses information from the environment via their senses (Renn, 2004, p. 406). In turn, risk perception is the process by which people construct their own reality and reconstruct previously assimilated risk through subjective judgements (Fischhoff et al., 1978; Kahneman et al., 1982; Slovic, 1990). This mental process is constructed by how information about the risk source is communicated, the psychological mechanisms for processing uncertainty, and earlier experience. These notions and associations help individuals understand their surroundings, influence their reaction to technological risk, and drive decision-making processes at various levels of society (Renn, 1992; Sjöberg, 2004).

Siegrist and Árvai (2020) underscore the importance of understanding risk perception and the factors that influence it by highlighting how people's behaviour changes after incidents of high impact on society, the environment, or themselves. Examples of such changes are the implementation of an international safety convention at sea in response to the sinking of the Titanic in 1914 (IMO, 2023), the opposition towards – and fear of – nuclear power and radiation after the Chernobyl accident in 1986 (Drottz-Sjoberg & Persson, 1993), and the rapid changes in people's behaviour as a response to the COVID-19 pandemic (Kuhn et al., 2021). Such examples indicate that how people perceive risk is important because it influences individual behaviour, decision-making, and the acceptance of technologies, policies, and norms, which, in turn, have implications for risk exposure, risk communication, and risk management. There are several notable paradigms within the psychology approach of risk perception (Siegrist &

Árvai, 2020), and the following sections elaborate on revealed and expressed preferences, the psychometric paradigm, trust in risk perception, and heuristics and biases.

3.3 Perceived benefit within revealed/expressed preferences

Historically, perceptions of risk and benefit have changed as societies evolved and technologies advanced. Previous studies have shown that people tend to tolerate certain risks if the perceived benefits outweigh them. The studies of Starr in 1969 and Fischhoff et al. in 1979 have served as foundational to many subsequent investigations into perceived risk and benefit within the psychology approach.

Starr's "revealed preference" approach was developed based on data of past behaviour for weighing technological risks against benefits to investigate the optimum balance between the risks and benefits associated with any activity (Slovic, 1987). This approach has the benefit of investigating people's behaviour rather than their attitudes. However, the revealed preference has been debated at length; the method has been criticised assuming that past behaviour is a valid indicator of present preferences and that the quantitative analysis of marked behaviour accurately reflects the public's safety preferences (Fischhoff et al., 1978; Slovic, 1990).

Following the debate around Starr's methodology, Fischhoff et al. (1978) introduced the "expressed preference" approach. This alternative approach uses questionnaires to measure people's attitudes towards the risks and benefits of various activities and technologies. Such studies focus on obtaining present values rather than historical preferences and suggest that societies may accept higher levels of risk for beneficial activities and tolerate higher risk levels for voluntary activities (LeBlanc & Biddle, 2012). The use of psychometric questionnaires has been criticised for assuming that people provide meaningful answers to difficult questions and that responses to hypothetical questions align with actual behaviour. Even so, this approach is well recognised and widely used (Sjöberg, 2005; Sjöberg et al., 2004). The insights obtained from the "expressed preference" approach, especially those by Fischhoff et al. (1978), played an important role in laying the groundwork for the more comprehensive framework named the psychometric paradigm.

3.4 The psychometric paradigm

Within risk perception research, the psychometric paradigm stands out as an important framework that has significantly shaped understanding of how individuals perceive and assess risks. This paradigm, as pioneered by Slovic, Fischhoff, and Lichtenstein, sought to identify key dimensions through which people evaluate risks (Siegrist & Árvai, 2020). Their research determined that people not only consider the statistical probability of harm but also have nuanced and multidimensional views of risks. Research within this paradigm primarily uses quantitative techniques to measure people's perceptions, beliefs, and attitudes towards various risks and seeks to address questions such as, Why do people feel more threatened by some hazards than by others? Why are certain risks acceptable while others are not, even if they have similar probabilities or consequences (Slovic, 1990)?

The original model in the psychometric paradigm is based on explanatory scales, such as New–Old and Voluntary–Unvoluntary, and outlines nine dimensions of risk perception. Table 1 gives a brief overview of the frequently used dimensions within this framework (Farahmand et al., 2009; Fischhoff et al., 1978).

Table 1: *Nine dimensions of risk perception within the psychometric paradigm (Fischhoff et al., 1978)*

Voluntariness	Risks that are taken voluntarily, like skydiving, are generally perceived as less threatening than involuntary risks, such as being exposed to pollution.
Immediacy of Effect	Immediate threats, such as major plane accidents, are viewed differently from long-term risks, like developing cancer due to prolonged exposure to a hazardous substance.
Knowledge to the Exposed	Risks are perceived differently depending on whether the affected individuals are aware of and understand the risk.
Knowledge to Science	There is a distinction in perception between risks that science understands well and those that are less known or involve more uncertainties.
Control	Risks that individuals feel they have personal control over, such as driving a car, are generally seen as less threatening than uncontrollable risks, like natural disasters.
Newness	Novel risks or those that are new to science or society can be perceived as more threatening than familiar risks.
Chronic vs. Catastrophic	Chronic risks, which cause harm over a longer period, such as smoking, are perceived differently from catastrophic risks that cause immediate widespread harm, such as nuclear accidents.
Dread	This dimension pertains to the sense of fear and terror associated with a particular risk. Risks that evoke a high level of dread, such as terrorist attacks, tend to be perceived as more threatening.
Severity of Consequences	This dimension relates to the potential harm or impact of the risk. The more severe the potential outcomes, the higher the perceived risk.

These the nine dimensions are often reduced by factor analysis to the two influential factors of dread risk and unknown risk. These two compiled factors seem to support many of the distinctions in how people perceive risk. Dread risk relates to how much fear or anxiety a certain risk evokes and encompasses the dimensions related to catastrophic potential, lack of control, involuntary nature, and threat to future generations (Fischhoff et al., 1978). Unknown risk (or unfamiliarity) concerns how well understood and known the risk is to individuals and captures the dimensions related to the degree to which the risk is known to science and those exposed, its newness, and the observability of its effects (Slovic, 1990). These two factors have become central to discussions regarding why some risks, even those with low probabilities, can provoke strong public reactions. The insight gained from these dimensions has allowed for a broader understanding of public attitudes towards various hazards, such as technological risks (nuclear power or gene technology), health risks (smoking or blood transfusion), or environmental risks (earthquakes or flooding; (Siegrist & Árvai, 2020). By realising that perception is shaped by these subjective, qualitative factors, and not just objective data, risk communicators, policymakers, and industries can better address concerns and develop more effective risk communication strategies (Renn, 1992).

The psychometric paradigm is part of this thesis theoretical foundation because of its well-established approach to understanding qualitative dimensions of risk perception, such as knowledge and personal control. Its comprehensive framework aligns with the main objective of exploring deck officers' cyber risk perceptions, providing insights into the emotional and cognitive dimensions of the officers' attitude towards cyber risks. Unlike the Protection Motivation Theory, which focuses on people's motivations and behavioural intentions to protect themselves against threats (Haag et al., 2021), the psychometric paradigm's broad approach is more aligned with this thesis's exploratory nature.

Despite its contributions, the psychometric paradigm has been subject to several criticisms and debates. The framework does not adequately address how and why individuals differ in their judgements of risk, and the use of aggregated data creates a stronger correlation between the dimensions than would be observed in the raw data (Siegrist et al., 2005). This leads to a focus on how the characteristics of hazards result in different responses by individuals and not on how individual differences may result in different perceptions of risk (Siegrist & Árvai, 2020, p. 2193). Moreover, the use of aggregated data frequently leaves a significant portion of

variance in individual differences unexplained. The potential for drawing misleading conclusions from analyses at this aggregated level has been widely discussed and may be referred to as an "ecological fallacy" (Sjöberg et al., 2004, p. 18). Despite these criticisms, the psychometric paradigm remains a foundational model in risk perception research. It provides a structured way to measure people's attitudes towards various risks and is useful for highlighting the relative positionality of risks encountered in everyday life (Siegrist et al., 2005). However, as with all models, it is essential to consider the model's limitations and the broader context in which risk perceptions form and evolve.

3.5 Trust

The need for trust arises in uncertain environments and risky situations, making trust particularly important where complex systems generate risks different from routine experience (Chryssochoidis et al., 2009). According to Siegrist (2021), trust mechanisms play a crucial role in shaping people's perception of risks and acceptance of technologies by reducing decision-making complexity in complex environments. As people depend on each other, and increasingly on technology, to perform their duties within modern society, trust becomes essential in enabling both physical and technology-mediated interactions between people themselves and the technology they depend on (Riegelsberger et al., 2005). Without trust to facilitate and enable interactions, technological progress and economic wealth would be impossible (Freudenburg, 1993).

The concept of trust can be challenging to define due to its elusive nature and the lack of consensus regarding what the term entails and its dimensionality (Chryssochoidis et al., 2009; Earle, 2010). However, it is postulated that many trust researchers within the risk domain accept some version of the following definition: "Trust is a psychological state comprising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another" (Rousseau et al., 1998, p. 395). Within this definition, trust is often understood as two-dimensional, one that is based on social trust and one that is based on confidence (Siegrist, 2021).

Social trust relates to the judgement of similarities in intentions and values (Siegrist, 2021), which encompasses trust in organisations, regulatory bodies, industries, and other collective entities. Studies show that people often trust institutions with values similar to their own (Earle

& Siegrist, 2008). For instance, if a deck officer is unsure about the risks of a recently installed safety management system, they might rely on their trust in the maritime regulatory bodies, the suppliers of the system, or their shipping company's IT department.

In contrast, confidence is based on past experiences that suggest that future events will occur as expected (Siegrist, 2021, p. 483) and believing that others can effectively do what they claim. Confidence is argued to be closely related to "competence trust", which is trust in others' skills and abilities (Siegrist et al., 2003). Studies on confidence indicate that if people believe that an organisation or a system is competent, they are more likely to trust its risk assessments or recommendations (Earle et al., 2012). For example, the deck officers' confidence in the expertise and capabilities of the nation's maritime regulatory agency or coastguard in assisting them during a cyber-attack can greatly influence how they perceive and respond to the associated risks.

The conceptual difference between social trust and confidence is important because trust is not an appropriate term to describe reliance on technological systems (Siegrist, 2021). Trust in a person differs from trust in an object, such as a vessel or a car; for example, technology may not function as expected, but it will not "deceive" people because it does not have the intention of doing so unless it is manipulated or designed for this purpose. This is why people can be sceptical of an industry but still use the technology it offers. However, it might be difficult, or even impossible, to decide if a questionnaire item is measuring trust or confidence. Consequently, people base their trust on either performance or on value aspects as interpretations about the context and the participants' knowledge tend to vary when answering such questionnaires (Earle et al., 2012; Siegrist et al., 2000).

The development and use of technology introduce complexity in various situations, and trust is critical if people possess limited knowledge about the risks and hazards in question (Siegrist, 2021). For instance, studies on gene technology indicate that people use their levels of trust in industry or governmental agencies to assess the risks associated with the technology (Siegrist, 2000). People might find it hard to understand gene technology, and as a result, their risk perceptions are not based on scientific data but on their trust in the stakeholders that produce and regulate such technologies. If there is high trust in those stakeholders, there is an increased likelihood of technology acceptance and lower associated risks (Siegrist et al., 2000). Trust does not just affect risk perception; it also influences behaviour. When people trust the sources

or entities associated with a particular technology or practice, they are more likely to accept and adopt it. This acceptance extends to buying products, supporting policies, or even advocating for the technology in question. In contexts in which trust has been found relevant for people's perception of risk, it seems that degree of knowledge, the perceived importance of the issue, and the way trust is measured are relevant for the observed correlation (Earle et al., 2012).

Technological development enables more interactions between humans over distance and is increasingly replacing traditional forms of physical interactions. Relying on digital technologies to communicate or learn about the world mediates experiences through a combination of objects, interfaces, and software (Bodó, 2021, p. 2675). Riegelsberger et al. (2005) propose a framework for technology-mediated interactions focusing on contextual and intrinsic properties that support trustworthy behaviour. The contextual properties of temporal, social, and institutional embeddedness provide incentives for an actor to behave in a trustworthy manner. Temporal embeddedness refers to the trust developed over repeated interactions, considering past interactions and future expectations. Social embeddedness considers how trust is influenced by social networks and dependent on the reputation of the trusted actor. Finally, institutional embeddedness relates to organisational control structures, processes, and norms shaping the behaviour of employees and the expectations of the trusting actor. These contextual properties provide a complementary view of trust aspects in technology-mediated interactions by looking at factors leading to trustworthy behaviour of the trusted party (Riegelsberger et al., 2005).

The multidimensional and context-dependent nature of trust makes it difficult to operationalise the concept and develop valid measurements. Creating instruments that are both valid (accurately reflect the true essence of trust) and reliable (consistently measure trust) is a significant research challenge. Furthermore, trust is one of many factors influencing risk perception and behaviour, and its effect may be intertwined or overlap with individual knowledge, past experiences, societal values, and emotional responses (Earle, 2010). This overlap complicates the task of isolating the influence of trust on risk perceptions, making it essential to approach the research findings with a degree of caution. The inclusion of trust as a theoretical aspect in this thesis is grounded in findings from the qualitative study, which

highlighted its importance in handling cyber risks related to vessel systems. This prompted further investigation of trust in the subsequent questionnaire study.

3.6 Heuristics and biases

A major development within psychological research on risk perception was the discovery of a set of mental strategies that people use to make sense of an uncertain world (Kahneman et al., 1982). These strategies are called heuristics, meaning that they replace a target attribute that is not cognitively attainable (e.g. the objective probability of a malware attack) with a seemingly related attribute that comes to mind more easily (e.g. the number of recalled malware-attacks) (Kahneman, 2011). These rules of thumb, or mental shortcuts, are useful in many circumstances, but they also lead to biases with serious implications for risk assessment (Slovic, 1987). Such cognitive biases can be described as a systematic discrepancy between the "right" answer in a situation and the decision-maker's actual answer (Montibeller & Von Winterfeldt, 2015, p. 1231). For instance, Kahneman and Tversky (1973, 1974) and Kahneman et al. (1982) conducted various laboratory experiments showing that people's subjective assessments of probabilities are influenced by media coverage, personal experience, anxiety leading them to deny uncertainty, overestimation or underestimation of risks, and judgements based on unjustified confidence.

It is important to emphasise that reliance on heuristics in shaping risk perceptions and decisions does not imply irrationality. Moreover, relying on heuristics does not necessarily lead to biased judgements. Heuristics provide individuals with cognitive tools to make decisions under uncertainty, and on many occasions, these decisions result in rational judgements or accurate estimates (Siegrist & Árvai, 2020). These cognitive processes help the brain interpret the world consistently over time, imparting a sense of stability that makes individuals capable of handling stressful and unfamiliar situations.

Previous research has identified a large set of heuristics that people might use when making decisions, as well as biases that result from relying on such heuristics (Kahneman, 2011; Montibeller & Von Winterfeldt, 2015). Though it is beyond the scope of this thesis to account for all these heuristics and biases, the next sections provide a brief overview of the availability heuristic and optimistic bias, which are frequently used and studied in the risk domain and in the context of cyber risks (Siegrist & Árvai, 2020). The rationale for focusing on the availability

heuristic and optimistic bias in this thesis are twofold. Firstly, both the systematic literature review and the findings in the qualitative study revealed a prominent focus on optimistic bias. Secondly, the reliance on the availability heuristic is known for leading to biases such as the optimistic bias and influence multiple dimensions within the psychometric paradigm (Bada & Nurse, 2020; Larsen & Lund, 2021).

3.6.1 The availability heuristic

One of the most influential heuristics in risk perception is the availability heuristic, which refers to the tendency of individuals to estimate the likelihood of an event based on how easily examples of that event come to mind (Tversky & Kahneman, 1973). Essentially, events that are more memorable, recent, or emotionally charged are often perceived as being more probable than they actually are. Availability is useful for assessing frequency or probability since occurrence of large (or very frequent) groups are usually recalled better and faster than occurrences of less frequent groups. However, Tversky and Kahneman (1974) stress that availability is affected by factors other than frequency and availability, leading to predictable biases.

Familiarity and salience affect the ability to retrieve instances (Montibeller & Von Winterfeldt, 2015). For example, events that are extensively covered by the media, such as high-profile cyber-attacks or substantial data breaches within the health sector or within municipalities, imprint on individuals' consciousnesses. As a result, the media spotlight might amplify the perceived risk, making similar threats seem more imminent or prevalent than they statistically are and making other areas prone to the same risk more forgettable. Salience relates to the impact of seeing or experiencing something in real life. That is, experiencing a ransomware attack likely impacts on a person's subjective probability more than reading about a cyber-attack in the paper (Tversky & Kahneman, 1974).

The bias of imaginability also plays an important role in evaluating probabilities because the ease with which disasters or risks come to mind does not necessarily reflect the actual likelihood of them occurring (Kahneman, 2011). If the potential consequences of connecting a vessel's propulsion system to the internet are difficult to imagine or do not come to mind, the cyber risks involved in doing so might be underestimated.

Lastly, the availability heuristic provides an explanation for the illusory correlation bias, which refers to the perception that there is a stronger association between two events than actually exists (Tversky & Kahneman, 1974). It is the tendency to see relationships in certain situations due to subjective beliefs, even when no relationship exists statistically. The bias can emerge from the strength in the associative bond between these events, leaving a judgement that the events have been frequently paired (Tversky & Kahneman, 1973). For example, if an individual has one negative experience with the IT department in their company, they might prematurely conclude that all IT departments are similarly inefficient or unhelpful, even if this is not generally the case.

In summary, the availability heuristic serves as a useful cognitive shortcut, enabling quick decisions without extensive information gathering. However, it is not fully clear in which situations and contexts people rely on this heuristic, making it difficult to operationalise and measure (Siegrist & Árvai, 2020). Furthermore, as the examples above illustrate, it also carries the potential for bias. Over-reliance on the availability heuristic can lead to a misjudgement of actual risks and lead people to believe that they are less, or more, susceptible to negative outcomes, which is often called optimistic bias (Kahneman, 2011; Weinstein & Klein, 1996).

3.6.2 Optimistic bias

Studies on comparative risk assessments might explain why people are concerned about various risks (e.g. cyber risks like phishing or social engineering) and still engage in risky behaviours (like visiting unsecure websites or casually signing up for newsletters). Historically, researchers have shown that there is a systematic discrepancy between how individuals assess their own risk of experiencing negative events and their peers experiencing them (Weinstein & Klein, 1996). This tendency, termed “unrealistic optimism” or “optimistic bias”, occurs when people believe they are more likely to experience positive outcomes and less likely to face negative outcomes than others. It is consistent across different cultures, genders, educational backgrounds, and ages (Campbell et al., 2007).

For instance, previous research has shown that individuals frequently underestimate their health risks compared to others of the same age and gender. This bias extends to various health concerns, including cardiac disease, cancer, and influenza (Rhee et al., 2012; Weinstein, 1987). Optimistic bias also appears in other areas, such as perceptions of car accident risks or

becoming a crime victim. Previous research has found the same effect when people evaluate their risk of being exposed to cyber incidents; that is, they believe that others are more exposed to cyber risks than they are themselves (Cho et al., 2010; Haltinner et al., 2015).

In 1980, Weinstein identified several factors that influence optimistic bias in risk perception, such as perceived desirability, probability, controllability, and personal experience. The perceived probability of an event and its desirability were related to optimistic bias in positive events. In contrast, for negative events, personal experience and perceived controllability were strongly correlated with this bias (Weinstein, 1980). Controllability is the attribute that has received the most attention, displaying a strong correlation with optimistic bias; that is, people who believe they have control over potential threats experience lower levels of anxiety (Rhee et al., 2012, p. 224). The social distance of a comparison target has also been shown to influence the degree to which people display optimistic bias, meaning that optimistic bias seems to be greater when people compare themselves to an average person than when they compare themselves to a specific target, such as a friend or colleague (Rhee et al., 2012; Weinstein & Klein, 1995).

Maintaining positive beliefs and displaying unrealistic optimism can have positive effects, such as heightened motivation and sustained persistence during challenging situations. However, much of the research on optimistic bias has focused on the potentially disadvantageous consequences of not engaging in self-protecting behaviour due to unrealistic beliefs. If someone believes that it is unlikely that something negative will happen to them, they might indulge in riskier behaviour or neglect to take reasonable precautions. Consequently, such skewed perceptions amplify the risk of encountering undesired or harmful events (Campbell et al., 2007). This implies that if deck officers believe they are less susceptible to cyber risks than their peers, they might neglect necessary precautions.

4 Methodological Considerations

This section outlines the research design and the methodological considerations taken in each phase of this thesis. To investigate the main objective – exploring deck officers' cyber risk perception – a sequential mixed methods design was chosen. This design allowed for each phase to inform the subsequent one, resulting in a logical and informed research flow. The research methods used within this design were a systematic literature review, in-depth interviews, and a self-administrated questionnaire. Consequently, this section provides a rationale for choosing the research design and elaborates on how the three research methods were operationalised according to Figure 1. Prior to delving into these topics, a brief discussion of the philosophical assumptions influencing the research processes is provided.

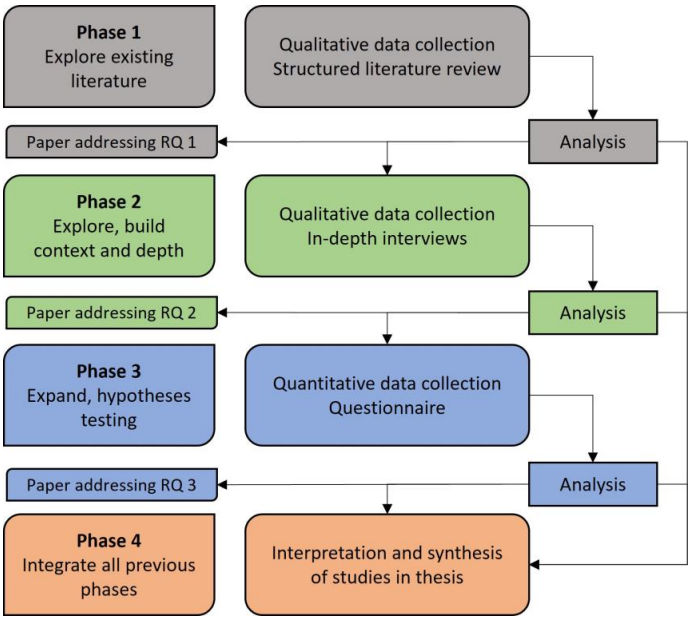


Figure 1: *Research strategy with sequential exploratory design*

4.1 Philosophical assumptions

Scientific research is built on sets of beliefs and philosophical assumptions. Creswell and Creswell (2023) use the term worldview to mean "a basic set of beliefs that guide action" (p. 7). As understanding the researcher's underlying assumptions and worldviews is essential for contextualising the methodological decisions made throughout the research process, this

section clarifies the paradigms upon which this thesis is built. Given the sequential design, different phases of the research are anchored in distinct philosophical traditions (Creswell & Creswell, 2023). The qualitative phases, for instance, draw on constructivist traditions, focusing on the construction of meaning and the interplay between the researcher and participants. Conversely, the quantitative phase aligns more closely with positivist traditions, emphasising empirical observations and the pursuit of objective patterns within the data.

From a constructivist perspective, reality is not seen as a singular, fixed entity waiting to be discovered but rather as being continually shaped and reshaped by individual experiences and interactions. This viewpoint holds that there can be multiple valid constructions or interpretations of reality, each influenced by individual perspectives and sociocultural contexts. Within this paradigm, knowledge is not found or measured but co-constructed (Creswell & Creswell, 2023; Creswell & Poth, 2018).

The systematic literature review of the first phase was conducted using a constructivist approach. While this phase may appear to be an objective synthesis of existing knowledge, the process of reviewing, synthesising, and interpreting literature can be constructive. The choices made about which studies to include, how to interpret their findings, and how to present them were influenced by my perspective and prior understanding as a researcher, with knowledge emerging not just from the literature but also from the interpretive act.

Following this phase, the in-depth interviews aimed to deeply understand and interpret deck officers' experiences and perceptions. The insights gathered were co-constructed, emerging from the interplay between the researcher and the participants. The researcher's active role is acknowledged, with a recognition that the findings reflect a combination of the participants' voices and the researcher's interpretations, background, and worldview (Creswell & Poth, 2018). This process of generating knowledge emphasises the richness and depth of insights that a constructivist approach offers.

The positivist paradigm holds that knowledge is primarily derived from empirical and observable phenomena. Within the positivist framework, the researcher is an objective observer, striving to uncover generalisations about the world through structured observation or experimentation (Ringdal, 2018). From the perspective of this paradigm, there is an objective reality that can be increasingly understood through empirical facts. Working from it, the

researcher should aspire to conduct research that is free from their own biases and values, operating under the premise that objective and neutral investigations can lead to more valid and reliable conclusions. While this approach has its strengths, especially in producing quantifiable and generalisable findings, it has also been critiqued for potential oversimplifications and neglect of subjective human experiences (Creswell & Creswell, 2023).

Transitioning from positivism, postpositivism acknowledges the existence of an objective reality but also recognises the inherent limitations in our ability to know that reality fully. Unlike the pure positivist stance, postpositivism understands that all observations and interpretations are fallible and influenced by existing theories and biases (Creswell & Creswell, 2023). Within this framework, the researcher assumes a detached role while also acknowledging and remaining reflective about potential biases. While the questionnaire study in this thesis was guided by empirical and systematic methods within positivist traditions, it was conducted through a postpositivistic lens. This means that while observable patterns are investigated based on defined hypotheses, I maintained an awareness that findings are conditional and open to revision (Creswell & Poth, 2018).

Nevertheless, the overarching philosophy guiding this study is pragmatic. In the research context, pragmatism is inherently flexible and action-oriented. Rather than becoming entangled in the debates between constructivism and positivism, pragmatism is driven by the research problem itself. This paradigm is concerned with which practical methods and approaches can best illuminate the issues investigated. Therefore, the choice of method – whether qualitative or quantitative – is dictated by its utility and relevance to the research questions at hand (Creswell & Creswell, 2023).

A pragmatic lens acknowledges that no single method can capture the entirety of a complex issue, such as maritime cyber risk perception. Hence, by combining qualitative insights from individual experiences with quantitative data revealing broader patterns, this study adopts a pluralistic approach (Creswell, 2022). Pragmatism also recognises the role of values in research. Accordingly, this approach does not claim to take a detached, value-neutral stance but accepts that interpretations are, in part, shaped by the researcher's beliefs and experiences (Creswell & Poth, 2018). However, the focus remains on generating useful, actionable knowledge, emphasising outcomes and practical implications.

4.2 Mixed methods research: An exploratory sequential design approach

Creswell (2022) defines mixed methods research as "a methodology to research in the social, behavioural, and health sciences in which the investigator gathers both quantitative and qualitative data, integrates or combines the two, and then draws interferences from the integration that provides insight beyond what can be learned from the quantitative or qualitative data" (p. 2). This methodological approach utilises the strengths of both qualitative and quantitative research traditions. By combining these methods, researchers can capture the depth, nuance, and context from qualitative data and complement it with the breadth, generalisability, and statistical power of quantitative data (Creswell & Creswell, 2023). Several research designs fall under the umbrella of mixed methods, ranging from those that simultaneously handle both quantitative and qualitative methods to those that emphasise the different methods in sequential phases. The choice of design often relies on the research objectives and the study context (Creswell, 2022).

The primary objective of this thesis is to explore deck officers' cyber risk perceptions in depth. Given the emerging nature of maritime cybersecurity and the limited existing literature on cyber risk perception in this context, an exploratory sequential design approach was deemed most appropriate. This design begins with a qualitative exploration of a phenomenon, followed by a quantitative phase that builds on and generalises the qualitative findings. In this thesis, data collection was planned in three sequential phases, with each phase's outcome informing the subsequent one. The following sections will delve into the specifics of these phases: (1) systematic literature review, (2) qualitative study with in-depth interviews, and (3) quantitative study with questionnaire.

4.3 Systematic literature review

In the first phase of this research project, I familiarised myself with the particular research areas of maritime cybersecurity and risk perception. As I was not deeply familiar with these topics before, it was crucial to gain an overview of the relevant literature. The main idea was to review the application of psychological models investigating cyber risk perception and make recommendations that could inform the subsequent phases of this study.

Following the guide by Okoli and Schrams (2010) on conducting a systematic literature review, the aim in this phase was to write a structured review that was systematic, explicit, comprehensive, and reproducible. The main objective was to investigate the current state of research within psychology approaches to cyber risk perception in general and to the maritime domain specifically. By understanding the landscape of cyber risk perception research, gaps related to the maritime domain could be identified. The review also gave me an opportunity to grasp key concepts and definitions within the chosen research areas.

The systematic literature review was planned in four phases according to the chosen guidelines. Before embarking on the execution, a protocol was developed for the training, criteria refinement, and testing of search strings (Okoli & Schabram, 2010). Eight databases were chosen due to the multidisciplinary nature of the research area. For the final protocol used to execute the review, see Appendix 1, which provides details of each phase in the process and information about the chosen databases, key words, and search strings. The searches were subject to no time limitations and were conducted during June 2021. Key inclusion and exclusion criteria were established for the practical screening, and the selection phase uncovered 99 articles. Criteria were developed to assess the quality of the 99 articles, and this quality appraisal phase resulted in a reduction to 25 papers. The criteria for the practical screening and quality appraisal are included in the protocol (Appendix 1).

The research questions guided the data extraction process from the 25 eligible papers. Information about context, methodology, research questions, findings, and conclusions was systematically extracted from the papers. This served as the material for the synthesis stage, consisting of a qualitative synthesis of both the quantitative and qualitative studies within the literature review (Okoli & Schabram, 2010). The analysis of the relevant papers resulted in a list of significant dimensions affecting cyber risk perception in different online environments. Dimensions within the psychometric paradigm and cognitive biases were elaborated on and provided the foundation for the qualitative study in the subsequent phase.

4.3.1 Strengths and limitations

Conducting a systematic literature review for this thesis was crucial to achieving a comprehensive understanding of the available literature, and it provided a high standard of rigour to the theoretical background. The structured approach ensured comprehensiveness and

reproducibility and minimised biases, providing a sound foundation for justifying future research directions. Furthermore, acquiring the skills to plan and execute a literature review is a valuable skill when pursuing an academic career as it ensures that research is grounded in a thorough understanding of existing knowledge.

However, one of the challenges faced in this research was the nascent evolutionary state of the cyber risk perception research field, especially in the maritime context. While a literature review ensures comprehensive coverage of existing studies, it is also bound by the available literature. In this case, in which limited studies were available, the review results might not provide the best knowledge that more time could give. Although this limitation had its challenges, it highlighted the novelty and importance of the research conducted in this thesis. As the field of maritime cybersecurity is growing, particularly with an increased focus on human behaviour, we can anticipate a significant knowledge expansion in the coming years.

4.4 Qualitative study with in-depth interviews

The initial phase of this study revealed the limited studies available within research on maritime cyber risk perception, so a qualitative approach using constant comparative analysis (CCA) was chosen to explore this phenomenon within offshore operations. CCA focuses on developing theory grounded in empirical material and is suitable for research questions for which theories are not able to explain the research problem, theories need to be developed further, or there is a need for an analytical analysis method (Corbin & Strauss, 2015; Creswell & Poth, 2018). It provided an appropriate methodological approach for this study in which the main objective was to develop a contextual model with descriptions of factors influencing deck officers' cyber risk perception in offshore operations. Grounded in data collected from participants' experiences of offshore cyber risks, an iterative process was used to develop thick descriptions as a foundation for the contextual model (Postholm, 2019).

4.4.1 Participants and sample size

Theoretical and purposeful sampling was conducted to ensure that the participants could contribute to the development of thick descriptions. Theoretical sampling is a key feature in CCA, for which the researcher collects data that will maximise the opportunities to develop

concepts and identify relationships between them (Corbin & Strauss, 2015). Inclusion criteria were deck officers working offshore with some years of operational experience.

The participants were primarily recruited through my professional network and targeted requests in Facebook groups for Norwegian seafarers. The study was completed with interviews with nine deck officers: six participants were recruited through acquaintances and three participants through Facebook groups. While using personal networks can introduce bias, I recruited participants based on them being deck officers working in the offshore industry. I had no prior personal or professional relationship with eight of the nine participants, and the one participant I was acquainted with had no contact with me over the past four years. Recruiting through my professional network was deemed necessary due to access considerations. The interviewees were working offshore at the time of the interviews and had between five and 25 years of working experience at sea. Within the sample size, theoretical saturation was pursued. The data are believed to be sufficient to give descriptions of deck officers' cyber risk perception within the chosen context of offshore operations (Creswell & Creswell, 2017).

4.4.2 Data collection

Data were collected using semi-structured, in-depth interviews. Four interviews were conducted face-to-face with the participants, and five were conducted digitally through Microsoft Teams as the COVID-19 pandemic prevented in-person meetings. The research questions guided the development of an interview guide with themes and questions to frame the conversations, which is presented in Appendix 2. To ensure the effectiveness of the interview guide, a pilot interview was conducted with a participant who shared similarities with the target population. The purpose of the pilot interview was to assess the appropriateness of the questions and to ensure they were open-ended. The guide was slightly updated based on the feedback received, a question related to vessel operations and minor changes in formulations was added. I focused on keeping the dialogue dynamic and unstructured so that the participants were able to freely talk about their experiences (Kvale & Brinkmann, 2015).

The interviews lasted 30–90 minutes and were tape-recorded after I had received written consent from the participants. Follow-up questions and summaries of the participants' statements were used as validating strategies to reassure the participants that I understood their

statements. The interviews were both conducted and transcribed in Norwegian, as the interviewees were native Norwegian speakers. The transcriptions were kept in separate documents, and the software NVivo was used to aid with data analysis (Corbin & Strauss, 2015).

4.4.3 Data analysis

The data were analysed according to the three phases of CCA. The main categories were developed in the "open coding" phase, the sub-categories within the "axial coding" phase, and the core categories within the "selective coding" phase (Postholm, 2019). The process was iterative, and the phases were repeated as needed. The coding phases were also conducted in different orders, which is not uncommon as this analysis method is not seen as a strictly chronological process (Creswell & Poth, 2018).

The concept of theoretical saturation refers to the point at which no new information or themes contribute to the description of deck officers' cyber risk perceptions (Corbin & Strauss, 2015). To achieve this, each interview was analysed and compared to identify common themes and patterns, and after conducting nine interviews, saturation was reached. Achieving saturation is a complex process that involves exploring each category or theme in depth, identifying its various properties and dimensions. While researchers could continue to collect data indefinitely, at some point, they must determine that their research has been sufficiently well-developed for their purposes (Corbin & Strauss, 2015, p. 140). During the final interview, it became apparent that the data was no longer providing new insights, particularly with respect to recurring data on topics such as the experiences of distance to cyber risks, descriptions of the OT systems, and trust in others for cyber defence. This recognition of saturation was confirmed through a detailed review of the interview transcripts.

The transcriptions were coded in NVivo by analysing each sentence and labelling them for further development within the categories (Charmaz, 2006). The coding process was conducted in Norwegian and given a suitable English translation when the categories were finalised. The translation process was undertaken rigorously to ensure the integrity of the participants' responses. A "bottom-up" approach was initiated in the analysis process, with careful consideration given to the participants' meaning in their utterances and how to frame the quotes (Kara, 2015; Kvale & Brinkmann, 2015).

Four main categories emerged from the analysis of the data:

- Distance to cyber risks.
- The reliable cyber-physical systems.
- Internet of Ships: More restricted flexibility.
- Trust in others for cyber defence.

These categories formed the basis of the contextual model highlighting the factors influencing cyber risk perception, which subsequently informed the design of the quantitative phase and its hypotheses.

4.4.4 Ethical considerations

Researchers have ethical responsibilities when planning and executing research projects, and scholars emphasise the importance of abiding by the pillars of research ethics (Charmaz, 2006; Corbin & Strauss, 2015; Kvale & Brinkmann, 2015). Ethical guides, theories, and committees have been important in creating an ethical framework for all phases of this qualitative study. The first step was to report to and gain approval from the Norwegian Centre for Research Data. The approval letter is presented in Appendix 3. In this process, an information sheet and consent form for potential participants were drafted. This form was originally written in Norwegian, and a translated version is attached in Appendix 4.

Prior to collecting written consent from the participants, I informed them of the general purpose of the study and how confidentiality would be maintained and made sure they were comfortable with the interview situation. Participants were also informed of the option to withdraw at any time without consequences. When analysing the data, I removed potential identifying details of the participants and used composite stories when writing the results (Creswell & Poth, 2018).

Being ethical in qualitative research involves being aware of the responsibilities to provide rigour, transparency, methodological compliance, mutual trust, and understanding throughout the process. Ensuring the ethical integrity of this study has been important, and to the best of my knowledge, this research has been conducted taking into consideration both procedural and practical dimensions of ethical challenges.

4.4.5 Validity and methodological considerations

Creswell and Poth (2018, p. 255) define validity in qualitative research as a process for assessing the accuracy of findings as best described by the researchers and participants, which involves a combination of qualitative strategies. Validity is a frequently debated term in qualitative studies. Corbin and Strauss (2015) argue for instead using the terms "credibility" and "trustworthiness" and suggest "believable" as a preferred term to "validity". They emphasise that findings should reflect participants', researchers', and readers' experiences with phenomena while acknowledging that the findings provided are only one of many plausible interpretations of the data (Corbin & Strauss, 2015, p. 346).

Guided by these perspectives, validation strategies, such as the researcher's lens and the participant's lens, were conducted (Creswell & Poth, 2018). This included seeking participant feedback, generating thick descriptions, clarifying my own biases, and engaging in reflection. Furthermore, the quality criteria provided by Corbin and Strauss (2015) were used as guidance and a tool for reflection in all phases of this study. The criteria provide checkpoints to evaluate methodological consistency, quality, and applicability of studies using a constant comparative approach (Corbin & Strauss, 2015, pp. 350-352).

Conducting qualitative research is also accompanied by methodological considerations that influence the research process. As a primary instrument for data collection and analysis, the researcher's subjectivity influences both the interview setting and the interpretation of data. Researchers build their worldview, biases, and assumptions into the methodology, which affects the research problems they engage in and research questions they choose. I remained aware of this subjectivity, particularly throughout the analysis process. Strategies such as methodological compliance, making comparisons, and enhancing sensitivity were used to control the intrusion of biases and assumptions (Corbin & Strauss, 2015, p. 47).

4.5 Quantitative study with questionnaire

The contextual model from the qualitative study described the dimensions of deck officers' cyber risk perception. This third study sought to further explore parts of the qualitative findings through a quantitative approach. A cross-sectional survey design was chosen to provide a snapshot of the current state of cyber risk perceptions among deck officers working offshore. The aim was to generalise the initial insights to the broader population of officers by measuring

cyber risk perceptions and developing statistical models for prediction. Specific focus was given to examining how risk perception varied in relation to vessel IT and OT systems and the influencing role of various independent predictors across these system categories. Founded in previous research and the qualitative phase, a self-administrative questionnaire was developed. The Wilcoxon signed-rank test and hierarchical regression analyses were performed to test significance and correlations.

4.5.1 Participants and sampling

The online survey received a total of 303 submissions, with answers from 293 deck officers working offshore in Norwegian-based shipping companies. A control question was asked at the beginning of the questionnaire. If participants answered "No" to the question "Are you currently working as a deck officer on a vessel in the offshore industry?", they were rerouted to a page indicating that they were not part of the target group. Of the 303 respondents, 10 were not deck officers on offshore vessels, resulting in 293 qualifying participants.

The participants offered the perspectives of on-board decision-makers and spanned various experience levels and ranks. Clustering sampling within shipping companies was used to gain access to potential participants within the population. Eleven of the largest offshore shipping companies with main offices in Norway were recruited for this study, and the survey was provided to them to distribute among their deck officers. The choice of these large companies ensured comprehensive coverage of deck officers working in diverse conditions within offshore operations. This sampling method allowed for an efficient data collection process as working with sizeable shipping companies enabled distribution to the target population and ensured a broad sample representation (Ringdal, 2018).

4.5.2 Instrumentation

The instrument utilised for this quantitative study was a structured self-administered questionnaire, designed to measure levels of perceived cyber risk towards vessel IT and OT systems, together with measures of perceived system benefit, experience with cyber-attacks, amount of cybersecurity training, and trust in different stakeholders. The goal was to create an instrument that was both comprehensive in covering the chosen indexes and concise enough to ensure active participation. The questions were framed based on previous research on maritime

cybersecurity and cyber risk perception (Larsen et al., 2022). Summative indexes were created to represent the measured constructs. A detailed description of the survey design and the questions measuring each index are provided in the methods section of Paper Three, and Appendix 5 displays how the online questionnaire was presented to the participants.

A panel of academic experts and former deck officers was involved in the review process of the questionnaire. They provided feedback on questionnaire wording and comprehensiveness and specified the importance of defining terms like cyber risk and trust when presenting the questions to respondents. A pilot test was conducted with seven participants similar to the target population to ensure clarity and identify potential difficulties. This phase resulted in a few adjustments to the questionnaire wording, such as adding abbreviations after the systems focused on in the questionnaire.

4.5.3 Data collection and analyses

The survey was administered online using a secure platform called Nettskjema to ensure participants' anonymity and data protection (Gulbrandsen, 2017; University of Oslo [UiO], 2018). The participants could answer the survey in either Norwegian or English, making it available for non-Norwegian speaking deck officers. Participants were provided with information at the beginning of the questionnaire that detailed the study's purpose, its expected duration, and their rights as participants (Appendix 5). A reminder email was sent to the shipping companies after two weeks, asking them to resend the survey to encourage participation. The survey was available to potential participants between 19 October and 31 December 2022, providing a designated timeframe for response submission.

When the data collection phase was completed, the dataset and codebook were downloaded from Nettskjema and imported to SPSS. Since the electronic survey required answers to all questions, there were no missing values in the dataset. The option "Don't know/Don't use this" was given a value of 0 in the dataset. A few participants responded that their rank was second or third mate, so they were clustered with first mate and labelled second mate to avoid confusion with the term chief mate. Outlier detection was assessed using histograms and boxplots. Based on the outliers limited impact on the overall dataset, no data were removed.

Descriptive statistics was obtained to understand the dataset. Percentages, means, standard deviations, and frequencies were computed to give an overview of the general trends within

the dataset. Then, the non-parametric Wilcoxon signed-rank test was utilised to test for significant discrepancies between the participants' cyber risk perceptions of vessel IT and OT systems. This test was used because it is not restricted by the assumption of normal distribution and because the two conditions (level of cyber risk perception in relation to IT and OT) came from the same participants (Field, 2018). Further, two hierarchical regression analyses were performed to test the causal relationship between the independent variables (perceived benefit, trust, cybersecurity training, experience with cyber-attacks) and the dependent variables (cyber risk perception of IT and OT).

4.5.4 Validity and reliability

Validity refers to the extent to which an instrument accurately measures what it is intended to measure. Considering construct validity, the questionnaire items were developed based on previous studies of risk perception, perceived benefit, and trust (De Smidt & Botzen, 2018; Larsen et al., 2022; Siegrist, 2000; Siegrist et al., 2000; Van Kleef et al., 2010). Furthermore, the use of feedback from academic experts and deck officers in the development of the questionnaire enhanced face and content validity. Since the sample contained deck officers from eleven major offshore shipping companies in Norway, the findings' applicability to other groups or contexts might be limited. However, given the number of respondents and stature of the selected companies in the maritime domain, there is an expectation that the results can inform broader discussions in the industry, especially regarding the distinct differences in cyber risk perceptions towards IT versus OT. Offshore vessels operated from Norway are often technically advanced (Karan, 2019), but most of the IT and OT systems listed in the questionnaire are standard system categories for merchant vessels (Akpan et al., 2022). Even so, the external validity or generalisability of the findings to other shipping companies, other regions, or other maritime professionals remains an area for further exploration.

Reliability, in turn, concerns the consistency of the measurements. Cronbach's alpha coefficient was used to assess the reliability of the applicable variables, and the four reflective variables were all above the acceptable limit of 0.7 (Field, 2018). Due to the cross-sectional nature of the study, test–retest reliability was not assessed. However, this would be a valuable consideration for a future longitudinal study to ascertain the consistency of responses over time.

4.5.5 Ethical considerations

Ethical considerations are important in all research, and it is essential to be aware of the ethical obligations we have towards participants in quantitative and qualitative studies. Informed consent was used to assure that participation was voluntary, and no personal information was collected to maintain anonymity and confidentiality. Individual responses could not be traced back to participants as the online tool did not collect IP addresses, usernames, email addresses, or other identifiable information. To ensure transparency, the shipping companies and participants were informed that they would have access to the final research publications.

4.5.6 Limitations

Acknowledging limitations provides a comprehensive perspective of the study's findings and offers directions for future research. While the sampling methodology allowed for effective data collection, it may have introduced biases. Specifically, the perceptions of the deck officers from the selected shipping companies may not fully represent smaller entities or those outside of Norway. This could potentially limit the generalisability of the findings to the broader population of deck officers within the maritime industry. Furthermore, the reliance on self-reported data brings potential challenges of social desirability bias which may impact the degree of truthfulness in the participants' answers (Creswell & Creswell, 2023). Because of privacy concerns, it is also not possible to verify that only deck officers participated in the survey.

The study's cross-sectional design might also introduce temporal limitations as the data offer a snapshot of the participants' perception at a singular moment. Given the maritime domain's evolving nature, perceptions could shift as technologies advance and new cyber threats emerge, making the findings time sensitive. Moreover, the study's scope is concentrated on particular constructs, chosen based on the initial qualitative findings and previous research. Consequently, there might be other impactful factors influencing cyber risk perceptions that this study did not explore. In translating qualitative insights into quantifiable survey scales, there is an inherent risk of potentially oversimplifying certain aspects or missing nuanced perspectives (Creswell, 2022).

4.6 Considerations and challenges of mixed methods and sequential research design

Mixed methods research has gained attention for its ability to combine the depth of qualitative research with the breadth of quantitative studies. At its core, mixed-methods designs aspire to provide a comprehensive understanding of research phenomena by utilising the strengths of both qualitative and quantitative data (Creswell, 2022). This synergistic approach, however, brings with it the complexities and challenges of designing and executing research that must satisfy the rigour and requirements of both paradigms.

The decision to use an exploratory sequential design within mixed methods approaches for this thesis was guided by the main objective of exploring deck officers' cyber risk perceptions in offshore operations. By leveraging the strengths of both qualitative depth and quantitative breadth, this research provides rich and multidimensional findings. The sequential approach ensured a structured progression, in which each phase built on the last, while the exploratory nature preserved the flexibility to adapt and focus on the emergent themes.

Nevertheless, utilising mixed methods and the sequential design was not without challenges, and the use of both qualitative and quantitative methods was time-consuming. The timeframe for research projects with multiple phases can be longer than with single-phase designs, and the mixed-methods approach requires in-depth knowledge about both research categories. Quantitative research was especially demanding for me as I only had experience with qualitative research. Furthermore, keeping a consistent focus was a challenge, and the temporal gaps felt extensive because of the sudden explosion of digitalisation in the maritime domain during the COVID-19 pandemic. It was crucial to ensure that the quantitative phase aligned with the initial objectives identified during the qualitative phase, making it necessary to constantly revisit and re-evaluate the research questions and the data collection tools. Interpreting and presenting both qualitative and quantitative data in a way that captures their full depth and breadth without overwhelming the reader was challenging. However, in terms of gaining a holistic understanding of cyber risk perceptions, the potential benefits of conveying this magnitude outweigh the challenges.

5 Summary of Findings and Contributions

This section summarises the objectives, research questions, findings, and contributions of the three papers that form the backbone of this thesis. For a comprehensive overview, please refer to the papers in Part II of this thesis.

5.1 Paper 1

Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review

In this paper, the aim was to introduce an approach to investigating cyber risk perception and to provide an overview of current research within this field. A systematic literature review was chosen as the data collection method, and the focus was placed on key dimensions within the psychometric paradigm, heuristics, and cognitive biases, with a particular emphasis on investigating determinative factors.

The main research question in this paper aligns with RQ 1 from Section 1.1: What is state-of-the-art research within the field of cyber risk perception in general, and in the context of the maritime domain?

The following sub-questions were outlined to achieve this main goal:

1. What are the main dimensions within the psychometric paradigm and cognitive biases related to cyber risk perception?
2. What is the state-of-the-art research within the field of maritime cyber risk perception, and what recommendations can be given for future research within this field?

Using the systematic literature review guide by Okoli and Schabram (2010), 25 relevant articles describing 24 dimensions of cyber risk perception were identified. Interestingly, none of these articles or dimensions were specific to the maritime domain. The nine dimensions from the psychometric model, along with perceived benefit and the optimistic bias, were presented and discussed in a maritime context. Table 2 presents an overview of these dimensions.

Results from the review showed that the concept of cyber risk perception is complex, with intertwined determinative factors and cognitive processes that can vary between populations and professions. Consequently, the findings underscore the necessity of maritime-specific studies, and the paper posits that future investigations would benefit from descriptive and inductive research approaches. Contextual studies within maritime cyber risk perception are essential for the development of targeted cyber risk mitigation tools.

Table 2: *Dimensions related to cyber risk perception (Larsen & Lund, 2021; Larsen et al., 2022, p. 3)*

Voluntariness	The extent to which people perceive exposure to a cyber risk as voluntary affects how risky they perceive the related activity to be.
Immediacy of risk consequences	The greater the perceived immediacy of cyber risks is, the higher the perceived risk seems to be.
Knowledge to exposed party	When people have knowledge of, and are familiar with, the cyber risk in question, they perceive the risk as lower than if they have limited knowledge.
Knowledge to science/experts	People's level of perceived risk is affected by the extent to which they believe the cyber risks are known to experts or science.
Controllability	Risk perception levels can be reduced if people believe they can control the cyber risks and prevent them from happening.
Catastrophic potential	Cyber risks with a larger impact on a single occasion (catastrophic risk) are perceived as riskier than cyber risks with less impact (chronic risk).
Dread vs. common	Measures whether the cyber risk in question is something people have great dread of or have learned to live with.
Newness	New or novel risks tend to be perceived as riskier and less controllable than familiar risks.
Severity of consequences	When risks are perceived to have more severe consequences, they are perceived to be riskier.
Perceived benefit	If people perceive that technology has high benefits, they tend to perceive that the associated cyber risks are lower.
Optimistic bias	People tend to believe that others are more exposed to cyber risks than they are themselves, providing indications that people interpret uncertain situations in a self-serving direction.

The main contribution of this paper is the application of psychological models to investigate cyber risk perception. It also presents a compilation of relevant empirical studies, underscoring the critical need for research on cyber risk perception within the maritime context.

5.2 Paper 2

A Model of Factors Influencing Deck Officers' Cyber Risk Perception in Offshore Operations

This paper aimed to investigate factors influencing deck officers' cyber risk perception in offshore operations. Using in-depth interviews and CCA, the paper developed a contextual model with thick descriptions of the discovered dimensions that influence cyber risk perception. This paper was inspired by the results and empirical studies found in the first paper in this thesis, and the main research question aligns with RQ 2 from Section 1.1: What factors can influence deck officers' perceptions of cyber risks in offshore operations, and how can these factors be described?

The contextual model, detailed in Figure 2, revealed several influencing dimensions. Notably, deck officers' perceptions are shaped by a sense of distance from cyber risks, the impact of digitalisation on their working environment, their belief in the reliability of the on-board cyber-physical systems, and trust in their technology suppliers for cyber defence. The findings indicated several possible explanations and relations between the factors within the model, which aligns with the complex nature of people's perceptions of cyber risks as highlighted in the literature review.

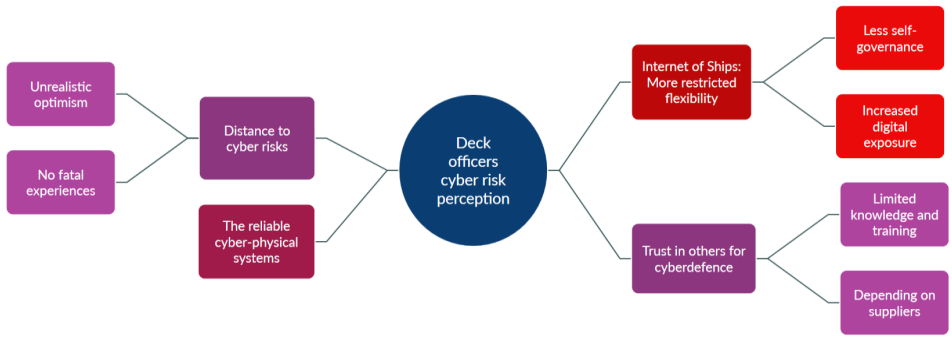


Figure 2: *Contextual model of factors influencing deck officers' cyber risk perception (Larsen et al., 2022, p. 5).*

Considering the insights from the model, this study recommended a multifaceted approach to developing targeted cyber risk mitigation measures on different levels in shipping companies. Table 3 renders the mitigation measures outlined in the paper, and proposed strategies included enhanced risk communication, operational training, awareness campaigns, vessel-specific

procedures, and cybersecurity policies. Furthermore, the research highlights the importance of transparent communication from management concerning the need for digitalisation.

Table 3: *Targeted cyber risk mitigation measures on different levels in shipping companies (Larsen et al., 2022)*

Implementation level	Cyber risk mitigation measures	Targeted categories in the contextual model
Individual (Deck officer)	Targeted risk communication with regards to personal/general cyber risk. Increase domain-specific knowledge about cybersecurity. More extensive cybersecurity course/training. Operational training in simulators.	Distance to cyber risks. The reliable cyber-physical systems. Trust in others for cyber-defence.
Vessel (Crew)	Operational training on cyber incidents with severe consequences. Onboard awareness campaigns with examples of cyber incidents. Vessel-specific policies and procedures for cyber security.	Trust in others for cyber-defence. The reliable cyber-physical systems.
Shipping company (Management)	Communication of need for digitalization and new IT-systems. Involvement of maritime crew in decision making on a higher level. Increase trust between vessel and shipping company. High-level company procedures for cybersecurity. Increase risk communication in all levels of the organization.	Internet of Ships: More restricted flexibility.

A salient contribution of this study lies in the exploration of a novel research field in the maritime context, providing in-depth insights into deck officers' perceptions of cyber risks. The contextual model serves as a foundation for further exploration, offering a starting point for future research aimed at uncovering additional nuances and factors that shape cyber risk perception in this operational domain.

5.3 Paper 3

Maritime Decision-Makers and Cybersecurity: Deck Officers' Perception of Cyber Risks Towards IT and OT Systems

In the third paper, the focus shifts to a quantitative investigation of deck officers' cyber risk perception of IT and OT systems on offshore vessels. The research question and hypotheses were informed by the main themes found in the contextual model from the second article, and the hypotheses align with RQ 3 from Section 1.1:

- H1: Deck officers perceive lower cyber risks towards OT systems than IT systems.
- H2: There is a difference in how the independent variables of perceived benefit, trust, cybersecurity training, and experience with cyber-attacks predict deck officers' cyber risk perception towards their vessels' IT and OT systems.

These hypotheses were tested using the Wilcoxon signed-rank test and hierarchical regression analyses with data from 293 deck officers. H1 was supported as the analysis revealed a significant disparity between the levels of cyber risk perception between IT and OT systems. H2 was partly supported, and the regression models unveiled interesting correlations. Figure 3 presents an overview of the hierarchal regression models with the independent variables and their corresponding significance level and beta values.

Multiple independent variables were considered in the regression models, comprising perceived benefit, cybersecurity training, previous experience with cyber-attacks, and trust in various stakeholders. A significant discovery was the role of perceived benefit, which was found to positively influence cyber risk perception across both IT and OT systems. Surprisingly, trust, which encompassed measures of social trust and confidence, did not emerge as a significant predictor. Furthermore, only OT system-related cyber risk perceptions were influenced by cybersecurity training and past experiences with cyber-attacks.

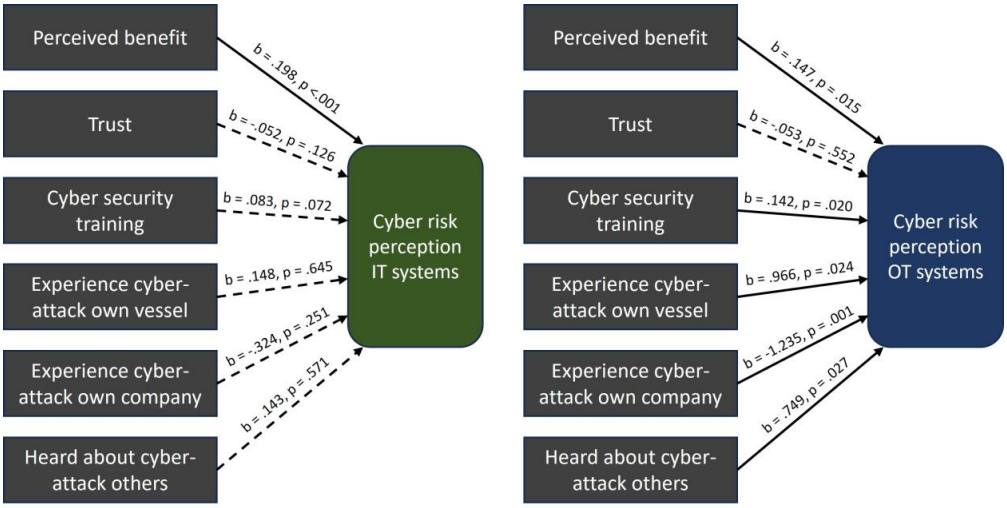


Figure 3: *Results of the second step of the hierarchical regression analyses. Dotted line indicates no significant relationship. Beta value and significance level are given for each independent variable.*

The findings in this study offer strategic recommendations to bridge the gap between theory and practice in maritime cybersecurity. Table 4 outline these recommendations, which include implications related to risk communication tools, training programmes focusing on OT, reporting mechanisms, and holistic cybersecurity policies tailored to the particularities within the maritime domain.

Table 4: *Practical recommendations (Haugli-Sandvik et al., in press)*

Acknowledge the difference between IT and OT systems.	The nature of information and operational technology is different, and this influence cyber risk perceptions. Acknowledgement of this difference can aid the process of implementing and revising cyber risk management strategies.
Increased collaboration between maritime stakeholders.	Increase stakeholders' communications related to cybersecurity decisions and actions. Emphasize the need for open dialogues, feedback sharing and joint efforts to address cyber risks within the maritime value chain.
Specific risk communication tools for IT and OT systems.	Develop specific risk communication tools for IT and OT systems with strategies that provide relevant and timely information about cyber incidents. Give transparent and contextually rich information about incidents involving vessels, shipping companies and other maritime companies. Focus on rewarding compliance and good security behaviour.
Tailored cybersecurity training programs with operational focus.	Revise current cybersecurity training programs to ensure a focus on operational training and OT systems. Consider the importance of continuous training and learning approaches to strengthen management strategies and cyber incident responses.
Cyber incident reporting system.	Work to establish structured incident reporting mechanisms to capture cyber incidents, impacts and lessons learned. More comprehensive data of industry-wide incident trends will support more efficient and accurate decision-support tools for cyber risk assessments.
Substantiated and holistic cybersecurity policies.	Create holistic policies to substantiate these cybersecurity recommendations. Highlight the importance of policymaking for enhanced decision making and cyber risk management.

This paper provides insights into the previously unexplored perspective of deck officers' perception of cyber risks in a highly operational working environment. It emphasises the crucial role of understanding human behaviour in maritime cybersecurity and offers evidence that human cognition differentiates between cyber risks across system categories within the same context.

6 Discussion

The overall objective of this thesis was to explore deck officers' cyber risk perception in offshore operations, particularly focusing on factors influencing the cognitive processes at play. The research unfolded through an exploratory sequential design, encompassing three interlinked studies. Initially, a systematic literature review was conducted to establish the theoretical foundation and identify research gaps. Subsequently, these insights informed the design of an interview study, which aimed at developing a contextual model of deck officers' cyber risk perception. The findings from this phase shaped the third phase, comprising a questionnaire study to measure levels of cyber risk perception and investigate causal relationships. This research design enabled a holistic understanding of cyber risk perception in offshore operations and set the stage for the discussion in this section. Within it, the findings from each study are compiled and examined to help achieve the main research objective.

The ensuing discussion complements the individual analyses presented in each paper in Part II. Rather than reiterating every aspect of the prior discussions, the focus will be on how findings from the subsequent phases can inform the preceding ones, coherently structured to reflect the progressive inquiry conducted (Creswell, 2022). Initially, the discussion will expand on the significance of the literature review, evaluating its role in delineating the theoretical landscape. Next, the findings and discussion of the in-depth interviews will be elucidated, considering the theoretical frameworks and the subsequent quantitative study. Finally, additional aspects of the questionnaire study will be elaborated on before a synthesis of the collective insights is drawn into a characteristics model of factors influencing deck officers' perceptions of cyber risks in offshore operations. The section concludes with an overview of the overall thesis's limitations and strengths.

6.1 Psychological frameworks

The systematic literature review of the first paper revealed theoretical frameworks for investigating cyber risk perception. Findings from the identified studies using the psychometric paradigm or investigating heuristics and biases provided a theoretical foundation for the thesis's subsequent research phases. The studies presented in the review made evident that theories within the psychological paradigm could be applied to investigate various cyber risks,

ranging from ICT risks faced by electric power supply companies to the online privacy risks of using social media platforms like Facebook (Garg & Camp, 2015; Skotnes, 2015).

The nine dimensions in the psychometric paradigm seemed to adequately explain what influenced different populations' perceptions of risks tied to various online activities. For example, by investigating perceived risks related to social media, sharing personal information online, financial activities, and other internet-related activities, various studies found that multiple factors within the psychometric paradigm were determinate for the participants' cyber risk perceptions (Gabriel & Nyshadham, 2008; Garg et al., 2014; LeBlanc & Biddle, 2012; Van Schaik et al., 2018). Furthermore, heuristics and tendencies of optimistic bias were investigated in relation to privacy risks and security management (Campbell et al., 2007; Rhee et al., 2012).

The frameworks and theories for studying risk perception within the psychological approach originate from research on physical risks related to nuclear power, health, and the environment (Spencer, 2016). These physical risks can be perceived as tangible because they are often immediate, familiar, or well-understood, and have observable or sensory consequences. Conversely, cyber risks may be intangible because of complex interactions and delayed consequences, presenting a challenge for individuals trying to fully grasp the risks' potential impact (Backman, 2023; Perrow, 1999). Furthermore, the lack of a sensory experiential element in cyber risks may influence the cognitive processing and assessment of such risks (Garg & Camp, 2012).

Consequently, the cognitive processes involved in understanding physical risks might differ from those involved in understanding cyber risks, as can be substantiated by the findings from the in-depth interviews and the questionnaire. The dimensions in the contextual model from the qualitative study demonstrate the complexity of how cyber risks are perceived. For instance, the interviewed deck officers described a low perception of cyber risks to their vessels and at the same time expressed insecurity about the consequences of connecting more systems online. Furthermore, the explanation percentage of the regression models in the third study was low at between 8.5 and 11.8 percent, leaving almost 90 percent of the variance unexplained. This indicates that other factors have more explanatory power than those tested in the questionnaire study.

While exploring other research fields beyond risk perception in the context of maritime cybersecurity and offshore operations falls outside the scope of this thesis, acknowledging potential interdisciplinary overlap is necessary. Disciplines such as cyberpsychology, human factors engineering, and security management may include theories or models that could enrich or extend the understanding acquired from the psychological paradigm. Insights from these fields, for instance, might offer broader understandings of human interaction with technological systems or organisational resilience, which could further explicate the complexities of cyber risk perception.

At the same time, findings from the literature review provided insights into how heuristics, biases, and the psychometric paradigm could serve as theoretical lenses to explore how individuals perceive cyber risks in various contexts. Furthermore, the study's discussion underscores the importance of considering the particularities within the maritime context and focusing on the human operator in a highly operational working environment. The conclusion, based on the study's discussion, recommended adopting a descriptive and inductive approach to explore deck officers' cyber risk perception in offshore operations. This recommendation was the steppingstone for the next phase as it became clear that using a qualitative approach with in-depth interviews in the second study would allow for an open approach to investigating the contextual nuances and descriptions of deck officers' cyber risk perception.

6.2 Context-specific factors influencing cyber risk perception

The qualitative phase allowed for an open exploration of cyber risk perception, grounded in the interviewed deck officers' firsthand experiences and the interpretations of the interviews. This approach provided rich, context-specific insights that were instrumental in identifying themes and patterns when developing the contextual model. The narratives encapsulated within the model provided a picture of deck officers who felt distanced from cyber risks, had no experience with fatal cyber incidents, and possessed limited cybersecurity knowledge and training; yet they were simultaneously experiencing a rapidly changing working environment due to technological developments, over which they seemingly have little control.

The interviewed deck officers perceived low cyber risks to their vessels. They had limited experience with cyber-attacks and believed that the on-board operational technology was secure. A statement from one of the interviewees illustrates this point: "The focus has been on

attacks against IT systems, and these systems are unbelievably more innocent than an operational system. If there is an attack on the IT system, it will not have any direct impact on the operation, other than that we have to handle the documentation in a slightly different way." This statement is substantiated by the results from the quantitative study, which showed that previous experience with cyber-attacks significantly influenced the perception of cyber risks to OT systems. Hence, if deck officers consider cyber risks towards IT less important than those towards OT because of their limited impact on operational security and safety, and they deem the OT systems secure and controllable, their overall perceptions of cyber risks might be influenced by familiarity and controllability, which are typical mechanisms in the availability heuristic and the optimistic bias (Montibeller & Von Winterfeldt, 2015; Weinstein, 1980). Consequently, if the risk communication and training that the officers receive focuses mainly on mitigating and managing cyber risks to IT systems, it would have a limited impact on their perception of cyber risks.

Another part of the contextual model outlined how increased use of IT systems for administrative work and the remote monitoring of OT systems resulted in less flexibility and self-governance at work. The interviewed deck officers described situations in which paperwork proved to be time-consuming and redundant and in which monitoring on-board machinery led to questions about fuel consumption and cost savings. These descriptions suggested that deck officers might have negative perceptions about the benefits of IT systems. However, results from the quantitative study showed that deck officers perceived both IT and OT systems as having high levels of benefit. Given these results, this part of the contextual model likely highlights the unwanted consequences of digitalisation more than the benefits of specific systems.

Accordingly, the consequences of digitalisation, such as the implementation of sensor technology and streaming of vessel performance data, may lead officers to feel monitored and controlled by shore management. One interviewee expressed these sentiments clearly: *"*I have a feeling that they really don't trust us, and that we somehow are deprived of decisions that we previously could just make on our own. Now there is this guardianship that is watching over us. However, in many situations, we need to think quickly and just get it done. So everyday work is now more and more computerised and monitored."

Such statements may indicate that deck officers perceive a loss of credibility or trust from their shipping company. Data from the questionnaire study also illustrated no significant correlation between trust in other stakeholders and cyber risk perception, suggesting that other types of trust are more influential, such as the level of confidence that deck officers have in the technological systems (Siegrist, 2021) or the importance of feeling trusted by their employer. It is essential to acknowledge these distinctions when implementing measures to foster enhanced trust between deck officers and onshore management and to further investigate the relationship between trust, perceived benefit, and cyber risk perception (Siegrist, 2000).

The absence of a significant correlation between trust and the dependent variables in the quantitative study might be a result of oversimplifying a complex relationship between the deck officers and other stakeholders. The officers' reliance on technological suppliers for OT cybersecurity may stem from factors other than mere trust or confidence (Bodó, 2021). Investigating how this relationship might be influenced by organisational structures, norms, and regulatory frameworks – known as institutional embeddedness – may provide deeper insights into the interactions between deck officers and OT suppliers. It is plausible that this embeddedness, along with other contextual properties such as the longevity of relationships or the reputation of the company, influences the officers' perception of the suppliers' trustworthy behaviour (Riegelsberger et al., 2005). Consider situations where deck officers must rely on technicians remotely connecting to their vessel's OT systems for critical updates or troubleshooting. The trust placed in the technician might not stem from direct social trust or confidence in that person's individual capabilities but could be influenced by the officers' trust in the broader organisational structures and reputation of the supplier company. Such trust, built upon the contextual properties of the supplier, might influence how deck officers perceive cyber risks associated with these remote interactions (Riegelsberger et al., 2005).

Rapid technological development, coupled with increased exposure to cyber risks, creates a complex working environment on board vessels (Kuhn et al., 2021; Schinas & Metzger, 2023). The interviewed deck officers highlighted that while new systems and solutions are continually implemented on board, the officers often do not receive corresponding training or education. Consequently, they find themselves increasingly dependent on external stakeholders, such as technology suppliers, to ensure and maintain system security. The results from the regression analyses demonstrated that cybersecurity training influences cyber risk perception of OT

systems, underscoring the importance of providing the officers with training and knowledge related to the operational systems.

Nevertheless, drawing from the qualitative insights, the second study greatly informed the construction of the hypotheses in the quantitative phase. In particular, the findings regarding trust in others for cyber defence and the distinct descriptions of OT versus IT influenced the focus of the questionnaire. Grounding the hypotheses in both lived experiences and previous research on cyber risk perception ensured the development of a relevant questionnaire.

6.3 Perception of cyber risks towards IT and OT systems

The quantitative phase aligned with the third study, which sought to extend the qualitative insights by gathering data from a larger sample of deck officers working offshore. This approach allowed for empirical testing of previously identified relationships and patterns, specifically concerning IT and OT. The analyses showed that deck officers perceive cyber risks to IT and OT systems differently. Furthermore, the varied influence of the independent variables of perceived benefit, trust, cybersecurity training, and experience with cyber-attacks provided insights into how cyber risk perception varies among different system categories within the same context.

As discussed in the previous sub-section, the questionnaire revealed that deck officers generally perceived both IT and OT as having significant benefits. Furthermore, the results indicated a positive correlation between perceived benefits and the deck officers' level of cyber risk perception. This finding, although surprising in regard to the positive correlation, aligns with existing research in the sense that individuals are more likely to accept associated risk when they perceive high benefits – especially when the adoption of technology or the engagement in related activities is seen as voluntary (Frewer et al., 1998; Van Schaik et al., 2020).

However, on offshore vessels, the integration of technological systems is considered a mandatory aspect of the working environment rather than a voluntary choice, which contrasts with the voluntary nature of technology adoption observed in other contexts (Garg et al., 2014; Sjöberg & Fromm, 2001). To support this argument, the qualitative study's contextual model illustrates how digitalisation and increased connectivity can reduce the working flexibility for deck officers. While the questionnaire study revealed a significant relationship between perceived benefits and cyber risk perception, it is essential to consider other dimensions, such

as voluntariness, which may also have a significant influence (Slovic, 1990). That said, the studies in this thesis are not specifically designed to investigate how deck officers perceive technology adoptions on their vessels. Therefore, it is important to further investigate the relationship between perceived benefit, voluntariness of technology adoption, and perception of cyber risks in this context.

When trying to understand the concerns of the interviewed deck officers, it became apparent that their primary apprehensions regarding digitalisation often revolved around its impact on their daily working routines rather than the increased exposure to cyber risks. For example, as mentioned above, one deck officer described how remote monitoring of the main engines led to questions from the shipping office regarding fuel consumption. However, there was no mention of the security levels of the installed sensors or the potential consequences of work disruptions due to a cyber incident. Many of the interviewed officers also pointed out that digitalisation resulted in increased reporting demands. Rather than replacing old systems, new ones often added another layer, compounding the officers' reporting tasks. Furthermore, the interviews were characterised by an absence of reflections on the potential cyber vulnerabilities, data breaches, or operational interruptions that these digital systems might introduce. This illustrates how the officers' immediate operational concerns may overshadow broader concerns about cybersecurity.

This distinction in assessing the potential consequences of digitalisation and connectivity touches upon a crucial aspect of how individuals assess technological risks. That the deck officers' primary concerns diverge from cyber risks has several implications. First, it suggests that the deck officers participating in the questionnaire might have formed their opinions while answering the questions and not based on their actual beliefs or behaviours. This would decrease the credibility of the questionnaire's results since ad-hoc generated opinions do not necessarily reflect reality (Sjöberg et al., 2004).

Second, since, at the moment, there have been few cyber-attacks on vessels with severe consequences, the officers' lack of concern about the potential consequences of cyber risks could result from relying on the availability heuristic or displaying optimistic bias (Haltinner et al., 2015; Tversky & Kahneman, 1974). Furthermore, if the deck officers do not engage in cybersecurity concerns for their on-board systems, they might perceive cyber risks as less

significant. Such reasoning may explain the lack of significant influence of trust on the deck officers' cyber risk perception (Earle et al., 2012).

Furthermore, the deck officers' apparent lack of cybersecurity concerns might create an environment for potential errors and violations, aligning with James Reason's (1990) insights into causes of accidents in complex systems. If cyber risks are not perceived as significant or integral to their daily routines, security measures in place might be more likely to be ignored or violated. This could manifest in various ways, such as delaying critical system updates due to operational considerations or disregarding cybersecurity protocols when charging personal devices in OT systems on the bridge.

Lastly, the way deck officers assess the potential consequences of cyber risks affects how knowledge building and information sharing should be conducted by management. If the officers are preoccupied with how digitalisation affects their daily routines, they may be less likely to engage with, or prioritise, other aspects of the technology, such as associated cyber risks (Tsohou et al., 2015). If this is the case, it becomes essential for management not only to provide cybersecurity training but also to understand and address deck officers' actual concerns. Overlooking these concerns could be considered latent failures (Galieriková, 2019), diminishing the effectiveness of training programmes and hindering participation in knowledge-building initiatives. It is important to recognise how latent failures can contribute to active failures such as errors or violations, since it can lead to system disasters (Reason, 1990). For instance, the intentional delay of a system update might introduce vulnerabilities a cyber threat can exploit, leading to a successful cyber-attack on the vessel's systems.

The findings of this thesis do not conclusively determine how perceptions of consequences related to technological systems influence the perception of cyber risks. However, it can be reasonably hypothesised that cyber risks may be perceived as intangible with uncertain consequences and a low likelihood of occurrence, especially if they are associated with an OT system. Given such perceptions, deck officers might naturally prioritise more tangible risks associated with on-board technology. Consider these examples of tangible risks: The risk of a fire on a vessel due to the deep fryer is immediately understood due to its visible and well-understood nature, prompting on-board crew to recognise and respect the mitigation measures in place. Similarly, the risk of a vessel collision or grounding due to unsafe navigation are well understood, which is why "Rules of the Road at Sea" exist and passage planning is universally

conducted. In contrast, the cyber risk of a vessel collision due to malware in the navigational system may seem less tangible due to more complex interactions and may not evoke the same intuitive understanding of the possible consequences (Fan & Yang, 2023; Perrow, 1999). Furthermore, cyber risk mitigation measures in place are not yet universal like those mitigating fire and vessel collisions (Chubb et al., 2022).

While there are indications that cyber risks may not be at the forefront of deck officers' concerns due to their intangible or less immediate nature, recent maritime industry studies and reports provide a silver lining. There is evidence of growing awareness about cybersecurity issues across both management and crew within shipping companies (Chubb et al., 2022; DNV, 2023; Knight & Sadok, 2021; Pavlinović et al., 2022). This is undoubtedly a positive development. However, mere awareness is just the beginning; the true challenge lies in understanding the potential risks and having actionable means to address them efficiently. Without accessible and comprehensible tools for cyber risk mitigation, this awareness will remain somewhat stagnant.

6.4 A characteristics model of factors influencing cyber risk perception

To enhance cybersecurity in offshore operations, it is essential to recognise that mitigation strategies extend beyond technical measures and security protocols and should include an understanding of how individuals perceive and evaluate cyber risks (Bada & Nurse, 2020). The aim of this section is to synthesise the findings in this thesis to provide an overview of characteristics influencing deck officers cyber risk perception in offshore operations.

This thesis has investigated perceptions of cyber risks, utilising risk perception theories from the psychology approach. The research has provided insights into how the operational and fast-changing working environment, the intangible nature of cyber risks, and the distinct differences between the technological systems influence these perceptions. Additionally, statistical models evince the distinct differences between cyber risk perceptions of IT and OT systems and how perceived benefits, cybersecurity training, and previous experience shape individual perceptions.

The collective insights be synthesised into a characteristics model, offering a road map for understanding cyber risk perceptions. This model, as depicted in Figure 4, aims to extricate the intertwined factors influencing perceptions of cyber risks. These factors can be divided into

characteristics of the context (offshore vessel working environment), the risk perceiver (deck officers), the risk (cyber risks), and the technological systems (IT/OT). These four high-level characteristics areas can be used to understand the particularities of deck officers' cyber risk perceptions in offshore operations.

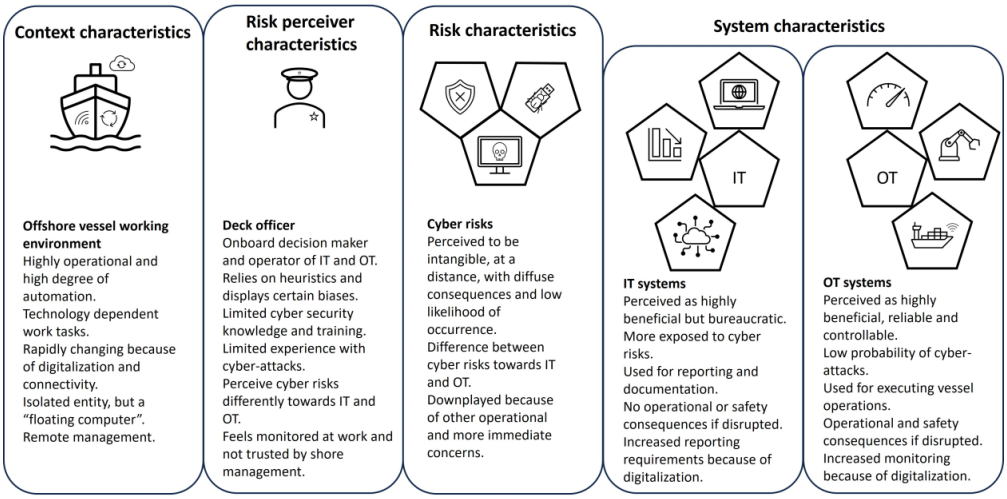


Figure 4: *Characteristics model of factors influencing cyber risk perception*

The context show that offshore vessels constitute distinctive working environments. Unlike conventional onshore workplaces and offices, vessels are highly operational, with advanced degrees of automation and are situated in remote locations away from on-shore management. The deck officers mainly have technology dependent work tasks and relies on the performance of the vessels' technological systems for safety and security.

The deck officers, who are the risk perceivers and operational decision-makers in this context, possess characteristics that influence cyber risk perception. Their reliance on heuristics, potential displays of biases, and often limited cybersecurity training and experience with cyber-attacks shape how they perceive and respond to cyber risks. Increased digitalisation and connectivity on-board vessels have led the officers to feel monitored at work and less trusted by their employers.

The characteristics of cyber risks affects how they are perceived, such as the notion of being intangible, having complex interactions, and perceived low likelihood of occurrence. The deck officers perceive cyber risks differently towards the on-board systems, and the importance of

considering these risks might be downplayed because of more immediate or operational concerns.

IT and OT systems have characteristics that cause deck officers to perceive cyber risks differently towards these system categories. Both categories of systems are perceived as beneficial, where IT is used for reporting and non-safety critical tasks and OT is used for operational purposes and are safety critical for the crew and its surroundings. Even so, digitalisation makes the officers' work tasks related to IT more bureaucratic and OT more monitored.

While each aspect of the characteristics model is important on its own, a holistic understanding of the combined interactions provides the foundation for cyber risk mitigation strategies. It is not enough to only gain insights into one of the four areas of the model. For example, it is crucial to understand the difference between using access control on a vessel and implementing this measure in an office landscape. Among other reasons, this difference arises because of the unique operational context and system characteristics on board vessels. Similarly, the development of cybersecurity training should be tailored to target the deck officers' perceptions and consider the particularities of the operational technology. Consequently, the characteristics in the model can be used to strategically draft cyber risk communication, cybersecurity training, policies, and vessel-specific procedures.

It is important to note that the descriptions in the model are tailored to the findings of this thesis. However, the overarching characteristics – the context, the risk perceiver, the risk, and IT/OT systems – are likely to be applicable beyond the context of offshore operations. The model is designed to be adaptable and evolve alongside changes in individuals' cyber risk perceptions. It allows for integration of new data specific to the applied context, and the high-level characteristics can be explored across vessel types, crew demographics, and technological systems.

The characteristics model serves as a roadmap for obtaining contextual knowledge that is essential for developing targeted cyber risk management strategies. The complexity of the influential factors on cyber risk perceptions suggests that a one-size-fits-all approach to maritime cybersecurity would be inadequate. Therefore, shipping companies should acquire this knowledge for their specific vessels and crew. By adopting cyber risk management

strategies based on insights from this model, companies can ensure that the mitigation measures are not only technically sound but also tailored to the individuals at the forefront of handling cyber risks at sea.

6.5 Limitations and strengths

As with any comprehensive research, this thesis possesses strengths that underpin the contributions as well as limitations that should be acknowledged. While several limitations have been previously addressed in Section Four and in the papers in Part II, there are some overarching points to consider for the entire research project.

First, the insights drawn from this thesis rely on the experiences and views of a specific number of deck officers from Norwegian shipping companies. While these participants provided invaluable insights, a broader and more diverse sample might offer a richer set of perspectives, especially as risk perceptions can differ across populations and work evironments (Campbell et al., 2007). Furthermore, the officers' understanding of cyber risks may differ from theoretical definitions, be context-dependent, or evolve over time. Consequently, the generalisability of the findings might be influenced by both the sampling nature and the participants' interpretations of cyber risks.

Second, this research captures deck officers' perceptions at a particular moment in time, and there are temporal gaps between the qualitative and quantitative studies. Given the constant evolution of the maritime industry and cyber risks, individual perceptions might also transform over time. The period between the second and third phases of this project might have resulted in perceptions shifts from the time when the interviews were conducted to when the questionnaire was disseminated. This underscores the importance of continuous research to capture this evolving field.

Lastly, the selection of theoretical frameworks and the focus of each research phase have undeniably shaped the outcomes of this thesis. As with any study, the chosen lens influences the view, potentially highlighting certain aspects while overshadowing others. The interpretations and findings are inherently influenced by the chosen theoretical perspectives on risk perception, as well as the thematic emphases on maritime cybersecurity and the experiences of deck officers working in offshore operations.

One of the primary strengths of this research is its novelty and detailed exploration of a specific demographic. Investigating deck officers' perceptions of cyber risks in offshore operations addresses and contributes to a domain that has, until now, remained relatively uncharted. By concentrating on deck officers from Norwegian shipping companies, the study was able to gather findings and achieve understandings that might not be captured in a broader, more generalised study.

Another strength is the methodological soundness of employing an exploratory sequential design, which allows for depth and breadth. This sequential approach ensured that the research was both comprehensive and focused. Furthermore, while the chosen theoretical frameworks influenced the perspectives of this study, they also provided a structured, well-defined lens through which the research was conducted. Grounding research in established theories ensures theoretical rigour and consistency, which allows future studies to do meaningful comparisons, and lays the groundwork for subsequent research.

Collaboration between academia and industry is important, and this study stands strengthened by its active engagement with industry stakeholders. Collaboration with shipping companies and other industry representatives ensures that the research is rooted in the real-world challenges that the maritime industry faces. Such collaborations enhance not only this study's relevance but also its applicability and practical impact.

Finally, a defining feature of this research is its holistic understanding of deck officers' cyber risk perceptions. By grounding the overall finding of this thesis in the characteristics model, it portrays the complex interplay between the risk perceiver, the operational context, the nature of cyber risks, and the on-board systems. This highlights the importance of understanding individual cyber risk perceptions to develop targeted risk mitigation strategies.

7 Conclusions

The main objective of this thesis was to investigate deck officers' perceptions of cyber risks in offshore operations. Employing an exploratory sequential design grounded in risk perception theories with a psychological approach, the research was structured to ensure that each phase informed and enriched the subsequent one. This led to a comprehensive understanding of the underlying factors shaping the officers' perceptions. As outlined in Section One, this thesis aimed to address three research questions in the subsequent phases.

To answer RQ 1, a systematic literature review was conducted. The aim was to establish the current state of research in cyber risk perception and to present methods for investigating people's perceptions of cyber risks using psychological models. This review identified 24 key dimensions that influence cyber risk perception and demonstrated how certain dimensions are relevant in the maritime context. Furthermore, this study highlighted research gaps in the existing literature.

Guided by the findings of the initial review, RQ 2 was investigated using in-depth interviews, which identified dimensions influencing deck officers' perceptions of cyber risks in offshore operations. These dimensions described the officers' perceived distance to cyber risks, influenced by unrealistic optimism and the absence of fatal experiences; their inherent trust in reliable cyber-physical systems; the way digitalisation restricts working flexibility; and the officers' dependence on trusting other stakeholders for cyber defence. These insights underscored the need for multifaceted cyber risk mitigation measures tailored to different levels within shipping companies.

Informed by the qualitative study, RQ 3 was conducted with a quantitative approach through a questionnaire. This study investigated the determinant factors shaping deck officers' cyber risk perceptions of IT and OT systems. The variables of perceived benefit, trust, cybersecurity training, and previous experiences with cyber-attacks were evaluated for their influence on cyber risk perceptions related to the two system categories. The results revealed distinct differences between cyber risk perceptions of IT and OT, and the varying significance of the independent variables again highlighted the importance of tailoring cybersecurity training and risk communication to deck officers.

The synthesis of these phases, which represents this thesis and incorporates the exploratory sequential design, led to the development of the characteristics model that bridges the insights from the phases into a unified framework. This model delineates the characteristics influencing deck officers' cyber risk perceptions, emphasising the importance of accounting for the context, the risk perceiver, the risk itself, and the on-board systems. Notably, the model illustrates how the working environment on offshore vessels, combined with deck officers' personal experiences and biases, the intangible nature of cyber risks, and the on-board system categories, forms distinct perceptions of cyber risks. Understanding the four aspects in this model offers a roadmap for developing cyber risk mitigation strategies that address cyber risk perceptions in specific contexts. As the maritime industry becomes increasingly interconnected and reliant on digital systems, understanding how cyber risk perceptions are shaped among operational decision-makers is crucial. This research provides foundational insights that can guide future efforts to enhance maritime cybersecurity practices.

7.1 Implications for practice

Insights from this research can assist maritime stakeholders in formulating relevant cyber risk management strategies. Recognising that perceptions of cyber risk are shaped by a combination of environmental factors, personal experiences and biases, the nature of the risk itself, and the characteristics of on-board systems, stakeholders are best positioned to develop cybersecurity strategies that resonate with offshore employees. This understanding not only forms the basis for more effective cyber risk communication but also facilitates the development of operational training programmes and cybersecurity policies that align with the experiences of deck officers on offshore vessels.

7.2 Implications for research

This research fills a significant gap in the maritime cybersecurity literature, emphasising the importance of understanding human cognitive processes that drives decision-making to develop targeted cyber risk mitigation strategies. Utilising an exploratory sequential design, this thesis provides a holistic understanding of deck officers' cyber risk perceptions. The findings highlight the importance of multidisciplinary research, bridging risk perception theories and the context-specific environment of maritime cybersecurity in offshore operations. This research offers a comprehensive model detailing the characteristics that influence deck

officers' cyber risk perceptions, which future studies can validate and explore the applicability of across contexts and demographics.

7.3 Future work

Insights from this thesis offer a foundation for subsequent research endeavours. Future research should further investigate heuristics and biases related to cyber risks, such as by examining how these biases might shape decision-making processes during real-time cyber-attack scenarios. Moreover, as technology and cyber threats continue to evolve, ongoing research is invaluable for keeping pace with this fast-changing environment. Expanding the scope of this research to include other roles within maritime companies could also provide a broader picture of cyber risk perceptions throughout the industry. For instance, exploring how the crew perceive cyber risks or how team dynamics on vessels influence such perceptions.

A study of the extent to which deck officers voluntarily adopt technology on vessels can provide additional insights to understand their cyber risk perceptions. Additionally, exploring how digitalisation can lead to human error or violations in vessel operations can also contribute to this understanding. The concept of trust warrants further exploration; it may be worthwhile to investigate the importance of having confidence in on-board technological systems and being trusted to perform work duties effectively.

Given the intangible nature of cyber risks, these risks might not always elicit the same perceptual understanding as traditional maritime risks caused by violation of rules or physical conditions. There is an opportunity for future research to delve deeper into this contrast, exploring the potential in understanding this divergence. Such knowledge could also bridge more multidisciplinary research focusing on building theoretical paradigms specific to how individuals perceive cyber risks and investigate the efficiency of cybersecurity measures targeting these perceptions. Finally, further investigating the validity and generalisability of the characteristics model can provide grounds for connecting research fields and extending our understanding of what influences perceptions of cyber risks.

References

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, *42*(12), 40-46. https://doi.org/10.1145/322796.322806

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, *236*, 106493. https://doi.org/10.1016/j.ocecoaman.2023.106493

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network*, *2*(1), 123-138. https://doi.org/10.3390/network2010009

Algarni, M., Almesalm, S., & Syed, M. (2019). Towards enhanced comprehension of human errors in cybersecurity attacks. Advances in Human Error, Reliability, Resilience, and Performance: Proceedings of the AHFE 2018 International Conference on Human Error, Reliability, Resilience, and Performance, July 21-25, 2018, Loews Sapphire Falls Resort at Universal Studios, Orlando, Florida, USA 9, https://doi.org/10.1007/978-3-319-94391-6_16

Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). A survey on cyber security threats in iot-enabled maritime industry. *IEEE Transactions on Intelligent Transportation Systems*, *24*(2), 2677-2690. https://doi.org/10.1109/TITS.2022.3164678

Backman, S. (2023). Normal cyber accidents. *Journal of Cyber Policy*, *8*(1), 114-130. https://doi.org/10.1080/23738871.2023.2281675

Bada, M., & Nurse, J. R. (2020). The social and psychological impact of cyberattacks. In V. Benson & J. McAlaney (Eds.), *Emerging Cyber Threats and Cognitive Vulnerabilities* (pp. 73-92). Academic Press. https://doi.org/10.1016/B978-0-12-816203-3.00004-6

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). Cyber security in the maritime industry: a systematic survey of recent advances and future trends. *Information*, *13*(1), 22. https://doi.org/10.3390/info13010022

BIMCO, CLIA, ICS, Intercargo, Intertanko, & OCIMF. (2020). *Guidelines on cyber security onboard ships - Version 4*. https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

Bodó, B. (2021). Mediated trust: A theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society*, *23*(9), 2668-2690. https://doi.org/10.1177/1461444820939922

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*, *39*, 100571. https://doi.org/10.1016/j.ijcip.2022.100571

Bridger, R. (2021). A Guide to Human Factors in Accident Investigation. In S. O. Johnsen & T. Porathe (Eds.), *Sensemaking in Safety Critical and Complex Situations* (pp. 13-32). CRC Press.

Campbell, J., Greenauer, N., Macaluso, K., & End, C. (2007). Unrealistic optimism in internet events. *Computers in Human Behavior*, *23*(3), 1273-1284. https://doi.org/10.1016/j.chb.2004.12.005

Caprolu, M., Di Pietro, R., Raponi, S., Sciancalepore, S., & Tedeschi, P. (2020). Vessels cybersecurity: Issues, challenges, and the road ahead. *IEEE Communications Magazine*, *58*(6), 90-96. https://doi.org/10.1109/MCOM.001.1900632

Chan, J. P., Norman, R., Pazouki, K., & Golightly, D. (2022). Autonomous maritime operations and the influence of situational awareness within maritime navigation. *WMU Journal of Maritime Affairs*, *21*(2), 121-140. https://doi.org/10.1007/s13437-022-00264-4

Charmaz, K. (2006). *Constructing grounded theory: A practical guide through qualitative analysis*. Sage Publications.

Chauvin, C. (2011). Human factors and maritime safety. *The Journal of Navigation*, *64*(4), 625-632. https://doi.org/10.1017/S0373463311000142

Cho, H., Lee, J.-S., & Chung, S. (2010). Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience. *Computers in Human Behavior*, *26*(5), 987-995. https://doi.org/10.1016/j.chb.2010.02.012

Chryssochoidis, G., Strada, A., & Krystallis, A. (2009). Public trust in institutions and information sources regarding risk management and communication: Towards integrating extant knowledge. *Journal of Risk Research*, *12*(2), 137-185. https://doi.org/10.1080/13669870802637000

Chubb, N., Finn, P., & Ng, D. (2022). *The Great Disconnect*. C. Thetius, HFV and HFV Consulting. https://safety4sea.com/wp-content/uploads/2022/03/Thetius-hfw-cyberowl-Great-disconnect-cyber-risk-management-2022_03.pdf

Corbin, J., & Strauss, A. (2015). *Basics of Qualitative Research - Techniques and Procedures for Developing Grounded Theory* (4 ed.). SAGE Publications, Inc.

Cordon, J. R., Mestre, J. M., & Walliser, J. (2017). Human factors in seafaring: The role of situation awareness. *Safety Science*, *93*, 256-265. https://doi.org/10.1016/j.ssci.2016.12.018

Creswell, J. W. (2022). *A concise introduction to mixed methods research* (2 ed.). SAGE Publishing.

Creswell, J. W., & Creswell, J. D. (2017). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage publications.

Creswell, J. W., & Creswell, J. D. (2023). *Research design: Qualitative, quantitative, and mixed methods approaches* (6 ed.). Sage Publications.

Creswell, J. W., & Poth, C. N. (2018). *Qualitative Inquiry and Research Design - Choosing Among Five Approaches* (4 ed.). SAGE Publications, Inc.

De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, *43*(2), 239-274. https://doi.org/10.1057/s41288-018-0082-7

DNV. (2023). *Maritime Cyber Priority 2023*. https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html

Drazovich, L., Brew, L., & Wetzel, S. (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), https://doi.org/10.1109/CSR51186.2021.9527922

Drottz-Sjoberg, B.-M., & Persson, L. (1993). Public reaction to radiation: fear, anxiety, or phobia? *Health Physics*, *64*(3), 223-231.

Earle, T. C. (2010). Trust in risk management: A model-based review of empirical research. *Risk Analysis: An International Journal*, *30*(4), 541-574. https://doi.org/10.1111/j.1539-6924.2010.01398.x

Earle, T. C., & Siegrist, M. (2008). On the relation between trust and fairness in environmental risk management. *Risk Analysis: An International Journal*, *28*(5), 1395-1414. https://doi.org/10.1111/j.1539-6924.2008.01091.x

Earle, T. C., Siegrist, M., & Gutscher, H. (2012). Trust, Risk Perception and the TCC Model of Cooperation 1. In *Trust in cooperative risk management* (pp. 1-50). Routledge.
Eie, K. M. (2020). Trusler og etterretning (Threats and cyber intelligence). In L. Øverlier (Ed.), *Digital sikkerhet - En innføring* (2 ed.). Universitetsforlaget.
Endsley, M. R. (1988). Situation awareness global assessment technique (SAGAT). Proceedings of the IEEE 1988 national aerospace and electronics conference, https://doi.org/10.1109/NAECON.1988.195097
ENISA. (2023). *European Union Agency for Cybersecurity - Glossary*. Retrieved 21.10.2023 from https://www.enisa.europa.eu/topics/risk-management/current-risk/risk-management-inventory/glossary?v2=1&tab=details
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., Lund, M. S., & Ostnes, R. (2022). Navigating through cyber threats, a maritime navigator's experience. *Applied Human Factors and Ergonomics International (AHFE International)*, *53*, 84-91. https://doi.org/10.54941/ahfe1002205
Fan, S., Blanco-Davis, E., Fairclough, S., Zhang, J., Yan, X., Wang, J., & Yang, Z. (2023). Incorporation of seafarer psychological factors into maritime safety assessment. *Ocean & Coastal Management*, *237*, 106515. https://doi.org/10.1016/j.ocecoaman.2023.106515
Fan, S., & Yang, Z. (2023). Systematic analysis of human factors in maritime transportation. 2023 7th International Conference on Transportation Information and Safety (ICTIS), https://doi.org/10.1109/ICTIS60134.2023.10243889
Farahmand, F., Dark, M., Liles, S., & Sorge, B. (2009). Risk perceptions of information security: A measurement study. 2009 International Conference on Computational Science and Engineering, https://doi.org/10.1109/CSE.2009.449
Farahmand, F., & Spafford, E. H. (2013). Understanding insiders: An analysis of risk-taking behavior. *Information systems frontiers*, *15*(1), 5-15. https://doi.org/10.1007/s10796-010-9265-x
Field, A. (2018). *Discovering statistics using IBM SPSS statistics* (5 ed.). Sage Publications Ltd.
Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., & Combs, B. (1978). How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. *Policy sciences*, *9*(2), 127-152. https://doi.org/10.1007/BF00143739
Freudenburg, W. R. (1993). Risk and recreancy: Weber, the division of labor, and the rationality of risk perceptions. *Social forces*, *71*(4), 909-932. https://doi.org/10.1093/sf/71.4.909
Frewer, L. J., Howard, C., & Shepherd, R. (1998). Understanding public attitudes to technology. *Journal of Risk Research*, *1*(3), 221-235. https://doi.org/10.1080/136698798377141
Gabriel, I. J., & Nyshadham, E. (2008). *A cognitive map of people's online risk perceptions and attitudes: An empirical study* Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa. https://doi.org/10.1109/HICSS.2008.6
Galieriková, A. (2019). The human factor and maritime safety. *Transportation Research Procedia*, *40*, 1319-1326. https://doi.org/10.1016/j.trpro.2019.07.183

Garg, V., Benton, K., & Camp, L. J. (2014). The privacy paradox: a Facebook case study. 2014 TPRC conference paper, https://doi.org/10.2139/ssrn.2411672
Garg, V., & Camp, J. (2012). *End user perception of online risk under uncertainty* 2012 45th Hawaii International Conference on System Sciences, Maui. https://doi.org/10.1109/HICSS.2012.245
Garg, V., & Camp, L. J. (2015). Cars, condoms, and facebook. In *Information security* (pp. 280-289). Springer. https://doi.org/10.1007/978-3-319-27659-5_20
Grech, M., Horberry, T., & Koester, T. (2008). *Human factors in the maritime domain*. CRC Press.
Gulbrandsen, A. (2017). *Informasjonssikkerhet og risikovurdering for Nettskjema*. University of Oslo. Retrieved 02.08.2023 from https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/
Haltinner, K., Sarathchandra, D., & Lichtenberg, N. (2015). Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. Cyber Security Symposium, Cham. https://doi.org/10.1007/978-3-319-28313-5_6
Haugli-Sandvik, M., Lund, M. S., & Bjørneseth, F. B. (in press). Maritime Decision-Makers and Cybersecurity: Deck Officers' Perception of Cyber Risks Towards IT and OT systems *International Journal of Information Security*.
Hetherington, C., Flin, R., & Mearns, K. (2006). Safety in shipping: The human element. *Journal of safety research*, *37*(4), 401-411. https://doi.org/10.1016/j.jsr.2006.04.007
Hopcraft, R. (2021). Developing maritime digital competencies. *IEEE Communications Standards Magazine*, *5*(3), 12-18. https://doi.org/10.1109/MCOMSTD.101.2000073
Hopcraft, R., & Martin, K. M. (2018). Effective maritime cybersecurity regulation–the case for a cyber code. *Journal of the Indian Ocean Region*, *14*(3), 354-366. https://doi.org/10.1080/19480881.2018.1519056
Huus, I. A. B., & Paulsen, R. K. (2022). *Securing Safety in the Norwegian Petroleum Industry with Digital Twins* Norwegian University of Science and Technology]. https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/3024592/no.ntnu%3Ainspera%3A107093487%3A30052606.pdf?sequence=1
Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *52*(2), 25-67. https://doi.org/10.1145/3462766.3462770
IMO. (2017). Guidelines on Maritime Cyber Risk Management. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf
IMO. (2019). *Maritime Security*. Retrieved 20.09.2023 from https://www.imo.org/en/OurWork/Security/Pages/Default.aspx
IMO. (2023). *International Convention for the Safety of Life at Sea (SOLAS), 1974*. Retrieved 10.09.2023 from https://www.imo.org/en/About/Conventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx
Jo, Y., Choi, O., You, J., Cha, Y., & Lee, D. H. (2022). Cyberattack models for ship equipment based on the MITRE ATT&CK framework. *Sensors*, *22*(5), 1860. https://doi.org/10.3390/s22051860
Kahneman, D. (2011). *Thinking, fast and slow*. Macmillan.

Kahneman, D., Slovic, S. P., Slovic, P., & Tversky, A. (1982). *Judgment under uncertainty: Heuristics and biases*. Cambridge university press.
Kanwal, K., Shi, W., Kontovas, C., Yang, Z., & Chang, C.-H. (2022). Maritime cybersecurity: are onboard systems ready? *Maritime Policy & Management*, 1-19. https://doi.org/10.1080/03088839.2022.2124464
Kara, H. (2015). *Creative research methods in the social sciences: A practical guide*. Policy Press.
Karan, C. (2019). *What are Offshore Vessels?* Marine Insight. Retrieved 07.08 from https://www.marineinsight.com/types-of-ships/what-are-offshore-vessels/
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/10.1016/j.ijcip.2022.100526
Kessler, G. C., & Shepard, S. D. (2022). *Maritime Cybersecurity - A Guide for Leaders and Managers* (Second Edition ed.). Amazon.
Kjerstad, N. (2017). *Fremføring av skip med navigasjonskontroll* (Vol. 4). Fagbokforlaget.
Knight, V., & Sadok, M. (2021). Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry. 7th International Workshop on Socio-Technical Perspective in IS Development, https://pure.port.ac.uk/ws/portalfiles/portal/49456351/paper19.pdf
Kuhn, K. (2022). *Enhancing Decision-Making about Cyber Risk: Perspectives from Maritime Security* Coventry University]. https://pure.coventry.ac.uk/ws/portalfiles/portal/57616704/CU_PhD_by_Pub_PostAward_Critical_Overview_Document_Kuhn.pdf
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. https://doi.org/10.1007/s13437-021-00235-1
Kvale, S., & Brinkmann, S. (2015). *Det kvalitative forskningsintervju* (3 ed.). Gyldendal Norske Forlag AS.
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/10.1016/j.martra.2022.100065
LeBlanc, D., & Biddle, R. (2012). Risk perception of internet-related activities. 2012 Tenth Annual International Conference on Privacy, Security and Trust, https://doi.org/10.1109/PST.2012.6297924
Lee, A. R., & Wogan, H. P. (2018). All at sea: The modern seascape of cybersecurity threats of the maritime industry. OCEANS 2018 MTS/IEEE Charleston, https://doi.org/10.1109/OCEANS.2018.8604554
Martínez, F., Sànchez, L. E., Santos-Olmo, A., Rosado, D. G., & Fernàndez-Medina, E. (2024). Maritime cybersecurity: protecting digital seas. *International Journal of Information Security*, 1-29. https://doi.org/10.1007/s10207-023-00800-0
Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. 519-530. https://doi.org/10.12716/1001.15.03.04

Meland, P. H., Nesheim, D. A., Bernsmed, K., & Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, *64*, 103050. https://doi.org/10.1016/j.jisa.2021.103050

Montibeller, G., & Von Winterfeldt, D. (2015). Cognitive and motivational biases in decision and risk analysis. *Risk analysis*, *35*(7), 1230-1251. https://doi.org/10.1111/risa.12360

Mraković, I., & Vojinović, R. (2019). Maritime Cyber Security Analysis–How to Reduce Threats? *Transactions on maritime science*, *8*(01), 132-139. https://doi.org/10.7225/toms.v08.n01.013

Möller, N. (2012). The concepts of risk and safety. In S. Roeser, R. Hillerbrand, P. Sandin, & M. Peterson (Eds.), *Handbook of risk theory: epistemology, decision theory, ethics, and social implications of risk* (Vol. 1, pp. 55-85).

NORMACyber. (2023). *NORMA Cyber Annual Threat Assessment 2023*. https://www.normacyber.no/news/48o1qpgi66klzqspdg7jg3kwta3172

Okoli, C., & Schabram, K. (2010). A guide to conducting a systematic literature review of information systems research. *Sprouts: Working Papers on Information Security*, *10*(26). https://d1wqtxts1xzle7.cloudfront.net/3250666/OkoliSchabram2010SproutsLitReviewGuide-libre.pdf?1390830932=&response-content-disposition=inline%3B+filename%3DA_Guide_to_Conducting_a_Systematic_Liter.pdf&Expires=1704803357&Signature=ag-OjytZHQxw1z-fyB8ZCFL5SH6vzF4-SRTxgVJMTZqkeVvsiKNnU98oy8JvL8o~5dsdLCb5MjsuSExemG4YkLbTdHIeO5dSSXHW7qxyBgeuAPeLqX09AdT2tXVytp0paR8TooYNhvRveubjNxxhwaPDFcTp1cXfAEmpGikNzG2sa-XJ7HIhiGw~iu9p8pSodVHHtRQuTfXzvqFA9IgDgLZzuqZPzTemVqWdToKLZttiwirKCAAttQ4DX9OXjvD3iqD70mPLWECVY~pBYrQ7rKZWCUCAjE67EyO6QUzABToHlgAwsuizNv~QWtsYQsLzXODHe-Ov7~GuQYIOhrXPnQ__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Oruc, A., Chowdhury, N., & Gkioulos, V. (2024). A modular cyber security training programme for the maritime domain. *International Journal of Information Security*, 1-36. https://doi.org/10.1007/s10207-023-00799-4

Pavlinović, M., Račić, M., & Karin, I. (2022). Cyber Risks in Maritime Industry–Case Study of Croatian Seafarers. Human Interaction, Emerging Technologies and Future Systems V: Proceedings of the 5th International Virtual Conference on Human Interaction and Emerging Technologies, IHIET 2021, August 27-29, 2021 and the 6th IHIET: Future Systems (IHIET-FS 2021), October 28-30, 2021, France, https://doi.org/10.1007/978-3-030-85540-6_14

Perrow, C. (1999). *Normal accidents: Living with high risk technologies*. Princeton university press.

Postholm, M. B. (2019). Analysing the Data Material Using the Constant Comparative Analysis Method and D-Analysis. In *Research and Development in School* (pp. 85-102). Brill. https://doi.org/10.1163/9789004410213_007

Potamos, G., Peratikou, A., & Stavrou, S. (2021). Towards a maritime cyber range training environment. 2021 IEEE International Conference on Cyber Security and Resilience (CSR), https://doi.org/10.1109/CSR51186.2021.9527904

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, https://doi.org/10.1007/978-981-19-6414-5_6
Progoulakis, I., Rohmeyer, P., & Nikitakos, N. (2021). Cyber physical systems security for maritime assets. *Journal of Marine Science and Engineering*, *9*(12), 1384. https://doi.org/10.3390/jmse9121384
Reason, J. (1990). *Human error*. Cambridge university press.
Refsdal, A., Solhaug, B., & Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management* (pp. 9-47). Springer. https://doi.org/10.1007/978-3-319-23570-7_5
Renn, O. (1992). Concepts of risk: a classification. In S. Krimsky & D. Golding (Eds.), *Social theories of risk* (pp. 53-79). CT: Praeger.
Renn, O. (2004). Perception of risks. *Toxicology letters*, *149*(1-3), 405-413. https://doi.org/10.1016/j.toxlet.2003.12.051
Rhee, H.-S., Ryu, Y. U., & Kim, C.-T. (2012). Unrealistic optimism on information security management. *computers & security*, *31*(2), 221-232. https://doi.org/10.1016/j.cose.2011.12.001
Riegelsberger, J., Sasse, M. A., & McCarthy, J. D. (2005). The mechanics of trust: A framework for research and design. *International journal of human-computer studies*, *62*(3), 381-422. https://doi.org/10.1016/j.ijhcs.2005.01.001
Ringdal, K. (2018). *Enhet og Mangfold* (4 ed.). Fagbokforlaget.
Roeser, S. (2012). *Handbook of risk theory: Epistemology, decision theory, ethics, and social implications of risk* (Vol. 1). Springer Science & Business Media.
Rousseau, D. M., Sitkin, S. B., Burt, R. S., & Camerer, C. (1998). Not so different after all: A cross-discipline view of trust. *Academy of management review*, *23*(3), 393-404. https://doi.org/10.5465/amr.1998.926617
Schinas, O., & Metzger, D. (2023). Cyber-seaworthiness: A critical review of the literature. *Marine Policy*, *151*, 105592. https://doi.org/10.1016/j.marpol.2023.105592
Sharma, A., Nazir, S., & Ernstsen, J. (2019). Situation awareness information requirements for maritime navigation: A goal directed task analysis. *Safety Science*, *120*, 745-752. https://doi.org/10.1016/j.ssci.2019.08.016
Short, J., James F, & Rosa, E. A. (2004). Some principles for siting controversy decisions: lessons from the US experience with high level nuclear waste. *Journal of Risk Research*, *7*(2), 135-152. https://doi.org/10.1080/1366987042000171276
Siegrist, M. (2000). The influence of trust and perceptions of risks and benefits on the acceptance of gene technology. *Risk analysis*, *20*(2), 195-204. https://doi.org/10.1111/0272-4332.202020
Siegrist, M. (2021). Trust and risk perception: A critical review of the literature. *Risk analysis*, *41*(3), 480-490. https://doi.org/10.1111/risa.13325
Siegrist, M., & Árvai, J. (2020). Risk perception: Reflections on 40 years of research. *Risk analysis*, *40*(S1), 2191-2206. https://doi.org/10.1111/risa.13599
Siegrist, M., Cvetkovich, G., & Roth, C. (2000). Salient value similarity, social trust, and risk/benefit perception. *Risk analysis*, *20*(3), 353-362. https://doi.org/10.1111/0272-4332.203034
Siegrist, M., Earle, T. C., & Gutscher, H. (2003). Test of a trust and confidence model in the applied context of electromagnetic field (EMF) risks. *Risk Analysis: An International Journal*, *23*(4), 705-716. https://doi.org/10.1111/1539-6924.00349
Siegrist, M., Keller, C., & Kiers, H. A. (2005). A new look at the psychometric paradigm of perception of hazards. *Risk Analysis: An International Journal*, *25*(1), 211-222. https://doi.org/10.1111/j.0272-4332.2005.00580.x

Sjöberg, L. (2004). Explaining individual risk perception: the case of nuclear waste. *Risk Management*, *6*(1), 51-64. https://doi.org/10.1057/palgrave.rm.8240172
Sjöberg, L. (2005). Risk perception as a factor in policy and decision making. *Management of uncertainty in safety cases and the role of risk*, 57-64. http://www.oecdnea.org/rwm/reports/2005/nea5302-management-uncertainty-risk.pdf#page=58
Sjöberg, L., & Fromm, J. (2001). Information technology risks as seen by the public. *Risk analysis*, *21*(3), 427-442. https://doi.org/10.1111/0272-4332.213123
Sjöberg, L., Moen, B.-E., & Rundmo, T. (2004). Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. *Rotunde publikasjoner Rotunde*, *84*, 55-76.
Skotnes, R. (2015). Risk perception regarding the safety and security of ICT systems in electric power supply network companies. *Safety Science Monitor*, *19*(1).
Slovic, P. (1987). Perception of risk. *Science*, *236*(4799), 280-285. https://doi.org/10.1126/science.3563507
Slovic, P. (1990). Perception of risk: Reflections on the psychometric paradigm. In *Theories of Risk*. Praeger.
Spagnoletti, P., & Za, S. (2022). Digital Resilience to Normal Accidents in High-Reliability Organizations. In *Engineering the Transformation of the Enterprise: A Design Science Research Perspective* (pp. 339-353). Springer. https://doi.org/10.1007/978-3-030-84655-8_21
Spencer, T. (2016). *Risk Perception*. Nova Science Publisher.
Starr, C. (1969). Social benefit versus technological risk. *Science*, 1232-1238. https://www.jstor.org/stable/1727970
International convention on standards of training, certification and watchkeeping for seafarers, (1978).
Strupczewski, G. (2021). Defining cyber risk. *Safety Science*, *135*, 105143. https://doi.org/10.1016/j.ssci.2020.105143
Tam, K., & Jones, K. (2019a). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*, 129-163. https://doi.org/10.1007/s13437-019-00162-2
Tam, K., & Jones, K. (2019b). Situational awareness: Examining factors that affect cyber-risks in the maritime sector. *International Journal on Cyber Situational Awareness*, *4*. https://pearl.plymouth.ac.uk/handle/10026.1/14948
Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. *computers & security*, *52*, 128-141. https://doi.org/10.1016/j.cose.2015.04.006
Tversky, A., & Kahneman, D. (1973). Availability: A heuristic for judging frequency and probability. *Cognitive psychology*, *5*(2), 207-232. https://doi.org/10.1016/0010-0285(73)90033-9
Tversky, A., & Kahneman, D. (1974). Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. *Science*, *185*(4157), 1124-1131. https://doi.org/10.1126/science.185.4157.1124
UiO. (2018). *Short introduction to Nettskjema*. Retrieved 27.09.2023 from https://www.uio.no/english/services/it/adm-services/nettskjema/about-nettskjema.html
Van Kleef, E., Fischer, A. R., Khan, M., & Frewer, L. J. (2010). Risk and benefit perceptions of mobile phone and base station technology in Bangladesh. *Risk Analysis: An*

International Journal, *30*(6), 1002-1015. https://doi.org/10.1111/j.1539-6924.2010.01386.x

Van Schaik, P., Jansen, J., Onibokun, J., Camp, J., & Kusev, P. (2018). Security and privacy in online social networking: Risk perceptions and precautionary behaviour. *Computers in Human Behavior*, *78*, 283-297. https://doi.org/10.1016/j.chb.2017.10.007

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior*, *75*, 547-559. https://doi.org/10.1016/j.chb.2017.05.038

Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., & Onibokun, J. (2020). Risk as affect: The affect heuristic in cybersecurity. *computers & security*, *90*, 101651. https://doi.org/10.1016/j.cose.2019.101651

Vasvári, T. (2015). Risk, Risk Perception, Risk Management-a Review of the Literature. *Public Finance Quarterly*, *60*(1), 29-48.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Weinstein, N. D. (1980). Unrealistic optimism about future life events. *Journal of personality and social psychology*, *39*(5), 806. https://doi.org/10.1037/0022-3514.39.5.806

Weinstein, N. D. (1987). Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample. *Journal of behavioral medicine*, *10*(5), 481-500. https://doi.org/10.1007/BF00846146

Weinstein, N. D., & Klein, W. M. (1995). Resistance of personal risk perceptions to debiasing interventions. *Health psychology*, *14*(2), 132. https://doi.org/10.1037/0278-6133.14.2.132

Weinstein, N. D., & Klein, W. M. (1996). Unrealistic optimism: Present and future. *Journal of Social and Clinical Psychology*, *15*(1), 1-8. https://doi.org/10.1521/jscp.1996.15.1.1

PART II

Paper 1

Cyber risk perception in the maritime domain: A systematic literature review

Authors: Marie Haugli Larsen and Mass Soldal Lund

IEEE Access, Volume 9, October 2021, Pages: 144895–144906, DOI: 10.1109/ACCESS.2021.3122433

IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 30, 2021, accepted October 13, 2021, date of publication October 25, 2021, date of current version October 29, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3122433

Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review

MARIE HAUGLI LARSEN[1] AND MASS SOLDAL LUND[2,3]
[1]Department of Ocean Operations and Civil Engineering, Norwegian University of Science and Technology, 6025 Aalesund, Norway
[2]Cyber Academy, Norwegian Defence University College, 2617 Lillehammer, Norway
[3]Department of Economics, BI Norwegian Business School, 0484 Oslo, Norway

Corresponding author: Marie Haugli Larsen (marie.h.larsen@ntnu.no)

This work was supported by the Grant from the Research Based Innovation Centre ''SFI Marine Operation in Virtual Environment (SFI-MOVE)'' by the Norwegian Research Council under Project 237929.

ABSTRACT This paper aims to present an approach to investigate cyber risk perception with use of recognized psychological models, and to give an overview of state-of-the-art research within the field of cyber risk perception in general and in the context of the maritime domain. The focus will be on determinative dimensions within the psychometric paradigm and cognitive biases, and to give recommendations on further research within these fields. Okoli and Schabram's eight-step guide to plan, select, extract, and execute a systematic literature review is used as guidance. The search process resulted in 25 relevant articles which describes 24 dimensions of cyber risk perception in different online environments. Research within the area of maritime cyber security is increasing, however, no studies relevant for our literature review were found within the maritime domain. The nine dimensions in the psychometric model, perceived benefit and the optimistic bias is presented and discussed in a maritime context. Cyber risk perception is a complex research-area where both determinative factors and other cognitive processes can be influenced by each other. This can indicate that the dimensions differ across populations and professions, creating grounds for why context-specific studies are important. Further research may benefit from more multidisciplinary, descriptive, and inductive approaches, and contextual studies within maritime cyber risk perception can contribute to develop targeted tools for risk mitigation to enhance safety at sea.

INDEX TERMS Maritime cyber security, risk perception, human behavior, psychometric paradigm, cognitive biases, marine safety, risk communication, cyberpsychology.

I. INTRODUCTION

In today's maritime operations there is an increasing reliance on digitalization, integration, automation, and networked-based systems. This increase in use of technology and connectivity makes operations at sea vulnerable to cyber risks [1], [2]. Recent security breaches put humans and the environment at risk and may generate financial losses for shipping companies [2], [3]. The hack of Maersk shipping lines in 2017 is one example of such a cyber incident. The ransomware attack caused a shutdown of Maersk operations in 13 international ports and losses of 300 million dollars [4], [5].

The International Maritime Organization (IMO) has recognized the urgent need to raise awareness on cyber risks and threats, publishing a resolution stating that an approved safety management system should consider cyber risks [6], [7]. Part of this process is the acknowledgement of cyber security as a human behavioral issue, and not just something the IT-departments should deal with [3], [8]. This is also substantiated by data indicating that human behavior is a frequent cause of cyber incidents, maliciously or unintentionally [9]–[12]. Even so, the main causes of cyber incidents occurring are complex, and in the context of maritime cyber security the humans can be both a vital resource and a risk [10], [13]. Therefore, it can be of importance to explore and understand human behavior in order to develop targeted frameworks, policies, and awareness and training programs which enable humans as resources while decreasing the cyber risks [11], [14], [15].

A way to understand human behavior is to investigate their risk perception to guide directions for developing appropriate

The associate editor coordinating the review of this manuscript and approving it for publication was Pedro R. M. Inácio.

mitigating measures. Risk perception is believed to be a significant social and psychological phenomenon, driving decision-making at various levels in society, and being an important factor in understanding people's reaction to technological risks [16], [17]. People use their subjective perceptions to construct their own reality and evaluate risk. How this happens is based on how information of a specific risk is communicated, the psychological mechanisms for processing uncertainty, and pervious experience [16], [18], [19].

Knowledge about what dimensions affect people's perception of specific risks (i.e. maritime cyber risks) can be used to outline tools to target human behavior, like policies, risk communication, training, and procedures [19]–[21]. Hence, it may be beneficial to identify the existing research specifically related to what dimensions affect people's perception of cyber risks. This can aid future research to address what tools can be developed to mitigate emerging cyber risks. To identify what research has already been conducted in this field, it is necessary to map out relevant papers systematically. The focus of this article is the psychometric paradigm and cognitive biases related to cyber risks at the individual level. In the maritime context, the stakeholders considered are the users of onboard systems, such as the deck officers, engineers, able seamen, and other onboard crew.

A. RESEARCH GOALS AND LAYOUT

This article presents a systematic literature review which purpose is to analyze existing studies and their findings, to summarize the research efforts regarding cyber risk perception. This study will answer the following research question: "What is state-of-the-art research in the field of cyber risk perception in general, and in the context of the maritime domain?" To achieve this, the structured literature review aims to answer the following sub-questions:

1. What are the main dimensions within the psychometric paradigm and cognitive biases related to cyber risk perception?
2. What is state-of-the-art research within the field of maritime cyber risk perception, and what recommendations can be given to future research within this field?

The paper is structured as follows: Section 2 presents background information about maritime cyber security and risk perception. Section 3 describes the methodology used to conduct the structured literature review. Section 4 presents the findings. Section 5 discusses the findings related to the research questions presented above. Section 6 concludes the research and provides recommendations for future research.

II. BACKGROUND

A. MARITIME CYBER SECURITY AND CYBER RISKS

The term 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" [22]. This definition includes users of cyberspace as assets in need of protection. At sea this is an important aspect since crew safety is crucial. The following paragraph will outline how cyber security can be related to safety.

Safety can be seen as the protection of life and health by the prevention of physical injury caused by damage to assets or to the environment [23]. Cyber security focuses on threats that can cause harm through cyberspace, and safety concerns incidents that can harm the surroundings (e.g., human life and health, physical assets, and environment). Even though the focuses of the two fields are different, they intertwine with each other in the way that safety incidents may have security impacts, in the same way that security incidents may have safety impacts [24]. For example, a cyber attack on a vessel's power distribution system that leads to a blackout, could have fatal safety consequences for the crew onboard. Furthermore, a safety incident, such as a fire or a collision, could leave onboard systems in an emergency state in which they could be more vulnerable to cyber risks.

Cyber risk can be defined as a risk that is caused by a threat that exploits cyberspace, e.g., services, computer systems, embedded processors and controllers, information in storage or transit [24]. When talking about cyber risks to systems onboard ships, it is common to divide the systems into two categories: Operational Technology (OT) and Information Technology (IT). The OT-systems onboard vessels are cyber-physical systems interacting with its surroundings [24], controlling the physical devices and processes onboard, e.g., cargo management systems, bridge systems, propulsion and machinery management, and power control systems. In contrast, the IT-systems manage data, e.g., access control systems, passenger servicing and management systems, public networks, administrative and crew welfare systems, communication systems, and ship to shore interfaces [6].

Historically, OT and IT have been stand-alone and separated systems, but because of the technological development and increase in connectivity, IT- and OT-systems are getting integrated to a larger extent than before. This creates new vulnerabilities, especially since disruption of the OT-systems may impose significant risk to the safety of crew members, the marine environment, the cargo, and the ship itself [15], [25].

Potential cyber-attacks towards the OT- and IT-systems can be divided into two main groups: un-targeted cyber-attacks (when the attacker uses tools and techniques available on the internet to locate and exploit widespread vulnerabilities) and targeted cyber-attacks (when the attacker use sophisticated tools and techniques specifically created for targeting a shipping company or a vessel) [25]. Combined with the increase in connectivity, the potential cyber-attacks create a whole new dimension of vulnerabilities towards vessels today. In [26], the authors give an overview of 46 maritime cyber security incidents from the last ten years and presents a list of the top 10 cyber threats towards the maritime industry. The incidents are relatively few, but with large consequences. However,

their study finds an increase in incidents over the period. Onboard and onshore IT-systems are most affected, but the study also identifies manipulation of GPS/GNSS signals and incidents targeting onboard OT-systems.

In the last decade, research has focused on vulnerabilities created by increased connectivity and lack of protection measures in the OT- and IT-systems. There are several incidents where the GPS-signal to an onboard Electronic Chart Display and Information System (ECDIS) has been spoofed or altered. In 2018, a group of researchers did an experiment where they attacked an Integrated Navigation System (INS) on a military training vessel with malware through use of an USB-stick and managed to alter the position of the vessel on the ECDIS-display [13].

Criminals can also benefit from the vulnerabilities in the maritime sector [4]. In 2013 the Belgium and Dutch authorities reported that members of a criminal group smuggled drugs through the harbor of Antwerp to the Netherlands. To do this, they used hackers to access the IT-systems which controlled the movement and location of containers [27].

A crew connectivity survey from 2018, with 6000 participating seafarers, reveals that 47% of the seafarers had sailed on a vessel that has been the target of a cyber-attack [9]. This can indicate that cyber-attacks at sea are happening quite frequently. However, a lack of a formal reporting system, or fear of reputation loss due, makes the reports of these incidents difficult to find [2].

The increase in connectivity and the technical development creates rapid changes in the maritime working environment and introduces new cyber vulnerabilities [5]. Therefore, it is important to make sure that the humans are kept in the loop [28]. To achieve this, one important aspect might be to understand how the crew is perceiving cyber risks towards the onboard systems, and what dimensions that affect these perceptions [29], [30].

B. RISK PERCEPTION

People use their subjective perception to construct their own reality and evaluate risk. How this happens is based on the psychological mechanisms for processing uncertainty, previous experience, and how information of a specific risk is communicated [16]. Risk perception can be defined as "a brain process where we reconstruct the previously assimilated risk through a subjective judgement" [31]. Since the 1970's researchers have identified a range of perception models and factors used by society in perceiving and assessing risk [16], [32]. Research within this field is multidisciplinary, and there are models of the risk perception process emerging from engineering, psychology, sociology, culture, and cognitive science [18], [31].

The psychometric paradigm, emerging from the psychology-field, is an acknowledged model within the field of risk perception research [31], [32]. The model is used in many disciplines and widely recognized [20]. It describes nine dimensions of risk perception, and is based on several explanatory scales such as *new-old, voluntary-unvoluntary,* etc. This scaling and multivariate analysis technique is used to produce quantitative representations, called "cognitive maps", of people's risk attitudes and perceptions, in order to understand and predict risk responses [19], [21]. The psychometric model is criticized for using aggregated data, giving the dimensions a stronger correlation than if they use raw data [18], [33], [34]. Even so, many studies have used this approach in studying risk perception across various risky domains [34]–[36].

The work of Kahneman and Tversky on heuristics and biases has played an important role in the discussion of risk perception [37]–[40]. Both the psychometric dimensions and heuristics may influence certain biases in risk perception. A recognized and well documented bias is the optimistic bias, which demonstrates a systematic discrepancy between people's risk perceptions and their actual risk for experiencing negative or positive events [41]–[45].

Research in perception of cyber risks draws to some extent on the psychometric paradigm [46], and studies within this field has increased in recent years [47]. Another emerging research field within human behavior in cyberspace is cyberpsychology [30], [48]. This research paradigm applies psychological theories to explain how individuals interact in cyberspace, and how new identities are built in cyberspace through social interactions [49], [50]. The cyberpsychology paradigm and the risk perception paradigm are studying subjective variables, but they prioritize different variables [51]. Research shows that there is a cross-effect between perceptual and/or attitudinal factors in these paradigms, making the psychometric dimensions affecting online behavior and vice versa [30]. The next section will outline the research methodology used in this study, and how relevant literature was acquired.

III. RESEARCH METHODOLOGY

This study was conducted under the guidance published by Okoli and Schabram [52]. They present an eight-step guide to conducting a Systematic Literature Review (SLR), as illustrated in Fig. 1. This section will describe the planning, selection, extraction, and execution stages of this process.

A. PLANNING

To conduct this SLR in line with the purpose outlined by the research goals and layout, a protocol was created. The protocol was first used to conduct a training process, and to reveal limits and issues to be resolved before the search for relevant literature was conducted. After this process, the protocol was developed further, with more detailed criteria for the quality appraisal, and a table for documenting the search history.

B. SELECTION

1) SEARCHING THE LITERATURE

Relevant papers were detected by passing keywords to the search field in several digital databases. Because of the multidisciplinary nature of the research area, the databases

were chosen to include the range of research fields within cyber risk perception and the maritime domain. The keywords were selected to promote the emergence of research results that would assist in answering the research questions. The Boolean operators were restricted to AND. An example of the search strings used is:

"maritime" AND "information security" AND "risk" AND "perception"

- The digital databases searched were:
- SpringerLink
- Science direct
- PsycINFO
- Web of Science
- SAGE journals
- IEEE Xplore: digital library
- EBSCO (Academic Search Complete, CINAHL Complete, EconLit with Full Text, Psychology and Behavioural Sciences Collection, Sociology Source Ultimate)
- Taylor & Francis Online

The following keywords was used when conducting the search: risk perception, cyber threat, cyber risk, cyber security, information security, security risk, risk, maritime, marine, offshore, cyberpsychology, policy. The full list of search strings is found in the appendix.

The searches were run against the title, keywords or abstract, depending on the database. No time limitations were used in the searches, and they were conducted in June 2021. The results from these searches were filtered through the practical screening criteria and then the quality appraisal criteria, presented in the following sections.

C. PRACTICAL SCREENING

To establish which papers should be included in the SLR, the key inclusion and exclusion criteria used for the practical screening phase were as follows:

- The paper must be peer-reviewed and published in a conference proceeding or journal.
- The paper must contain research related to perception of cyber risks.
- The paper must be written in English.
- Grey literature such as blogs and government documents are not assessed.

The practical screening in the nine chosen databases identified 80 articles. Backtracking was done by reading the reference lists of the identified articles, adding an additional 19 articles to the list.

D. EXTRACTION

1) QUALITY APPRAISAL

After all the potentially eligible articles were chosen in the practical screen, the next step was to examine the articles more closely to assess their quality. The following inclusion and exclusion criteria were chosen to ensure the methodological quality of the articles [52]:

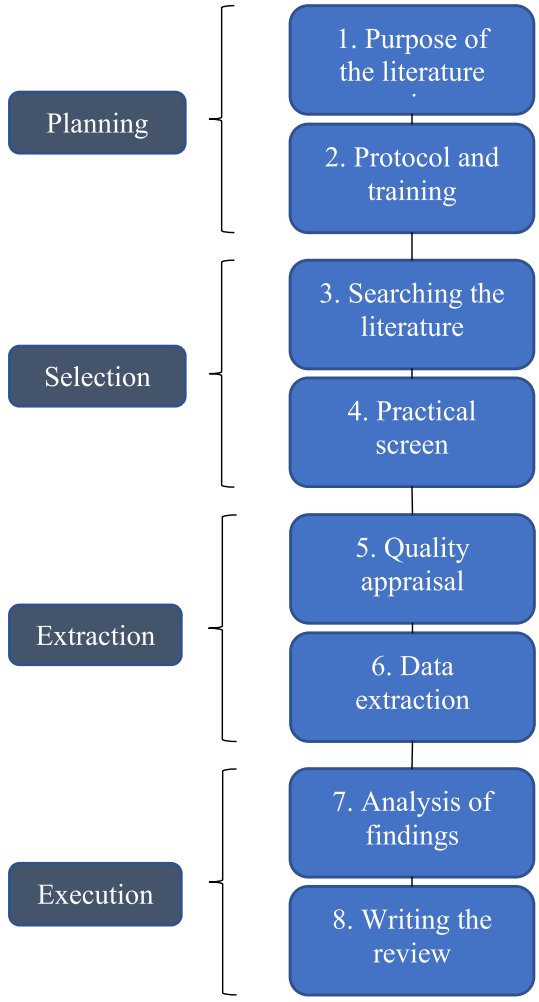


FIGURE 1. A systematic guide to literature review development [52].

- The paper must present empirical data related to risk perception research within the psychometric paradigm, research developed within this paradigm, or research related to cognitive biases and risk perception.
- Papers focusing on risk perception research within other theoretical frameworks than the psychometric paradigm, e.g., protection motivation theory, are not included.
- Papers focusing on gender or geographical factors are not included.
- The purpose of the paper must be within these classifications:
  - How policies
  - should be outlined
  - Risk communication
  - Risk mitigation measures or demand for risk mitigation

- Prediction of security behavior

When all 99 articles from the practical screening were tested against the quality criteria, the number of articles was reduced to 25. The selection process of papers is shown in Fig. 2, and the rationale for exclusion of studies in Fig. 3. Number of papers published over time is presented in Fig. 4.

E. DATA EXTRACTION

In this stage, relevant information was systematically taken from each of the 25 papers that passed the quality appraisal. The data extraction process was initially tested on 3 studies before being expanded to include all the papers. The data from each study were extracted and categorized. The categories given to the data were as follows:

- Context data: Information about the purpose of the study.
- Methodology: Information about methodology and data collection methods.
- Research questions: The research questions or hypothesis outlined in the study.
- Qualitative data: Findings and conclusions relevant for this SLR's research questions.

F. EXECUTION

The information from the data extraction stage were analyzed by conducting a qualitative synthesizes of the qualitative and the quantitative studies selected [52]. Relevant information about the different dimensions of cyber risk perception were extracted and synthesized. The product of this process is presented in the next section.

IV. RESULTS

This section presents the findings linked to the research questions outlined in research goals and layout.

A. DIMENSIONS OF CYBER RISK PERCEPTION

The 25 articles describe 24 dimensions of cyber risk perception in different online environments. Table 1 presents an overview of the dimensions and which articles they appear in as determinate factors. Because of the focus on the psychometric paradigm and cognitive biases in this SLR model, this section will further describe the nine dimensions in the psychometric model (voluntariness, immediacy of risk consequences, knowledge to exposed, knowledge to science/experts, controllability, catastrophic potential, dread vs. common, newness, severity of consequences), perceived benefit, and the optimistic bias [19], [21], [42]. These dimensions also coincide with the most referred dimensions in the articles.

1) VOLUNTARINESS

To what extent people think they get into risky online situations voluntarily has been found a negative determinant of risk perception in seven studies in this review [47], [53]–[58]. It seems that the less voluntary people perceive exposure to a cyber threat to be, the riskier they perceive the specific threat to be. One example is a study of Facebook-users perception of security and privacy threats [58]. The findings in these studies provide support for Starr's [75] notion of people's risk-benefit trade-offs, and it may also lead to optimism bias regarding cyber risks [44].

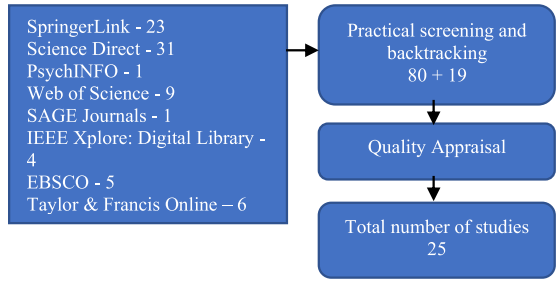


FIGURE 2. Selection process of papers.

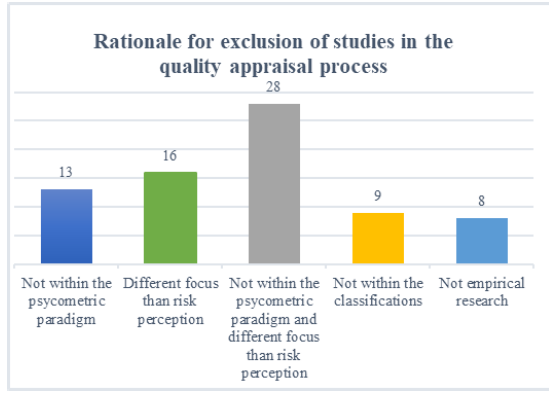


FIGURE 3. Rationale for exclusion of studies in the quality appraisal process.

2) IMMEDIACY OF RISK CONSEQUENCES

Several of the studies investigated if immediacy of risk consequences has an impact on people's perception of various cyber risks [36], [47], [57]–[62]. These findings indicate that the greater the perceived immediacy of cyber risks are, the higher the perceived risk seems to be. This is consistent with previous work that indicates that perceived risk is reduced when negative consequences are likely to be delayed [76].

3) KNOWLEDGE TO EXPOSED

This dimension is investigating to what extent the cyber risks are known by the persons who are exposed to such risks [19]. The findings indicate that in most cases when people have knowledge of, and are familiar with the cyber risk in question [72], they perceive the risk as lower than if they have limited knowledge [56], [57], [61], [63]–[65]. In one of the studies the result was the opposite, but the values were not statistically significant [58]. In another study, knowledge to

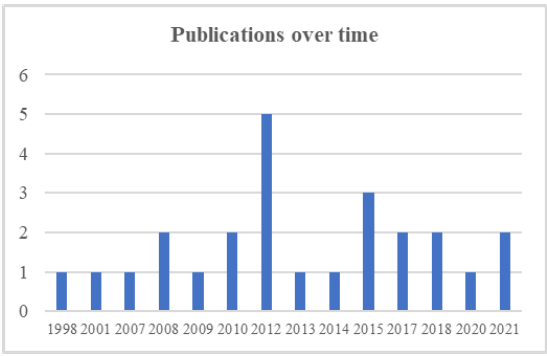


FIGURE 4. Number of papers published over time.

the exposed was found to be not significant before it was clustered together with knowledge to science [55].

4) KNOWLEDGE TO SCIENCE/EXPERTS

To what degree people believe cyber risks are known to experts, or science, affects people's level of perceived risk [21], [32]. Three studies in this SLR found this dimension a determining factor of perceived risk, seeing that knowledge to experts in general tends to reduce perceived risk [55], [57], [58]. Findings in two studies of online privacy risks suggest that people tend to share more information online when knowledge to experts is regarded as high [57], [58].

5) CONTROLLABILITY

To the extent people believe they can control threats and avoid them from happening, their perception of risk is reduced [32]. Findings in seven of the studies may suggest that this can be the case for various cyber risks [36], [47], [53], [55], [56], [64], [66]. Perceived control over individual threats was found to be a negative predictor of perceived risk. It is also indicated that some of these risks can be seen as controllable as typical lifestyle risks – e.g. smoking and drinking alcohol [53]. The feeling of control can also be an influencing factor in optimistic bias [41].

6) CATASTROPHIC POTENTIAL

Three of the studies found catastrophic potential as a positive determinant for cyber risk perception [47], [54], [58]. This is consistent with the idea that threats with a larger impact on a single occasion (catastrophic risk) are perceived riskier than threats with less impact (chronic risk), which also can be related to the availability heuristic [19], [72], [73].

7) DREAD VS. COMMON

Dread vs. common measures whether the online risk in question is something people have learned to live with, or whether it is a risk they have great dread for [21], [55]. Five of the articles in this review found this dimension to have great impact on people's risk perception of various online risks [36], [47], [54], [55], [58], [65]. Dreaded online risks are identity theft, social engineering, sharing of personal information in social networks and cyber bullying [36], [54].

TABLE 1. Overview of determinate dimensions of risk perception. The dimensions discussed further are emphasized.

Dimensions of cyber risk perception	Articles describing the dimensions
Voluntariness	[47], [53]-[58]
Immediacy of risk consequences	[36], [47], [57]-[62]
Knowledge to exposed	[55]-[58], [61], [63]-[65]
Knowledge to science/ experts	[55], [57], [58]
Controllability	[36], [47], [53], [55], [56], [64], [66]
Catastrophic potential	[47], [54], [58]
Dread vs. common	[36], [47], [54], [55], [58], [65]
Newness	[36], [55]
Severity of consequences	[47], [56]-[58], [64], [67]
Unfamiliarity of risks	[36], [68]
Optimistic bias	[44], [53], [66], [69], [70]
Self-efficacy	[69]
Attitude	[53], [54]
Sensation-seeking	[71]
General/personal risk	[53], [70]
Organizational trust	[72]
The availability heuristic	[68], [72]
Affect	[73]
Perceived benefit	[62], [67], [73], [74]
Awareness	[63], [64]
Understanding	[62]
Impact/temporal impact	[55], [64]
Possibility	[64]
Potential for embarrassment	[67]

8) NEWNESS

If the risks in question are regarded as new or novel, they tend to be perceived as riskier and less controllable [21]. The results in two of the studies show that newness, or unfamiliarity, can be a positive determinant for risk perception of online risks [36], [55]. One of the studies implies that when risks get older, they may be perceived as more low level, contextual and concrete [55].

9) SEVERITY OF CONSEQUENCES

When risks are perceived to have more severe consequences, they are perceived to be riskier [21]. This is consistent with the results in six of the articles in this review.

All studies reported high correlation between severity and risk perception of cyber risks and online activities with perceived high consequences [47], [56]–[58], [64], [67]. Financial activities, online gambling and sharing personal information are examples of activities with possible severe consequences [67].

10) PERCIEVED BENEFIT

Previous research has proven an inverse relationship between risk and benefit, where high-risk technologies tend to be perceived low in benefit, and vice versa [77]. This coincides with the results in four of the studies in this SLR when looking at the relationship between online risks and benefit [62], [67], [73], [74]. In [74], information technology in general was perceived as relatively low risk and high benefit technology. Further, activities related to information technology (i.e., sending/receiving email, online gambling, social networking) display the same inverse relationship between risk and benefit [67].

11) OPTIMISTIC BIAS

Studies of risk perception have shown that people demonstrate a strong tendency to interpret ambiguous information or uncertain situations in a self-serving direction, they have an ''optimistic bias'' [41], [78]. Five of the studies found that people tend to believe others to be more exposed to cyber risks then themselves [44], [53], [66], [69], [70]. Some results are also showing that optimistic bias is influenced by other risk perception dimensions, like voluntariness, controllability, the availability heuristic, and the difference between personal and general risk [44], [53], [70], [72].

B. CYBER RISK PERCEPTION IN THE MARITIME DOMAIN

The search stage of this SLR did not reveal any studies within cyber risk perception in the maritime domain. However, research conducted in the area of maritime cyber security has increased over the last decade, mainly focusing on emerging cyber risks, investigating people's awareness of these risks, and make recommendations on implementation of cyber security measures [9], [14]. Even so, this is a novel research-field, and have so far payed little attention to the decision-makers and their roles [3], [14].

Nonetheless, the recommendations given in literature to maritime companies on implementing cyber security measures, may indicate that research within cyber risk perception should be of interest. The recommendations include a top-down approach when implementing measures, development of an international and holistic cyber security policy, a tailored education program for the employees onshore and offshore, development and implementation of company-specific procedures and risk assessment methods [1]–[3], [7], [8], [11], [15], [25]. The next section will discuss how research within cyber risk perception may contribute in the maritime context, and present limitations within this SLR.

V. DISCUSSION

The increase in connectivity and the technological development in the maritime domain make the distinction between safety and security incidents blurry and introduce new vulnerabilities at sea [24]. The crew need to ensure they don't lose control over the OT-technology onboard, and the maritime companies need to protect their IT-systems to avoid financial losses or loss of valuable information. In order to facilitate understanding and promote good security judgement, the maritime domain may be dependent on insight into human behavior and an understanding of how the crew perceive cyber risks to their onboard systems [46], [47], [79].

Research within the psychometric paradigm and biases about cyber risk perception elicit some reflections on how this can contribute to the maritime context. The results in this SLR show that the dimensions of voluntariness, dread and knowledge are often found to be determinants [47], [55], [64]. This coincides with the well-known study of Fischhoff *et al.* [21], which indicates that society may accept higher levels of risk with more beneficial activities and tolerate higher risk levels for voluntary activities. The study also showed that people's perceptions of common risks are normally reduced, while uncommon risks evoke dread. Use of technology are increasing in all professions, and for many people the use of internet is a common activity [47]. The extent to which the crew have awareness of the potential consequences of increased connectivity and use of technology can decide if they overestimate or underestimate the risk of a cyber incident [18]. This also evokes certain questions: Are the perceived benefits of the onboard technology so high that the crew accept the level of risk? Do they see the use of technology as voluntary activities, or more as something new and involuntary? Is this something the crew even consider since they are totally dependent on the OT-technology to function in their daily work? These can be important questions to answer in the cyber security policy-making process.

The working environment on board a vessel is considered quite isolated and confined [80], and the International Convention for the Safety of Life at Sea (SOLAS) is stating that the crew are responsible for their own safety, and to uphold the seaworthiness of their vessel [81]. To achieve this, the crew are dependent on the onboard systems to be working, and to have control over the vessel at all times. Controllability is a common determinant for risk perception [18], [36], [47], and due to the distinct nature of working at sea, this dimension can be important. To what extent the crew believe they can control cyber risks and avoid them from happening, can affect their level of risk perception. This may also be related to the dimensions of newness and knowledge to the exposed, since risks regarded as new or unfamiliar may be perceived as less controllable [19], [21], [55]. Knowledge about how the crew are experiencing cyber risks in terms of controllability and newness may be essential to develop appropriate training, procedures and raise awareness about the issue [31], [34], [46].

In a maritime environment, the severity and immediacy of risk consequences are important because of the limited resources available [80]. For example, if the vessel is in a distress situation and the crew need to evacuate, they cannot just ''leave the building''. Furthermore, the crew must be trained in handling emergency situations themselves since a rescue team can be very far away or not able to reach them at all. Because of this, the rules and regulations emphasize the importance of executing frequent risk assessments, training scenarios, and drilling exercises on board [28], [81], [82]. However, until recently, there has been a lack of focus from legislation on assessing and training to handle cyber risks on vessels [2], [25]. This, in combination with the intangible nature of cyber risks [55], might make it difficult for the crew to perceive the consequences of such risks towards their onboard systems. If this is the case, the dimension of catastrophic potential may also be of importance. The crew might perceive cyber risks as threats with less impact because examples of cyber incidents with catastrophic consequences may not come easily to mind [37], [38], [73].

How the onboard technology is affecting the crew's safety is something to consider, since they may not be able to perceive the risk to themselves, in line with the results showing that people display optimistic bias in relation to cyber risks [44], [53], [66], [69], [70]. People claim they are less at risk than their peers in many cases, and to what degree the crew exhibit unrealistic optimism in relations to cyber risks can give an indication to how policies should be outlined for communication purposes, and to predict the demand for risk mitigation [78], [83], [84].

The dimensions outlined in this SLR give a notion about how complex the research area of cyber risk perception is, where both determinative factors and other processes can influence each other. This also indicates that the dimensions differ across populations and professions, creating grounds for context-specific studies within maritime cyber risk perception. Previous research has proven that risk perception has implications on policy, risk communication and human behavior [20], [32], [38], [76], [85], making this an important research area for improving our ability to mitigate risks and enhance safety at sea.

Even if this SLR did not reveal any studies within maritime cyber risk perception, the research field of maritime cyber security is growing, and new research is emerging [2], [3]. However, most of this research lacks a theoretical foundation and make little use of models. The available literature on maritime cyber security predominantly applies insights of cyber security to a maritime context without considering the particularities of the maritime domain, while the literature that does, is usually concerned with maritime OT-systems and technical aspects of cyber security [3], [14], [10], [86].

It is well established that humans play an important role in cyber security. We have no indications that the situation should be any different in the maritime domain, and the SLR also indicates that not much research has been conducted within human behavior and maritime cyber security. This motivates research that gives the onboard crew the attention they deserve regarding this topic [11], [28]. This paper is a start on such work, where an established model for the human side of cyber security (i.e., cyber risk perception) is investigated with the purpose of understanding maritime cyber security on the premise of the humans operating in the maritime domain. As the SLR shows, this angle has not been taken before. Therefore, this paper discusses the possible implications of the model in a maritime context and indicates how these approaches can be utilized for further research.

A. LIMITATIONS

Since there is no extensive theory explaining cyber risk perception, there might be other factors relevant in addition to those presented in this SLR [31]. Because risk perception is a subjective cognitive process, the dimensions can vary from population to population, from context to context and from profession to profession [34], [87]. Limitations are also given in the studies sampling, where most of the participants was students, experts or populations chosen for demographic reasons. A weakness may be that some authors are represented with three or more articles in this SLR, making the total number of articles somewhat higher than the total number of studies.

Some of the studies in this SLR question the appropriateness of using a model developed for physical risks to measure cyber risks, but without going into further details about it. This topic may call for a greater discussion, and the research within cyber risk perception might benefit from applying variables from the cyberpsychology paradigm to understand the width of how cyberspace is affecting cyber risk perception and human behavior [30], [48]–[50].

VI. CONCLUSION

Throughout the decades of risk perception research, it has uncovered many determinative factors for people's perception of various risks [16]. The focus of this SLR has been on dimensions of cyber risk perception within the psychometric paradigm and cognitive biases in general, and in the maritime domain. By use of these recognized psychological models, humans' cyber risk perception can be investigated, and tools for risk mitigation developed. It is important to pay more attention to human behavior within maritime cyber security, and to understand how we can enable the humans operating in the maritime domain.

Further research may benefit from a more descriptive and inductive approach, to potentially discover new nuances of the dimensions affecting humans' perception of cyber risks. Another aspect to investigate further might be to what extent the risk perception paradigm and the cyberpsychology paradigm are interrelated, and how these research fields can complement each other.

Finally, to investigate what dimensions that are valid in the maritime domain, further research should focus on how the maritime crew are perceiving cyber risks. Contextual studies within the field of maritime cyber risk perception

may provide new knowledge which can aid the ongoing work of developing cyber security policies, procedures, education programs and risk assessment methods.

APPENDIX

Search strings used in the literature search:

"Risk perception" AND "security risk" AND "information security"
"Risk perception" AND "cyber risk" AND "cyber security"
"Risk perception" AND "cyber threats"
"Risk perception" AND "risk" AND "information security"
"Risk perception" AND "risk" AND "cyber security"
"Perception of cyber risk"
"Maritime" AND "Security" AND "risk perception" AND "information"
"Perception of risk" AND "cyber risk"
"Perception of risk" AND "cyber threats"
"Cyber risk" AND "risk perception" AND "policy"
"Maritime" AND "information security" AND "risk" AND "perception"
"Risk perception" AND "information security"
"Maritime" AND "Information security" AND "risk perception"
"Marine" AND "Cyber risk" AND "risk perception"
"Risk perception" AND "cyber security"
"Maritime" AND "cyber risk"
"Offshore" AND "Cyber risk" AND "risk perception"
"Offshore" AND "cyber security" AND "risk perception"
"Cyberpsychology" AND "risk perception" AND "cyber"
"Cyberpsychology" AND "risk" AND "perception"
"Cyberpsychology" AND "risk perception" AND "information security"

REFERENCES

[1] J. DiRenzo, D. A. Goward, and F. S. Roberts, "The little-known challenge of maritime cyber security," in *Proc. 6th Int. Conf. Inf., Intell., Syst. Appl. (IISA)*, Jul. 2015, pp. 1–5.

[2] P. McGillivary, "Why maritime cybersecurity is an ocean policy priority and how it can be addressed," *Mar. Technol. Soc. J.*, vol. 52, no. 5, pp. 44–57, Sep. 2018, doi: 10.4031/MTSJ.52.5.11.

[3] J. I. Alcaide and R. G. Llave, "Critical infrastructures cybersecurity and the maritime sector," *Transp. Res. Proc.*, vol. 45, pp. 547–554, Jan. 2020, doi: 10.1016/j.trpro.2020.03.058.

[4] C. Baraniuk, *How Hackers are Targeting the Shipping Industry*. London, U.K.: BBC News, 2017. [Online]. Available: https://www.bbc.com/news/technology-40685821

[5] M. Lehto, "Cyber security in aviation, maritime and automotive," in *Computation and Big Data for Transport*. Cham, Switzerland: Springer, 2020, pp. 19–32.

[6] IMO. (2017). *Guidelines on Maritime Cyber Risk Management*. [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3-GuidelinesOnMaritimeCyberRiskManagement(Secretariat).pdf

[7] I. Mraković and R. Vojinović, "Maritime cyber security analysis—How to reduce threats?" *Trans. Maritime Sci.*, vol. 8, no. 1, pp. 132–139, Apr. 2019, doi: 10.7225/toms.v08.n01.013.

[8] M. E. Whitman and H. J. Mattord, *Management of Information Security*, 6th ed. Boston, MA, USA: Cege, 2019.

[9] FuturenauticsMaritime, KVH, and Intelsat. (2018). *Crew Connectivity 2018 Survey Report*. London, U.K. [Online]. Available: http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf

[10] P. B. Kristoffersen, T. Hartvigsen, P. Myrvang, and A. Torjusen, *Digitale SåRbarheter Maritim Sektor*. Bærum, Norway: DNVGL, 2015. [Online]. Available: https://www.regjeringen.no/contentassets/fe88e9ea8a354bd1b63bc0022469f644/no/sved/7.pdf

[11] O. Fitton, D. Prince, B. Germond, and M. Lacy, *The Future of Maritime Cyber Seurity*. Lancaster, U.K.: Lancaster Univ., 2015. [Online]. Available: https://eprints.lancs.ac.uk/id/eprint/72696/

[12] KnowBe4. (2019). *The 2019 What Keeps You up at Night Report*. Clearwater. [Online]. Available: https://blog.knowbe4.com/the-2019-what-keeps-you-up-at-night-report

[13] O. S. Hareide, Ø. Jøsok, M. S. Lund, R. Ostnes, and K. Helkala, "Enhancing navigator competence by demonstrating maritime cyber security," *J. Navigat.*, vol. 71, no. 5, pp. 1025–1039, Sep. 2018, doi: 10.1017/S0373463318000164.

[14] A. Garcia-Perez, M. Thurlbeck, and E. How, "Towards cyber security readiness in the Maritime industry: A knowledge-based approach," *Semantic Scholar*, pp. 1–7, 2017. [Online]. Available: https://pure.coventry.ac.uk/ws/portalfiles/portal/12219284/Towards_Cyber_Security_Readiness_In_The_Maritime_Industry.pdf

[15] W. He and Z. Zhang, "Enterprise cybersecurity training and awareness programs: Recommendations for success," *J. Organizational Comput. Electron. Commerce*, vol. 29, no. 4, pp. 249–257, Oct. 2019, doi: 10.1080/10919392.2019.1611528.

[16] O. Renn, "Perception of risks," *Toxicol. Lett.*, vol. 149, nos. 1–3, pp. 405–413, Apr. 2004, doi: 10.1016/j.toxlet.2003.12.051.

[17] J. J. F. Short and E. A. Rosa, "Some principles for siting controversy decisions: Lessons from the US experience with high level nuclear waste," *J. Risk Res.*, vol. 7, no. 2, pp. 135–152, Mar. 2004, doi: 10.1080/1366987042000171276.

[18] S. Roeser, *Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk*. Berlin, Germany: Springer, 2012.

[19] P. Slovic, "Perception of risk," *Science*, vol. 236, pp. 280–285, Apr. 1987, doi: 10.1126/science.3563507.

[20] L. Sjöberg, "Risk perception as a factor in policy and decision making," in *Management of Uncertainty Safety Cases and the Role of Risk*. Stockholm, Sweden: OECD, 2005, pp. 57–64. [Online]. Available: http://www.oecdnea.org/rwm/reports/2005/nea5302-management-uncertainty-risk.pdf#page=58

[21] B. Fischhoff, P. Slovic, S. Lichtenstein, S. Read, and B. Combs, "How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits," *Policy Sci.*, vol. 9, no. 2, pp. 127–152, Apr. 1978, doi: 10.1007/BF00143739.

[22] R. von Solms and J. van Niekerk, "From information security to cyber security," *Comput. Secur.*, vol. 38, pp. 97–102, Oct. 2013, doi: 10.1016/j.cose.2013.04.004.

[23] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004, doi: 10.1109/TDSC.2004.2.

[24] A. Refsdal, B. Solhaug, and K. Stølen, "Cyber-risk management," in *Cyber-Risk Management*. Cham, Switzerland: Springer, 2015, pp. 9–47.

[25] *Guidelines on Cyber Security Onboard Ships—Version 3*, BIMCO, CLIA, ICS, Intercargo, Intertanko, and OCIMF, Bagsvaerd, Denmark, 2017.

[26] P. H. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. A. Nesheim, "A retrospective analysis of maritime cyber security incidents," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 15, no. 3, pp. 519–530, 2021.

[27] T. Bateman, "Police warning after drug traffickers' cyber-attack," in *BBC News*. London, U.K.: BBC, 2013.

[28] E. Erstad, R. Ostnes, and M. S. Lund, "An operational approach to maritime cyber resilience," *TransNav, Int. J. Mar. Navigat. Saf. Sea Transp.*, vol. 15, no. 1, pp. 27–34, 2021, doi: 10.12716/1001.15.01.01.

[29] M. Bada and J. R. Nurse, "The social and psychological impact of cyberattacks," in *Emerging Cyber Threats and Cognitive Vulnerabilities*. Amsterdam, The Netherlands: Elsevier, 2020, pp. 73–92.

[30] J. Wang and S. Kim, "Searching for new directions for energy policy: Testing the cross-effect of risk perception and cyberspace factors on online/offline opposition to nuclear energy in South Korea," *Sustainability*, vol. 11, no. 5, p. 1368, Mar. 2019, doi: 10.3390/su11051368.

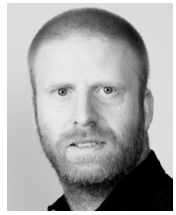
[31] T. Spencer, *Risk Perception*. Hauppauge, NY, USA: Nova Science Publisher, 2016.

[32] P. Slovic, "Perception of risk: Reflections on the psychometric paradigm," in *Theories of Risk*. New York, NY, USA: Praeger, 1990.

[33] L. Sjöberg, "Risk perception and societal response," in *Handbook Risk Theory*. Berlin, Germany: Springer, 2012, pp. 661–675.
[34] M. Siegrist, C. Keller, and H. A. L. Kiers, "A new look at the psychometric paradigm of perception of hazards," *Risk Anal.*, vol. 25, no. 1, pp. 211–222, Feb. 2005, doi: 10.1111/j.0272-4332.2005.00580.x.
[35] L. Sjöberg, B.-E. Moen, and T. Rundmo, "Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research," *Rotunde Publikasjoner*, vol. 84, pp. 55–76, Dec. 2004.
[36] I. J. Gabriel and E. Nyshadham, "A cognitive map of people's online risk perceptions and attitudes: An empirical study," in *Proc. 41st Annu. Hawaii Int. Conf. Syst. Sci. (HICSS)*, Jan. 2008, p. 274.
[37] D. Kahneman, S. P. Slovic, P. Slovic, and A. Tversky, *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge, U.K.: Cambridge Univ. Press, 1982.
[38] A. Tversky and D. Kahneman, "Availability: A heuristic for judging frequency and probability," *Cognit. Psychol.*, vol. 5, no. 2, pp. 207–232, Sep. 1973, doi: 10.1016/0010-0285(73)90033-9.
[39] B. Combs and P. Slovic, "Newspaper coverage of causes of death," *Journalism Quart.*, vol. 56, no. 4, pp. 837–849, Dec. 1979.
[40] M. G. McCombs and S. Gilbert, "News influence on our pictures of the world," in *Perspective Media Effects*, D. Nimmo and D Zillmann, Ed. Hillsdale, NJ, USA: Lawrence Erlbaum, 1986, pp. 1–16.
[41] N. D. Weinstein, "Unrealistic optimism about susceptibility to health problems: Conclusions from a community-wide sample," *J. Behav. Med.*, vol. 10, no. 5, pp. 481–500, Oct. 1987, doi: 10.1007/BF00846146.
[42] N. D. Weinstein and W. M. Klein, "Unrealistic optimism: Present and future," *J. Social Clin. Psychol.*, vol. 15, no. 1, pp. 1–8, Mar. 1996, doi: 10.1521/jscp.1996.15.1.1.
[43] N. D. Weinstein and W. M. Klein, "Resistance of personal risk perceptions to debiasing interventions," *Health Psychol.*, vol. 14, no. 2, p. 132, 1995, doi: 10.1037/0278-6133.14.2.132.
[44] J. Campbell, N. Greenauer, K. Macaluso, and C. End, "Unrealistic optimism in internet events," *Comput. Hum. Behav.*, vol. 23, no. 3, pp. 1273–1284, May 2007, doi: 10.1016/j.chb.2004.12.005.
[45] N. D. Weinstein, "Unrealistic optimism about future life events," *J. Personality Social Psychol.*, vol. 39, no. 5, p. 806, 1980, doi: 10.1037/0022-3514.39.5.806.
[46] J. R. C. Nurse, S. Creese, M. Goldsmith, and K. Lamberts, "Trustworthy and effective communication of cybersecurity risks: A review," in *Proc. 1st Workshop Socio-Tech. Aspects Secur. Trust (STAST)*, Sep. 2011, pp. 60–68, doi: 10.1109/STAST.2011.6059257.
[47] P. van Schaik, D. Jeske, J. Onibokun, L. Coventry, J. Jansen, and P. Kusev, "Risk perceptions of cyber-security and precautionary behaviour," *Comput. Hum. Behav.*, vol. 75, pp. 547–559, Oct. 2017, doi: 10.1016/j.chb.2017.05.038.
[48] R. McCall, "Infinite reality: Avatars, eternal life, new worlds, and the dawn of the virtual revolution," *Presence, Teleoperators Virtual Environ.*, vol. 20, no. 5, p. 502, 2011.
[49] A. K. Singh and P. K. Singh, *Recent Trends, Current Research in Cyberpsychology: A Literature Review*. Lincoln, NE, USA: Library Philosophy and Practice, 2019.
[50] J. R. Ancis, "The age of cyberpsychology: An overview," *Technol., Mind, Behav.*, vol. 1, no. 1, pp. 1–15, Sep. 2020, doi: 10.1037/tmb0000009.
[51] M. C. Howard and B. S. Jayne, "An analysis of more than 1,400 articles, 900 scales, and 17 years of research: The state of scales in cyberpsychology, behavior, and social networking," *Cyberpsychol., Behav. Social Netw.*, vol. 18, no. 3, pp. 181–187, 2015, doi: 10.1089/cyber.2014.0418.
[52] C. Okoli and K. Schabram. (2010). *A Guide to Conducting a Systematic Literature Review of Information Systems Research*. [Online]. Available: http://sprouts.aisnet.org/10-26
[53] L. Sjoberg and J. Fromm, "Information technology risks as seen by the public," *Risk Anal.*, vol. 21, no. 3, pp. 427–442, Jun. 2001, doi: 10.1111/0272-4332.213123.
[54] P. van Schaik, J. Jansen, J. Onibokun, J. Camp, and P. Kusev, "Security and privacy in online social networking: Risk perceptions and precautionary behaviour," *Comput. Hum. Behav.*, vol. 78, pp. 283–297, Jan. 2018, doi: 10.1016/j.chb.2017.10.007.
[55] V. Garg and J. Camp, "End user perception of online risk under uncertainty," in *Proc. 45th Hawaii Int. Conf. Syst. Sci.*, Jan. 2012, pp. 3278–3287, doi: 10.1109/HICSS.2012.245.
[56] V. Garg and L. J. Camp, "Cars, condoms, and Facebook," in *Information Security*. Cham, Switzerland: Springer, 2015, pp. 280–289.
[57] V. Garg, L. J. Camp, K. Connelly, and L. Lorenzen-Huber, "Risk communication design: Video vs. text," in *Proc. Int. Symp. Privacy Enhancing Technol. Symp.* Berlin, Germany: Springer, 2012, pp. 279–298, doi: doi.org/10.1007/978-3-642-31680-7_15.
[58] V. Garg, K. Benton, and L. J. Camp, "The privacy paradox: A Facebook case study," in *Proc. TPRC Conf. Paper*, 2014, doi: 10.2139/ssrn.2411672.
[59] F. Farahmand, M. J. Atallah, and E. H. Spafford, "Incentive alignment and risk perception: An information security application," *IEEE Trans. Eng. Manag.*, vol. 60, no. 2, pp. 238–246, May 2013, doi: 10.1109/.TEM.2012.2185801.
[60] F. Farahmand, M. Atallah, and B. Konsynski, "Incentives and perceptions of information security risks," in *Proc. ICIS*, 2008, p. 25.
[61] F. Farahmand, M. Dark, S. Liles, and B. Sorge, "Risk perceptions of information security: A measurement study," in *Proc. Int. Conf. Comput. Sci. Eng.*, 2009, pp. 462–469, doi: 10.1109/CSE.2009.449.
[62] F. Farahmand and E. H. Spafford, "Understanding insiders: An analysis of risk-taking behavior," *Inf. Syst. Frontiers*, vol. 15, no. 1, pp. 5–15, Mar. 2013, doi: 10.1007/s10796-010-9265-x.
[63] R. Skotnes, "Risk perception regarding the safety and security of ICT systems in electric power supply network companies," *Saf. Sci. Monitor*, vol. 19, no. 1, pp. 1–16, 2015.
[64] D.-L. Huang, P.-L.-P. Rau, and G. Salvendy, "Perception of information security," *Behav. Inf. Technol.*, vol. 29, no. 3, pp. 221–232, May 2010, doi: 10.1080/01449290701679361.
[65] N. Kostyuk and C. Wayne, "The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public," *J. Global Secur. Stud.*, vol. 6, no. 2, Mar. 2021, Art. no. ogz077, doi: 10.1093/jogss/ogz077.
[66] H.-S. Rhee, Y. U. Ryu, and C.-T. Kim, "Unrealistic optimism on information security management," *Comput. Secur.*, vol. 31, no. 2, pp. 221–232, Mar. 2012, doi: 10.1016/j.cose.2011.12.001.
[67] D. LeBlanc and R. Biddle, "Risk perception of Internet-related activities," in *Proc. 10th Annu. Int. Conf. Privacy, Secur. Trust*, Jul. 2012, pp. 88–95, doi: 10.1109/PST.2012.6297924.
[68] W. Xu, F. Murphy, X. Xu, and W. Xing, "Dynamic communication and perception of cyber risk: Evidence from big data in media," *Comput. Hum. Behav.*, vol. 122, Sep. 2021, Art. no. 106851, doi: 10.1016/j.chb.2021.106851.
[69] K. Haltinner, D. Sarathchandra, and N. Lichtenberg, "Can i live? College student perceptions of risks, security, and privacy in online spaces," in *Proc. Cyber Secur. Symp.* Cham, Switzerland: Springer, 2015 pp. 69–81, doi: 10.1007/978-3-319-28313-5_6.
[70] H. Cho, J.-S. Lee, and S. Chung, "Optimistic bias about online privacy risks: Testing the moderating effects of perceived controllability and prior experience," *Comput. Hum. Behav.*, vol. 26, no. 5, pp. 987–995, Sep. 2010, doi: 10.1016/j.chb.2010.02.012.
[71] J. Herrero, A. Urueña, A. Torres, and A. Hidalgo, "My computer is infected: The role of users' sensation seeking and domain-specific risk perceptions and risk attitudes on computer harm," *J. Risk Res.*, vol. 20, no. 11, pp. 1466–1479, Nov. 2017, doi: 10.1080/13669877.2016.1153504.
[72] G. de Smidt and W. Botzen, "Perceptions of corporate cyber risks and insurance decision-making," *Geneva Papers Risk Insurance Issues Pract.*, vol. 43, no. 2, pp. 239–274, Apr. 2018, doi: 10.1057/s41288-018-0082-7.
[73] P. van Schaik, K. Renaud, C. Wilson, J. Jansen, and J. Onibokun, "Risk as affect: The affect heuristic in cybersecurity," *Comput. Secur.*, vol. 90, Mar. 2020, Art. no. 101651, doi: 10.1016/j.cose.2019.101651.
[74] L. J. Frewer, C. Howard, and R. Shepherd, "Understanding public attitudes to technology," *J. Risk Res.*, vol. 1, no. 3, pp. 221–235, Jul. 1998, doi: 10.1080/136698798377141.
[75] C. Starr, "Social benefit versus technological risk," *Science*, vol. 165, no. 3899, pp. 1232–1238, Sep. 1969. [Online]. Available: https://www.jstor.org/stable/1727970
[76] D. Kahneman, *Thinking, Fast and Slow*. New York, NY, USA: Macmillan, 2011.
[77] A. S. Alhakami and P. Slovic, "A psychological study of the inverse relationship between perceived risk and perceived benefit," *Risk Anal.*, vol. 14, no. 6, pp. 1085–1096, Dec. 1994, doi: 10.1111/j.1539-6924.1994.tb00080.x.
[78] N. D. Weinstein, "Smokers' unrealistic optimism about their risk," *Tobacco Control*, vol. 14, no. 1, pp. 55–59, Feb. 2005, doi: 10.1136/tc.2004.008375.
[79] *Cybersecurity Culture Guidelines: Behavioral Aspects of Cybersecurity*, ENISA, Athens, Greece, 2019, doi: 10.2824/324042.
[80] M. Grech, T. Horberry, and T. Koester, *Human Factors in the Maritime Domain*. Boca Raton, FL, USA: CRC Press, 2008.

[81] *International Convention for the Safety of Life at Sea (SOLAS)*, IMO, London, U.K., 1974.
[82] *International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW)*, IMO, London, U.K., 1978.
[83] L. Sjöberg, "The different dynamics of personal and general risk," *Risk Manage.*, vol. 5, no. 3, pp. 19–34, Jul. 2003, doi: 10.1057/palgrave.rm.8240154.
[84] P. Harris, "Sufficient grounds for optimism?: The relationship between perceived controllability and optimistic bias," *J. Social Clin. Psychol.*, vol. 15, no. 1, pp. 9–52, Mar. 1996, doi: 10.1521/jscp.1996.15.1.9.
[85] B.-M. Drottz-Sjöberg, "Risk perceptions related to varied frames of reference," in *Proc. SRA Eur. 3rd Conf., Risk Anal., Underlying Rationales*, 1993, pp. 55–69.
[86] SafetyatSea and BIMCO. (2019). *Cyber Security White Paper*. [Online]. Available: https:// cdn.ihsmarkit.com/www/pdf/1019/Safety-at-Sea-and-bimco-cyber-security-white-paper.pdf
[87] L. Sjöberg, "Explaining individual risk perception: The case of nuclear waste," *Risk Manage.*, vol. 6, no. 1, pp. 51–64, 2004, doi: 10.1057/.palgrave.rm.8240172.

MARIE HAUGLI LARSEN was born in Tromsø, Norway, in 1992. She received the B.S. degree in nautical science and the M.S. degree in management of demanding marine operations from the Norwegian University of Science and Technology (NTNU), in Aalesund, Norway, in 2016 and 2019, respectively, where she is currently pursuing the Ph.D. degree in maritime cyber security and human factors. Her research interests include maritime cyber risk perception, risk communication, and human behavior and decision making in operational environments.



MASS SOLDAL LUND was born in Oslo, Norway, in 1977. He received the B.S., M.S., and Ph.D. degrees in computer science from the University of Oslo, Norway, in 2000, 2002, and 2008, respectively. From 2002 to 2013, he was a Research Scientist with SINTEF, a research institute. In 2013, he started as an Associate Professor with the Cyber Academy, Norwegian Defence University College, Lillehammer, and received a Full Professorship, in 2018. Since 2019, he has been an Adjunct Professor at the BI Norwegian Business School. He is the coauthor of the book *Model-Driven Risk Analysis: The CORAS Approach* and more than 30 articles. His research interests include military cyberspace operations, incident response, threat modeling, maritime cyber security, cyber security education, and the history of computing.

Paper 2

A model of factors influencing deck officers' cyber risk perception in offshore operations

Authors: Marie Haugli Larsen, Mass Soldal Lund, and Frøy Birte Bjørneseth

Maritime Transport Research, Volume 3, June 2022, Article Number 100065, DOI: 10.1016/j.martra.2022.100065

Maritime Transport Research 3 (2022) 100065

Contents lists available at ScienceDirect

Maritime Transport Research

journal homepage: www.sciencedirect.com/journal/maritime-transport-research

A model of factors influencing deck officers' cyber risk perception in offshore operations

Marie Haugli Larsen [a,*], Mass Soldal Lund [b], Frøy Birte Bjørneseth [a,c]

[a] Department of Ocean Operations and Civil Engineering, Norwegian University of Science and Technology, Aalesund 6025, Norway
[b] Inland Norway University of Applied Sciences, Rena 2450, Norway
[c] Kongsberg Maritime, Aalesund 6025, Norway

ARTICLE INFO

Keywords:
Maritime cyber security
Risk perception
Human behaviour
Risk communication
Cyber risk management

ABSTRACT

Offshore operations onboard vessels are increasingly reliant on digitalization, integration, automation, and networked-based systems, which creates new dimensions of cyber risks. The causes of cyber incidents often include complex relationships between humans and technology, and in offshore operations, the onboard crew can be both a cyber security risk and a vital resource in strengthening the cyber security. This makes the behaviour of the decisionmakers onboard important in both preventing and handling cyber risks at sea. By use of in-depth interviews and the constant comparative analysis (CCA), this paper investigates factors influencing deck officers' cyber risk perception in offshore operations and presents a contextual model of these factors. The model indicates that deck officers' cyber risk perception can be affected by a feeling of distance towards cyber risks, being more restricted in their working environment because of digitalization, and trust in their reliable cyber-physical systems and suppliers. Further, targeted cyber risk mitigation measures should be implemented on multiple levels in shipping companies. The measures may benefit from focusing on increased risk communication, operational training, awareness campaigns, vessel-specific procedures, and policies, in addition to increased communication from management regarding the demand for digitalization. With this approach, the contextual model can contribute to the ongoing work of developing targeted measures for cyber risk mitigation in the maritime domain and can be used as a point of departure for further studies to discover additional nuances and factors within cyber risk perception in this domain.

1. Introduction

Offshore operations on ships depend on digitalization and automation processes, and the cyber-physical systems are more interconnected than before (Ben Farah et al., 2022). This makes the onboard systems interact in complex ways, making it difficult to defend the maritime transportation system against cyber-attack vectors (Hemminghaus et al., 2021; Kessler and Shepard, 2022). A growing concern is the security in offshore vessels operational technology (OT), which relies on industrial control systems (ICS) that manage real-time operational environments (Progoulakis et al., 2021). Cyber-attacks towards these systems can put both humans, the environment, and physical assets at risk (Alcaide and Llave, 2020).

During and after the covid-19 pandemic of 2020–2022 there has been a significant increase in cyber risks towards maritime

* Corresponding author.
E-mail address: marie.h.larsen@ntnu.no (M.H. Larsen).

https://doi.org/10.1016/j.martra.2022.100065
Received 31 March 2022; Received in revised form 24 May 2022; Accepted 6 June 2022
Available online 14 June 2022

industry (Meland et al., 2021). When cyber incidents occur and technology fails, the human operator is the first line defence against cyber risks (Akpan et al., 2022; Erstad et al., 2021). In these situations, the maritime crew can be both a vital resource and a risk, which makes the behaviour of the decision makers in maritime operations important in both preventing and handling cyber risks at sea (Larsen and Lund, 2021). Onboard offshore vessels the decision makers are usually the captain or the deck officers on watch. Further, to facilitate good security behaviour and develop targeted risk mitigation measures, there is a need for understanding the deck officers' cyber risk perception. Individual behaviour and acceptance of specific technology is influenced by risk perception, and improving our understanding of factors influencing this process, can improve our capabilities for risk communication, decision support and management (Siegrist and Árvai, 2020).

One way of elucidating human experience is to describe ongoing processes in real life through use of qualitative research methods (Kvale and Brinkmann, 2015). This study is using constant comparative analysis (CCA) to investigate maritime cyber risk perception, and the aim is to develop a contextual model of factors influencing deck officers' perception of cyber risks in offshore operations. The purpose is to provide descriptions of experiences and reflections which may lead to transferability beyond the presented context (Malterud, 2017; Postholm, 2006), and to aid the ongoing work of developing targeted tools for cyber risk mitigation in the maritime domain. To achieve this, the qualitative study aims to investigate what factors can influence deck officers' perception of cyber risks in offshore operations, and how these factors can be described. Further, the results are presented as a contextual model of these influencing factors, with descriptive categories and sub-categories. The work presented in this paper makes it possible to consider the particularities within the maritime domain while investigating the human side of maritime cyber security, and in this way, contributes to the body of knowledge within human behaviour and maritime cyber security (Larsen and Lund, 2021; Pseftelis and Chondrokoukis, 2021).

The paper is further structured as follows: The first section presents the maritime context and the psychology approach within risk perception research. Section two describes method and analysis, while section three outline the results of the study. Section four provides the discussion, ethical considerations, methodological implications, and limitations. Section 5 concludes the research and gives suggestions for future research.

1.1. The maritime context

The research field of maritime cyber security has increased over the last decade, and there is a growing interest and acknowledgement of the importance of implementing cyber risk mitigation measures within shipping companies (FuturenauticsMaritime et al., KVH 2018; Garcia-Perez et al., 2017). This can partly be because of the implementation of maritime cyber risk management by the International Maritime Organization (IMO, 2017; Karamperidis et al., 2021), but also because of the excessively increase in cyber-attacks in the maritime industry the last couple of years (Meland et al., 2021). Combined with the increase in connectivity, the potential cyber-attacks create a whole new dimension of risks towards vessels of today (Larsen and Lund, 2021). These cyber risks can be caused by a threat that exploits cyberspace, e.g., computer systems, information in storage or transit, or services (Refsdal et al., 2015).

Cyber security can be understood 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" (Von Solms and Van Niekerk, 2013). This makes the users, or human operators, important to consider when implementing proper cyber risk mitigation measures. In a maritime context it is vital to understand human behaviour, since the crew is "at the sharp edge in a potential maritime cyber emergency" (Erstad et al., 2021, p. 33). As stated earlier, one important aspect is to understand how the decision makers onboard vessels is perceiving cyber risks (Bada and Nurse, 2020; Larsen and Lund, 2021).

1.2. Risk perception research within the psychology approach

People have subjective judgements about characteristics and severity of risks, and research on risk perceptions is necessary for a deeper understanding of risk exposure, risk communication and risk management (Siegrist and Árvai, 2020, p. 2191). Further, risk perception is an important factor in investigating and understanding people's reactions to various technological risks, and risk perception processes are believed to be driving decision making at various levels in society (Larsen and Lund, 2021; Sjöberg, 2004).

Models of risk perception are emerging from research fields like cognitive science, psychology, sociology, engineering, and culture studies. However, risk perception can be seen as one of the most complex processes that happens in our brain, and there exists no theory or model with the capacity to put together all the factors that influence risk perception (Spencer, 2016). The psychological approach is trying to explain how people reconstruct previously assimilated risk through a subjective judgement, where the psychometric paradigm and research on heuristics and biases are well recognized fields of research (Kahneman, 2011; Siegrist and Árvai, 2020; Slovic, 1990; Weinstein et al., 2005).

1.2.1. The psychometric paradigm

The psychometric paradigm is an acknowledged model within the field of risk perception research (Slovic, 1990; Spencer, 2016), and was first published in a paper by Fischoff et al. in 1978. The original model describes nine dimensions of risk perception, and is based on explanatory scales such as New-Old, Voluntary-Unvoluntary, etc. The nine dimensions, with an interpretation of their application to cyber risks (Larsen and Lund, 2021), are presented in Table 1. The technique is used to create quantitative representations, "cognitive maps", of people's risk attitudes and perceptions, where the goal is to understand and predict risk responses

(Fischhoff et al., 1978; Slovic, 1987). This approach of studying risk perception is widely used across different domains, despite the criticism about the use of aggregated data to give the dimensions a stronger correlation (Gabriel and Nyshadham, 2008; Siegrist and Árvai, 2020; Siegrist et al., 2005; Sjöberg, 2012).

1.2.2. Heuristics and biases

Both the psychometric dimensions and heuristics may influence certain biases in risk perception. Kahneman and Tversky's work on how people use heuristics to evaluate information, has played an important role in the discussion of risk perception (Kahneman et al., 1982; Tversky and Kahneman, 1973). One frequently used heuristic in the risk domain is the availability heuristic (Siegrist and Árvai, 2020). When relying on this heuristic, people use the "ease with which instances or occurrences can be brought to mind" to consider the frequency or probability of an incident (Tversky and Kahneman, 1974, p. 1127). The heuristics can be useful shortcuts for thinking, but can also lead to inaccurate judgements or biases in some situations (Kahneman, 2011; Spencer, 2016). A well-documented and recognized bias that can be generated through use of cognitive heuristics, is the optimistic bias (Campbell et al., 2007; Weinstein, 1980). This bias demonstrates a systematic discrepancy between people's risk perceptions and their actual risk for experiencing positive or negative events (Roeser, 2012; Weinstein and Klein, 1996).

2. Method

A qualitative approach with use of constant comparative analysis (CCA) was selected. This method is suited for research in areas where theories are unavailable, or not able to explain the research problem (Corbin and Strauss, 2015; J.W. Creswell and Poth, 2018), which is the case with the little studied field of cyber risk perception in the maritime domain (Larsen and Lund, 2021). As stated earlier, the goal is to create a contextual model with descriptions of factors influencing deck officers' perception of cyber risks. Grounded in data collected from participants experiences, an iterative process was used for development of the categories within the model (Corbin and Strauss, 2015).

2.1. Participants and data collection

To ensure contribution to the development of thick descriptions and contextual model, the participants was purposefully sampled (J.W. Creswell and Poth, 2018). The development of a contextual model in qualitative studies rely on thick descriptions of human behaviour and experiences in a given context (Kvale and Brinkmann, 2015). Thick descriptions are used to pay attention to contextual details in observing and interpreting social meaning in qualitative studies (Mills et al., 2010). Inclusion criteria were deck officers working offshore with some operational experience. Further, the criteria for sampling size in CCA is saturation, which means that the data should be gathered until "no new concepts are emerging" (Corbin and Strauss, 2015, p. 134). This study was completed with 9 deck officers, and within this sampling, saturation was pursued. All the interviewees were working offshore and had between 5 and 25 years of operational experience.

Data was collected by in-depth interviews with the participants. The semi-structured interviews were guided by an interview guide consisting of questions and themes to get the conversation going (Kvale and Brinkmann, 2015). The interview questions were categorized in seven themes regarding perception of cyber risks and cyber security at the participants workplace. Table 2 gives an overview of the themes and questions used in the conversations.

The duration of the interviews were 30–90 min, and the conversations were sufficiently unstructured to allow the discovery of new themes and ideas (Corbin and Strauss, 2015). During the interviews there was an emphasis on validating the understanding of the participants statements by asking follow-up questions and doing a summary in the end of each interview. The interviews were conducted and transcribed in Norwegian.

Table 1
The nine dimensions in the psychometric paradigm related to cyber risks (Fischhoff et al., 1978; Larsen and Lund, 2021).

Voluntariness	To what extent people perceive exposure to a cyber risk as voluntary affect how risky people perceive the related activity to be.
Immediacy of risk consequences	The greater the perceived immediacy of cyber risks are, the higher the perceived risk seems to be.
Knowledge to exposed	When people have knowledge of, and are familiar with the cyber risk in question, they perceive the risk as lower than if they have limited knowledge.
Knowledge to science/ experts	Peoples level of perceived risk is affected by to what extent they believe the cyber risks are known to experts or science.
Controllability	Risk perception levels can be reduced if people believe they can control the cyber risks and avoid them from happening.
Catastrophic potential	Cyber risks with a larger impact on a single occasion (catastrophic risk) are perceived riskier than cyber risks with less impact (chronic risk).
Dread vs. common	Measures whether the cyber risk in question is something people have learned to live with, or whether it is a risk they have great dread for.
Newness	New or novel cyber risks tend to be perceived as riskier and less controllable than familiar risks.
Severity of consequences	When cyber risks are perceived to have more severe consequences, they are perceived to be riskier.

Table 2
Semi-structured interview guide.

Theme	Interview questions
Onboard systems and vessel operations	What kind of operations do you normally perform on your vessel?
	Have you gotten any new systems onboard lately?
	Do you feel that you understand the systems you use in daily operations?
	Do you feel confident in the use of these systems?
Cyber risk	What are you thinking about when I say cyber risks at sea?
Experience with cyber incidents	Can you tell me about a cyber incident you have experienced at work?
	Do you have any thoughts on what a cyber incident on your vessel might be?
	Have you heard about other vessels experiencing a cyber threat?
Procedures and training	In what way do you work with cyber security on board your vessel?
	What actions should be taken if a cyber incident occurs?
	How do you think other vessels and shipping companies work with cyber security?
Crew/organisation/shipping company	Do you find that your crew are concerned about how the onboard systems can be prone to cyber risks?
	How does the shipping company communicate with you about cyber security and potential cyber risks?
Cyber risk in operation	How do you experience the risk of a cyber incident occurring during an operation?
	Do you have any thoughts about what may affect your perception of cyber risks at work?
Connectivity onboard	In what way can you use your own devices onboard?
	Is the shipping company concerned about what is important for the crew in regards of access to the internet?
	Do you think there are any challenges associated with using your own devices on board?

2.2. Analytic approach

"The purpose of analysis is to reduce the amount of data a researcher has to work with by delineating concepts to stand for data" (Corbin and Strauss, 2015, pp. 75–76). To achieve this in the constant comparison analysis (CCA) method, conceptual headings are used to group incidents sharing some common characteristics. Important features to remember is that concepts vary in levels of abstraction, where basic-level concepts provide a foundation, and higher level, more abstract concepts provide the structure of a model (Corbin and Strauss, 2015).

In accordance with CCA, to reveal concepts in the transcriptions, the data material was analysed by asking questions about "what is really going on here?". A coding process was carried out by analysing sentences throughout the transcriptions and labelling them with terms describing their contents (Postholm, 2019). This coding was developed further into categories and guided the classification of emerging main categories and sub-categories. In this stage the raw material was sorted, and it became easier to see patterns.

The emerged categories appeared as basic-level concepts when the coding process was concluded, meaning the analysis had discovered more sub-categories than main categories. Hence, it was necessary to lift these concepts into a higher level to develop the contextual model. This was done by reanalysing the sub-categories and cluster them together. Table 3 shows one example of how multiple sub-categories were translated into a main category. The coding process was conducted with Norwegian terms first, and when the categories emerged, they were given a suitable English translation.

To help with development of the contextual descriptions, memos were written and attached to the categories (Corbin and Strauss, 2015). This helped with analysing the participants statements, and the reflections was helpful in development of the descriptions. In this process, a "bottom up" approach was initiated, trying carefully to consider the participants' meaning in their utterances, and how to frame the quotes (Kara, 2015; Kvale and Brinkmann, 2015). Four main categories emerged from the data material after the analysis, and together with the sub-categories, they form the foundation for the contextual model presented in the next section.

3. Results

Emerging from the analysis, Fig. 1 presents a contextual model of factors influencing deck officers cyber risk perception in offshore operations. The categories within the model reflect the participants utterances together with the interpretation of what is affecting their cyber risk perception. The model indicates that deck officers' cyber risk perception can be affected by a feeling of distance towards cyber risks, being more restricted in their working environment because of digitalization, and trust in their reliable cyber-physical systems and suppliers.

Table 3
Translation from sub-categories to main category.

Sub-categories	Main category
Limited cyber security training	Trust in others for cyberdefence
Knowledge of maritime cyber security	
Communication of cyber risks	
Trust in suppliers	

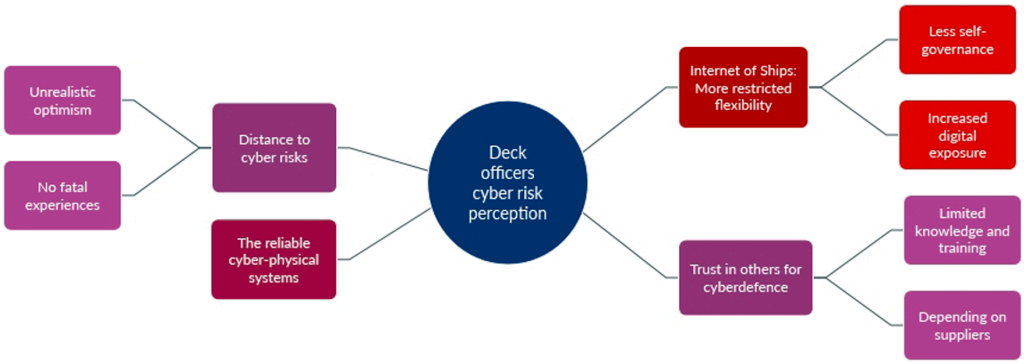


Fig. 1. Contextual model of factors influencing deck officers cyber risk perception.

3.1. Distance to cyber risks

Findings from the interviews show that the deck officers believe they are not exposed to cyber risks at work. This can be related to no fatal experiences with cyber incidents, or it may be a result of having unrealistic optimism regarding their exposure to these risks. All participants described it as a feeling of being at a secure distance to cyber risks.

3.1.1. No fatal experiences

The interviewees describe their experiences with cyber incidents, related to IT-systems or loss of GPS-signals. All nine participants had experienced a cyber incident, but according to themselves, no incidents with fatal or serious consequences. They thought worst case scenarios have low, or no, risk of happening. Table 4 is highlighting the cyber incidents the participants have experience with, together with their reflections concerning risk and consequence. An emerging trend is that frequent cyber incidents are perceived to have few consequences, while cyber incidents with severe consequences are unlikely, or have very low risk of happening.

3.1.2. Unrealistic optimism

The participants believe the cyber risk is low towards the vessels they are sailing with. The main arguments for this were the geographical area their vessels are operating in, that vital systems are not connected to the internet, and that the officers feel it is difficult to understand that anyone would be interested in attacking their ship. As one of the deck officers uttered:

Table 4
Experienced and reflected upon cyber incidents.

#	Cyber incident	Cause	Consequence	Respondents' reflections
2	Infection from USB-stick.	Human error.	Virus on onboard ECDIS.	High risk of happening, but no serious consequence.
4	Jamming of GPS-signals.	Military activity or unknown.	Loss of GPS-signal.	High risk of happening, no serious consequence, but "annoying" in operations.
1	Hardware failure in switch between DP-system and ECDIS causing denial of service.	Two broken switches.	Blackout on bridge.	Serious consequence, but not perceived as a cyber incident. Described as a "digital incident".
9	Fake e-mails.	Spam or social engineering.	No consequences.	Happens all the time.
1	Hardware failure.	Unknown.	System failure on onboard steering machine.	Serious consequences, but difficult to handle when you don't know the cause.
3	Loss of signal to onboard server.	Unknown.	Unstable internet or loss of access to onshore server.	High risk of happening, but no impact on the operational activities. Affects the ability to do paperwork and external communication.
3	Cyber incident waiting to happen during operation.	No assessment of cyber risks in planning of complex offshore operations.	Unprepared for cyber incidents during operations.	Lack of awareness and training make the crew unprepared to handle a cyber incident.
4	Imagined worst case scenarios, such as: hacked control systems or onboard units controlling pumps/valves, theft of personal information.	Cyber-attacks towards onboard IT- or OT-systems.	Loss of; control over vessel, personal information, position. Oil spill, financial loss and environmental damage.	Worst case scenarios are described as something not worth considering and very low risk of happening.

[#] Number of respondents.

"I have assessed the cyber risk to be low at the vessels I have sailed on. The activity is lower in the North Sea comparted to further down the continent, and we think cyber incidents is something that happens in the Gulf of Aden or around the Cape of Good Hope."

Further, it seems that their lack of experience with serious cyber risks makes it difficult to understand the possible motives for attacking vessels. Six of the interviewed officers said that they are not able to imagine the benefits of cyber-attacks towards vessels, and that their vessels are not interesting targets.

"How interesting can it be for someone to hack into that specific vessel, and why bother to attack the computer system on a vessel? It's like, you don't think that someone will steal from your house either. Maybe we are a bit naïve in our thinking. We cannot quite imagine what they want with the DP-system on a supply vessel."

3.2. The reliable cyber-physical systems

When dealing with cyber risks towards vessels, the participants described a difference between the onboard operational technology systems (OT-systems) and information technology systems (IT-systems). A clear trend was the impression of IT-systems as more prone to attacks than OT-systems.

"The focus has been on attacks against IT-systems, and these systems are unbelievably more innocent versus an operational system. If there is an attack on the IT-system, it will not have any direct impact on the operation, other than that we have to handle the documentation in a slightly different way."

This notion seems substantiated by the impression of OT-systems as safe because they are not necessarily online. This was an important aspect for all the officers, and several of them highlighted the importance of keeping the cyber-physical systems offline.

"The simplest form for risk management would be to say that none of our operational systems should be connected to the internet or connected to the possibility of external communication in operations."

When talking about how important OT-systems are for the vessels operations, all the participants were very clear about having enough understanding to operate these systems in a safe manner. Most of them seemed more comfortable with the operational technology than the IT-systems.

"I feel that I understand the systems I need for my daily work to keep the vessel and crew safe. It is all the other stuff that is only to satisfy the bureaucratic red tape our organization must use to get a job."

Even if the officers feel like they have control over the OT-systems, they also expressed a growing concern about the increase in online systems due to connectivity. This is further addressed in the next category.

3.3. Internet of ships: more restricted flexibility

In the last 20 years there has been a comprehensive digitalization in the offshore industry, and the deck officers feel this have changed their working environment and their relationship with the shipping office. It seems like they are experiencing an increased digital exposure and less self-governance at work.

3.3.1. Increased digital exposure

Digitalization is changing the working environment, and all the interviewees believe connectivity is making it difficult to know the status of their systems. Multiple of the officers expressed insecurity concerning how the onboard equipment are interconnected, and whether the different systems are exposed to cyber risks or not.

"In the past, cyber risk was a non-problem because the equipment was not connected to the internet. Amongst other things, we now run monitoring on machinery and remote logging on the DP-system. Everything is online and streamed in some form of Big Data."

In addition, the participants experience that some of the new systems installed onboard are insufficiently developed. As an example, statistics presented from the monitoring systems are not reflecting the dynamic work environment offshore. Consequently, the officers are questioned by management about their fuel consumption when performing operations.

"The digital world is not ideal, and there are some challenges. For example, that the tonnes of fuel we use vary with temperatures, and the system does not take this into account at all. Then the questions from management and customers come concerning why we have used so much fuel. Previously, this was not an issue. Now everything should be presented as statistics and referred to."

In addition, the officers believed the digitalization is creating more work for them in many situations, and especially when it comes to documentation. More than half of the interviewees told they must report the same information in more than three different places. This is mostly due to stakeholders having custom made systems, and that management does not get rid of the old ways of documenting when implementing new ones.

"I feel like the digitalization is creating more work, and I think many people in my situation also feel that. If they only had removed some of the old ways of documenting. For example, if we load and unload bulk, it is completely hopeless. It must be written in the bulk log, the

captain's log, on the whiteboard, in an excel sheet and in the loading program. It should be enough to write it down a couple of places and not five as it is now."

3.3.2. Less self-governance

The increased digital exposure at work has made it possible for the shipping company to follow the vessels operations closely, and the officers implied that this gives them less independence in their everyday working life. One captain explained how monitoring of the vessel's systems and performance affects the crew's ability to handle situations by themselves:

"I have a feeling that they really don't trust us, and that we somehow are deprived of decisions that we previously could just make on our own. Now there is this guardianship that is watching over us. However, in many situations, we need to think quickly and just get it done. So everyday work is now more and more computerized and monitored."

Further, the officers emphasized how the feeling of surveillance is affecting their mindset offshore, and how the monitoring generates conflicts between the shipping office and the vessels. One of several examples is that all the interviewees described how the intention of fuel-saving is creating challenges in their relationship with the shipping office and the other shift on their vessel.

"You feel like you have two eyes over your shoulder all the time. I think the intention is to handle it on an administrative level where you look at the vessels, not the captains. But of course, when they can log your fuel consumption and compare how much fuel you use in relation to the captain at home, then it can be a non-healthy competition."

It also seems like the feeling of being important for their employer may be impaired. More than half of the participants felt like they are just red numbers on a spreadsheet, and that management does not work in their favour. Another aspect described, is the belief that management wants to cut operational staff as much as they can because of increased automation.

"They don't give a damn. They see some red lines and some red numbers. I especially notice it with the shipping company I work for now. They are difficult. The crew on board are just some red numbers, that's how we experience it."

3.4. Trust in others for cyber defence

According to the participants, deck officers are operators and not technicians. They are educated in the operation of the vessels' systems, not defending them against cyber risks. The officers described how they have limited training and knowledge about cyber security, and how they are dependent on suppliers for the security of the vessels systems.

3.4.1. Limited knowledge and training

All the interviewed deck officers emphasised having limited knowledge and training in cyber security. Three of the interviewees said they have received policies and procedures, but none of the officers had experience with training on cyber security scenarios. Two participants have conducted tabletop exercises, but without really knowing what to discuss. Most of them don't believe they are able to handle cyber incidents.

"We get more equipment online, but I am not sure how to handle it, because we need IT-knowledge that navigators don't have. Is the system online so it can be hacked? What can we do to regain control? We have no idea about these things today."

Because of increased information from the shipping office, the officers believed they are more aware of cyber security issues now than before. They get more information on email, and everyone has completed an online course in information security. But the officers do not think these courses add any value, mainly because they focus on the information and communication systems and do not address operational systems or aspects.

"We never think that we can be hacked, jammed or that systems can be taken over. There is always talk about physical attacks such as bomb threats or stowaways. There should be more lifelong learning about privacy and security, not just an online course you sneak through in an afternoon. Just answer some questions and you're done."

Three of the participants described a difference between their own cyber security knowledge and the expectations from the IT-department. It seems like they experience a discrepancy between implementation of new technological solutions and onboard training. Multiple officers also experienced it difficult to communicate with their IT-departments.

"Those who impose these solutions on us, they do not follow up with training. They probably have a bachelor's degree and more within IT. We who went to vocational school did not get that, to put it mildly."

3.4.2. Depending on suppliers

Because of the deck officers' role as navigators and operators, the participants were clear on their dependence on technical support from suppliers if there is a problem with onboard systems. This seems to be a well-established way of solving problems, and the officers described this as a satisfactory arrangement.

"We have technical support from suppliers on all our systems. Officially we should go via the shipping office, but we have such a low doorstep that we can contact the suppliers directly. We can get help from them with everything from the cranes to the DP-system."

Even so, the participants had a notion that the shipping companies rely too much on their suppliers, as they often are responsible for both installation and maintenance of the onboard systems. The officers experienced that the suppliers are expected to have control over both the communication between the systems and the overall security.

> *"You could say that bringing the chart machines online was crazy, but we trusted that the supplier was taking care of our security. At the same time, we were also guaranteed by a supplier that connecting the DP-system and the bridge systems was safe. But then there was a blackout, and a service technician found an incorrect programming. Then I thought this could happen anywhere."*

4. Discussion

To handle the increase in cyber risks and attack vectors towards the maritime transportation system, there is a need for understanding cyber security on the premise of the humans operating in the maritime domain (Larsen and Lund, 2021, p. 144,902). Fig. 1 gives an indication of factors that can influence deck officers' perception of cyber risks, and this model can be used as a starting point for improving risk communication, decision support, training, and management within maritime cyber security.

Previous research shows that people display optimistic bias in relation to cyber risks (Campbell et al., 2007; Haltinner et al., 2015), and the feeling of distance to cyber risks gives an impression of a discrepancy between the deck officers risk perception and the possible risk for experiencing a cyber incident (Weinstein et al., 2005). The lack of experience with fatal cyber incidents can also be linked to the availability heuristic, since there seems be a difference between the subjective risk perception and the objective number of cyber incidents associated with the specific threat (Siegrist and Árvai, 2020; Tversky and Kahneman, 1973). Because of this discrepancy, and the increase in cyber risks towards the maritime domain (Meland et al., 2021), it can call for more targeted policies for risk communication to emphasize how the onboard technology can affect the crew's security and safety (de la Peña Zarzuelo, 2021).

However, it is important to bear in mind the fact that people can feel less motivated to pay attention to risk communication or to take action to mitigate risk if they don't feel at risk (Rhee et al., 2012; Siegrist and Árvai, 2020). It is important to consider what kind of cyber risk the communication and policies are targeting, since research shows that whether the risk in question is considered a personal or a general risk, can affect the demand for risk mitigation (Sjöberg, 2003). The difference in personal and general risks coincides with the notion that people's judgement of demand for risk mitigation are mostly related to consequences and not to probabilities, and that people often judge personal risks as smaller than general risks (Roeser, 2012; Slovic, 1987). If the deck officers have difficulties seeing cyber risks as a source of harm, or having catastrophic potential, they may ignore the probability of a cyber incident occurring (Van Schaik et al., 2020). This can be substantiated with the statement that "security risks are harder to evaluate and more intractable than physical risks due to a general lack of metrics, awareness of security incidents, and inherent haptic feedback" (Garg and Camp, 2012, p. 3278).

An influencing factor in optimistic bias is the feeling of having control over threats and be able to prevent them from happening (Harris, 1996; Larsen and Lund, 2021). When the OT-systems onboard vessels are perceived as reliable, and the deck officers feel they understand and can operate the technology in a safe manner, it can enhance the feeling of controllability (Gabriel and Nyshadham, 2008; Garg and Camp, 2015). To further substantiate this feeling, statistics show that the most frequent types of cyber incidents are happening towards shipping companies IT-systems, and there are less known cyber incidents where OT-systems have been affected (Meland et al., 2021). This makes the notion about IT-systems as more prone to cyber-attacks understandable. Even so, cyber incidents towards maritime OT-systems can have critical consequences, for both human safety, environmental aspects, and physical assets (McGillivary, 2018; Progoulakis et al., 2021). Because of this, the humans operating in the maritime domain should be prepared to deal with more severe cyber incidents. This can be done by providing the deck officers with domain-specific knowledge about cyber risks, and training in how to handle operational cyber incidents with potential severe consequences. One way of providing cyber security training is by use of maritime simulators, which can provide the deck officers with an arena to learn needed skills in a risk-free environment (Kim et al., 2021).

The difference in cyber risk perception towards IT- and OT-systems can also be linked to the negative experiences with use of IT-systems. Often, digitalization creates more administrative work, and less flexibility, for the deck officers. This coincides with the conception that society may accept higher levels of risk with more beneficial activities, and tolerate higher risk levels for voluntary activities (Fischhoff et al., 1978; Van Schaik et al., 2017). Previous research shows that people tend to see high benefit of using information technology in general (Frewer et al., 1998; Larsen and Lund, 2021), but in this context, it seems to be the opposite for the deck officers. They perceive parts of the digitalization measures implemented by the shipping companies in a negative way, and this can affect their perception of the benefits with the IT-systems used to enforce these measures. In addition, the experience of less self-governance can further reinforce this perception. Management should consider measures to improve the understanding of the underlying need for digitalization, together with more involvement of the maritime crew in decision making processes affecting their working life. Such measures should be implemented by a top-down approach, since management is vital in communicating the organization's need for technological development and holistic cyber security thinking (Parkin et al., 2021; Withman, 2019).

As discussed earlier, the risk mitigation measures should benefit from a focus on increasing deck officers' knowledge about maritime cyber security. The level of knowledge about the risks they are exposed to, affect their level of risk perception (Kostyuk and Wayne, 2021; Skotnes, 2015). Since the deck officers experience a lack of knowledge and limited training in cyber security, they should, according to previous research, perceive the risks of being exposed to cyber risks as high (De Smidt and Botzen, 2018; Larsen and Lund, 2021). However, it seems other factors, like the availability heuristic and optimistic bias, make the outcome inverse. Another factor enhancing this notion, might be the dependence on suppliers for overall security of onboard systems. The deck officers perception of cyber risks might be reduced if they believe the risks are known by their suppliers (Garg et al., 2014; Slovic, 1990). This

can be substantiated by research showing the importance of having trust in management, information providers and suppliers if people don't have sufficient knowledge about the risks in question (Siegrist et al., 2000; Sjöberg, 2012). Thus, how trust affects cyber risk perception in the maritime domain, might be an important aspect for further research. This is also interesting because it seems there is a difference in trust towards management in shipping companies and the trust deck officers display towards their suppliers of technology. Measures for increasing domain-specific knowledge and generating trust between management and offshore workers can target the experience of less self-governance and dependence on suppliers.

The model of factors influencing deck officers cyber risk perception provides a guide for the ongoing work of developing targeted tools for cyber risk mitigation in the maritime domain. By explicating the categories within the model, it seems like shipping companies may benefit from implementing measures on different levels within their organization. Table 5 summarizes parts of the discussion and gives an overview of suggested mitigation measures based on the targeted categories within the model, together with suggested implementation level in shipping companies. We believe these measures will enable the decision makers in offshore operations to prevent and handle future cyber incidents, and in this way, reduce cyber-attack vectors and increase safety within the maritime transportation system. By use of the contextual model and the suggested mitigation measures in Table 5, offshore shipping companies can start developing company-specific measures to improve their cyber security on different levels in their organization. Even so, one important aspect to remember is that maritime companies are diverse, and each company should perform their own cyber risk assessments to establish the need for protection against cyber risks (Ben Farah et al., 2022; Kessler and Shepard, 2022). However, further validation of the suggested measures is necessary, to explore in what extent they contribute to enhanced maritime cyber risk perception and facilitate good security behaviour.

4.1. Ethical considerations, methodological implications, and limitations

To be an ethical researcher, Kara (2015) emphasizes the importance of thinking ethically in all phases of research projects. Within this project, ethical considerations were made before, and during, all phases of the research. In the planning phase, the study was reported to, and approved by, the Norwegian centre for research data (NSD). In this phase the whole study was carefully planned, and decisions regarding analysis method, sampling, information sheet to participants, written consent, and interview guide were made.

"Researchers should take strategic action during the course of the research to ensure a research's validity and reliability" (Corbin and Strauss, 2015, p. 343). In this study, the perspectives provided by Cresewell and Poth (J.W. 2018) and by Corbin and Strauss (2015) are partially adopted. The strategies within the researcher's lens and the participant's lens have been used to guide the validation process. This includes "clarifying researcher bias or engaging in reflexivity" and "member checking" (J.W. Creswell and Poth, 2018, p. 261). To address reliability, good-quality recording devices have been used, the data material was transcribed by the researchers themselves, and research transparency in the method section was pursued.

A limitation in this study can be the small and homogenous sample (nine deck officers working offshore), which affect the development of the categories within the contextual model. One example of this can be the experience of optimistic bias related to the geographical area the interviewed officers worked in. If the interviewees worked in other areas, like the Gulf of Aden or around the Cape of Good Hope, it is reasonable to believe they would express themselves differently. But rather than representing a population, CCA is concept driven and seeks to investigate categories in depth (Corbin and Strauss, 2015). Thus, using CCA allowed for the in-depth analysis of the subjective perception of maritime cyber risks, focusing on the deck officers' experience in a specific context. Even so, there might be other factors relevant to explain cyber risk perception which this study did not reveal, and the model presented in this paper is not exhaustive.

The qualitative study presented in this paper investigates deck officers' perception of cyber risks in offshore operations, with the underlying theoretical epistemology that risk in essence is subjective and that notions of risk are therefore relative (Renn, 2004; Roeser, 2012; Slovic, 1987). Even so, with the increasing focus on risk management and the reliance on technology and human decision-making systems to predict the future, there is a significant debate about the concept of risk (Manuel and Ghana, 2017, p. 22). Some scholars argue for the positivistic belief that risk is objective, determinable and quantifiable (Renn, 1992). This notion leads to the discussion about real risk versus perceived risk (Spencer, 2016), which is not within the scope of this paper. However, the concept of risk is an important aspect of how risk management processes are understood and implemented to handle the future.

5. Conclusion

Understanding factors influencing the perception of specific risks is important in the work of developing targeted measures for cyber risk mitigation. In this paper a contextual model of deck officers cyber risk perception is presented and discussed, with the purpose of giving recommendations on implementation of such mitigation measures. The categories indicate that there are several possible explanations and relations between the different factors, which also coincides with the complex nature of peoples' perception of cyber risks in different contexts (Larsen and Lund, 2021). This model can be used as a point of departure for further studies to discover additional nuances and factors affecting decision makers cyber risk perception in the maritime domain. And while generalization of findings is not a goal in qualitative research, taking a quantitative approach to explore the factor relationship between the categories in the contextual model, could contribute to a wider understanding of the topic. Further investigations on how to operationalize maritime cyber risks for training on severe cyber incidents could be beneficial, and to consider how use of maritime simulators can enhance the cyber security training of decisionmakers in offshore operations. Regardless, we encourage future work to consider the human aspect of maritime cyber security, to enable decision makers to deal with the potential severe cyber incidents within the maritime transportation system.

Table 5
Targeted cyber risk mitigation measures on different levels in shipping companies.

Implementation level	Cyber risk mitigation measures	Targeted categories in the contextual model
Individual	Targeted risk communication with regards to personal/general cyber risk.	Distance to cyber risks.
(Deck officer)	Increase domain-specific knowledge about cyber security.	The reliable cyber-physical systems.
	More extensive cyber security course/training.	Trust in others for cyber-defence.
	Operational training in simulators.	
Vessel	Operational training on cyber incidents with severe consequences.	Trust in others for cyber-defence.
(Crew)	Onboard awareness campaigns with examples of cyber incidents.	The reliable cyber-physical systems.
	Vessel-specific policies and procedures for cyber security.	
Shipping company	Communication of need for digitalization and new IT-systems.	Internet of Ships: More restricted flexibility.
(Management)	Involvement of maritime crew in decision making on a higher level.	
	Increase trust between vessel and shipping company.	
	High-level company procedures for cyber security.	
	Increase risk communication in all levels of the organization.	

Declaration of Interests

None.

Acknowledgements and Funding

This work was supported by the Grant from the Research Based Innovation Centre "SFI Marine Operation in Virtual Environment (SFI-MOVE)" by the Norwegian Research Council under Project 237929.

References

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., Michaloliakos, M., 2022. Cybersecurity challenges in the maritime sector. Network 2 (1), 123–138. https://doi.org/10.3390/network2010009.
Alcaide, J.I., Llave, R.G., 2020. Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia 45, 547–554. https://doi.org/10.1016/j.trpro.2020.03.058.
Bada, M., Nurse, J.R., 2020. The social and psychological impact of cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press, pp. 73–92. https://doi.org/10.1016/B978-0-12-816203-3.00004-6.
Ben Farah, M.A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., Bellekens, X, 2022. Cyber security in the maritime industry: a systematic survey of recent advances and future trends. Information 13 (1), 22. https://doi.org/10.3390/info13010022.
Campbell, J., Greenauer, N., Macaluso, K., End, C., 2007. Unrealistic optimism in internet events. Comput. Human Behav. 23 (3), 1273–1284. https://doi.org/10.1016/j.chb.2004.12.005.
Corbin, J., Strauss, A., 2015. Basics of Qualitative Research - Techniques and Procedures for Developing Grounded Theory, 4 ed. SAGE Publications, Inc.
Creswell, J.W., Poth, C.N., 2018. Qualitative Inquiry and Research Design - Choosing Among Five Approaches, 4 ed. SAGE Publications, Inc.
de la Peña Zarzuelo, I., 2021. Cybersecurity in ports and maritime industry: reasons for raising awareness on this issue. Transp. Policy. 100, 1–4. https://doi.org/10.1016/j.tranpol.2020.10.001.
De Smidt, G., Botzen, W., 2018. Perceptions of corporate cyber risks and insurance decision-making. The Geneva Papers on Risk and Insurance-Issues and Practice 43 (2), 239–274. https://doi.org/10.1057/s41288-018-0082-7.
Erstad, E., Ostnes, R., Lund, M.S., 2021. An Operational Approach to Maritime Cyber Resilience. TransNav 15, 27–34. https://doi.org/10.12716/1001.15.01.01.
Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S., Combs, B., 1978. How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy Sci. 9 (2), 127–152. https://doi.org/10.1007/BF00143739.
Frewer, L.J., Howard, C., Shepherd, R., 1998. Understanding public attitudes to technology. J. Risk Res. 1 (3), 221–235. https://doi.org/10.1080/136698798377141.
FuturenauticsMaritime, K.V.H., & INTELSAT. (2018). *Crew Connectivity 2018 Survey Report*. F. Ltd. http://www.navarino.co.uk/wp-content/uploads/2018/04/Crew_Connectivity_2018_Survey_Report.pdf.
Gabriel, I.J., Nyshadham, E., 2008. A cognitive map of people's online risk perceptions and attitudes: an empirical study. In: Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008), Waikoloa.
Garcia-Perez, A., Thurlbeck, M., & How, E. (2017). Towards cyber security readiness in the Maritime industry: a knowledge-based approach. 1–7. https://pdfs.semanticscholar.org/0bca/56d7f4c56899540d3ee9180ee6c8557a813b.pdf.
Garg, V., Benton, K., & Camp, L.J. (2014). The privacy paradox: a Facebook case study. 2014 TPRC conference paper.
Garg, V., Camp, J., 2012. End user perception of online risk under uncertainty. In: Proceedings of the 2012 45th Hawaii International Conference on System Sciences, Maui.
Garg, V., Camp, L.J., 2015. Cars, condoms, and facebook. Information Security. Springer, pp. 280–289. https://doi.org/10.1007/978-3-319-27659-5_20.
Haltinner, K., Sarathchandra, D., Lichtenberg, N., 2015. Can I Live? College Student Perceptions of Risks, Security, and Privacy in Online Spaces. Cyber Security Symposium, Cham.
Harris, P., 1996. Sufficient grounds for optimism?: the relationship between perceived controllability and optimistic bias. J. Soc. Clin. Psychol. 15 (1), 9–52. https://doi.org/10.1521/jscp.1996.15.1.9.
Hemminghaus, C., Bauer, J., Padilla, E., 2021. BRAT: a bridge attack tool for cyber security assessments of maritime systems. TransNav 15 (1), 35–44. https://doi.org/10.12716/1001.15.01.02.
IMO. (2017). Guidelines on Maritime Cyber Risk Management. http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Documents/MSC-FAL.1-Circ.3%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat).pdf.
Kahneman, D., 2011. Thinking, Fast and Slow. Macmillan.
Kahneman, D., Slovic, S.P., Slovic, P., Tversky, A., 1982. Judgment Under uncertainty: Heuristics and Biases. Cambridge university press.
Kara, H., 2015. Creative Research Methods in the Social sciences: A practical Guide. Policy Press.
Karamperidis, S., Kapalidis, C., Watson, T., 2021. Maritime cyber security: a global challenge tackled through distinct regional approaches. J. Mar. Sci. Eng. 9 (12), 1323. https://doi.org/10.3390/jmse9121323.
Kessler, G.C., & Shepard, S.D. (2022). *Maritime Cybersecurity - A Guide for Leaders and Managers*(Second Edition ed.). Amazon.

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 J. Maritime Affairs 20 (2), 135–150. https://doi.org/10.1007/s13437-021-00242-2.
Kostyuk, N., Wayne, C., 2021. The microfoundations of state cybersecurity: cyber risk perceptions and the mass public. J. Glob. Sec. Stud. 6 (2) https://doi.org/10.1093/jogss/ogz077 ogz077.
Kvale, S., Brinkmann, S., 2015. Det Kvalitative Forskningsintervju, 3 ed. Gyldendal Norske Forlag AS.
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.
Malterud, K., 2017. Kvalitative Forskningsmetoder For Medisin Og Helsefag, 4 ed. Universitetsforlaget.
Manuel, M.E., Ghana, A., 2017. Maritime Risk and Organizational Learning, 1 ed. CRC Press. https://doi.org/10.1201/9781315593937.
McGillivary, P., 2018. Why Maritime cybersecurity is an ocean policy priority and how it can be addressed. Mar. Technol. Soc. J. 52 (5), 44–57. https://doi.org/10.4031/MTSJ.52.5.11.
Meland, P.H., Bernsmed, K., Wille, E., Rødseth, Ø.J., & Nesheim, D.A. (2021). A Retrospective Analysis of Maritime Cyber Security Incidents. 519–530. 10.12716/1001.15.03.04.
Mills, A.J., Durepos, G., Wiebe, E., 2010. Encyclopedia of Case Study Research. Sage. https://doi.org/10.4135/9781412957397.
Parkin, S., Kuhn, K., & Shaikh, S.A. (2021). Scenario-Driven Assessment of Cyber Risk Perception at the Security Executive Level. Workshop on Usable Security and Privacy, Auckland.
Postholm, M.B., 2006. Gruppearbeid som læringsaktivitet: en kvalitativ studie i universitetsklasserommet. Uniped (29), 23–31. https://digit.ntnu.no/assets/courseware/v1/99d9208c593e5777652c5ac56422525d/asset-v1:NTNU+MOOC002+2019-2020+type@asset+block/modelltekst.Postholm_1_.pdf.
Postholm, M.B., 2019. Analysing the data material using the constant comparative analysis method and ᴅ-analysis. Research and Development in School. Brill, pp. 85–102. https://doi.org/10.1163/9789004410213_007.
Progoulakis, I., Rohmeyer, P., Nikitakos, N., 2021. Cyber physical systems security for maritime assets. J. Mar. Sci. Eng. 9 (12), 1384. https://doi.org/10.3390/jmse9121384.
Pseftelis, T., Chondrokoukis, G., 2021. A study about the role of the human factor in maritime cybersecurity. SPOUDAI-J. Econ. Bus. 71 (1–2), 55–72.
Refsdal, A., Solhaug, B., Stølen, K., 2015. Cyber-risk management. Cyber-Risk Management. Springer, pp. 9–47. https://doi.org/10.1007/978-3-319-23570-7_5.
Renn, O., 1992. Concepts of risk: a classification. In: Krimsky, S., Golding, D. (Eds.), Social Theories of Risk. Praeger, CT, pp. 53–79.
Renn, O., 2004. Perception of risks. Toxicol. Lett. 149 (1–3), 405–413. https://doi.org/10.1016/j.toxlet.2003.12.051.
Rhee, H.-S., Ryu, Y.U., Kim, C.-T., 2012. Unrealistic optimism on information security management. Comput. Sec. 31 (2), 221–232. https://doi.org/10.1016/j.cose.2011.12.001.
Roeser, S., 2012. Handbook of Risk Theory: Epistemology, Decision Theory, Ethics, and Social Implications of Risk. Springer Science & Business Media (Vol. 1).
Siegrist, M., Árvai, J., 2020. Risk perception: reflections on 40 years of research. Risk Anal. 40 (S1), 2191–2206. https://doi.org/10.1111/risa.13599.
Siegrist, M., Cvetkovich, G., Roth, C., 2000. Salient value similarity, social trust, and risk/benefit perception. Risk Anal. 20 (3), 353–362. https://doi.org/10.1111/0272-4332.203034.
Siegrist, M., Keller, C., Kiers, H.A., 2005. A new look at the psychometric paradigm of perception of hazards. Risk Anal. 25 (1), 211–222. https://doi.org/10.1111/j.0272-4332.2005.00580.x.
Sjöberg, L., 2003. The different dynamics of personal and general risk. Risk Manage. 5 (3), 19–34. https://doi.org/10.1057/palgrave.rm.8240154.
Sjöberg, L., 2004. Explaining individual risk perception: the case of nuclear waste. Risk Manage. 6 (1), 51–64. https://doi.org/10.1057/palgrave.rm.8240172.
Sjöberg, L. (2012). Risk perception and societal response. In *Handbook of risk theory* (pp. 661–675).
Skotnes, R., 2015. Risk perception regarding the safety and security of ICT systems in electric power supply network companies. Safety Sci. Monitor 19 (1).
Slovic, P., 1987. Perception of risk. Science 236 (4799), 280–285. https://doi.org/10.1126/science.3563507.
Slovic, P., 1990. Perception of risk: reflections on the psychometric paradigm. Theories of Risk. Praeger.
Spencer, T., 2016. Risk Perception. Nova Science Publisher.
Tversky, A., Kahneman, D., 1973. Availability: a heuristic for judging frequency and probability. Cogn. Psychol. 5 (2), 207–232. https://doi.org/10.1016/0010-0285(73)90033-9.
Tversky, A., Kahneman, D., 1974. Judgment under Uncertainty: heuristics and Biases: biases in judgments reveal some heuristics of thinking under uncertainty. Science 185 (4157), 1124–1131. https://doi.org/10.1126/science.185.4157.1124.
Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., Kusev, P., 2017. Risk perceptions of cyber-security and precautionary behaviour. Comput. Human Behav. 75, 547–559. https://doi.org/10.1016/j.chb.2017.05.038.
Van Schaik, P., Renaud, K., Wilson, C., Jansen, J., Onibokun, J., 2020. Risk as affect: the affect heuristic in cybersecurity. Comput. Secur. 90, 101651 https://doi.org/10.1016/j.cose.2019.101651.
Von Solms, R., Van Niekerk, J., 2013. From information security to cyber security. Comput. Secur. 38, 97–102. https://doi.org/10.1016/j.cose.2013.04.004.
Weinstein, N.D., 1980. Unrealistic optimism about future life events. J. Pers. Soc. Psychol. 39 (5), 806. https://doi.org/10.1037/0022-3514.39.5.806.
Weinstein, N.D., Klein, W.M., 1996. Unrealistic optimism: present and future. J. Soc. Clin. Psychol. 15 (1), 1–8. https://doi.org/10.1521/jscp.1996.15.1.1.
Weinstein, N.D., Marcus, S.E., Moser, R.P., 2005. Smokers' unrealistic optimism about their risk. Tob. Control 14 (1), 55–59. https://doi.org/10.1136/tc.2004.008375.
Withman, M.M., Herbert, 2019. Management of Information Security, 6 ed. Cege.

Paper 3

Maritime decision-makers and cybersecurity: Deck officers' perception of cyber risks towards IT and OT systems

Authors: Marie Haugli-Sandvik, Mass Soldal Lund, and Frøy Birte Bjørneseth

International Journal of Information Security, in press

Maritime Decision-Makers and Cyber Security: Deck Officers' Perception of Cyber Risks Towards IT and OT systems

Marie Haugli-Sandvik[1], Mass Soldal Lund[2], Frøy Birte Bjørneseth[1,3]

[1]Norwegian University of Science and Technology, Department of Ocean Operations and Civil Engineering, 6025 Aalesund, Norway

[2]Inland Norway University of Applied Sciences, 2450 Rena, Norway

[3]Kongsberg Maritime, 6025 Aalesund, Norway

Corresponding author

Marie Haugli-Sandvik, email: marie.h.sandvik@ntnu.no, ORCID: 0000-0001-8308-1915

Abstract

Through a quantitative study of deck officers' cyber risk perceptions towards information (IT) and operational (OT) systems, this paper contributes to substantiate the importance of considering human behaviour within maritime cyber security. Using survey data from 293 deck officers working on offshore vessels, statistical analyses were conducted to measure and predict the participants cyber risk perceptions towards IT and OT systems. Performing a Wilcoxon signed-rank test revealed a significant discrepancy in the levels of cyber risk perception between the system categories. Hierarchical regression analyses were conducted to develop statistical models, considering multiple independent variables, including perceived benefit, cyber security training, experience with cyber-attacks, and trust towards various stakeholders. Key findings revealed distinct results for IT and OT systems, and the regression models varied in both predictive power and significance of the independent variables. Perceived benefit positively predicts deck officers cyber risk perception for both IT and OT systems, while trust, which included measures of social trust and confidence, was not found to be significant. Cyber security training and experience with cyber-attacks only influence deck officers' perception of cyber risks related to operational technology. Practical implications of this work provide actionable recommendations for the maritime industry, including tailored risk communication tools, training programs, reporting systems, and holistic policies.

Keywords

Maritime cyber security, cyber risk perception, IT and OT systems, perceived benefit, trust, cyber security training.

1 Introduction

In the aftermath of rapid digitalisation, which was further accelerated by the global COVID-19 pandemic, and with the war in Europe changing the cyber threat landscape, cyber-attacks have emerged as a mounting concern for the offshore industry [1]. The maritime sector, with its extensive reliance on interconnected systems, is particularly vulnerable to such threats [2]. A well-known example of a cyber-attack in the maritime industry was the ransomware NotPetya hitting the Maersk Shipping Company in 2017, resulting in a company loss of over 300 million USD [3]. Another notable cyber-attack occurred at the International Maritime Organization (IMO) in 2020, disrupting their systems shortly before the launch of their resolution on enhancing maritime cyber risk management [4]. Recent reports and papers provide an overview of cyber-attacks against both shipping companies and vessels, leaving no doubt that maritime cyber risks are omnipresent [5-7].

Consequently, there is a growing concern about the vulnerabilities inherent in maritime information and operational technology systems (IT and OT systems), and potential consequences of successful cyber-attacks targeting these systems range from substantial financial losses to environmental disasters and the potential loss of life at sea [8]. Safeguarding the integrity, confidentiality, and availability of critical maritime systems has become an essential task for industry stakeholders [9], especially in regard to the operational technology which governs offshore vessels physical assets [3].

At sea, the human operator plays a crucial role in the first line defence against cyber risks [10]. Previous research highlights the importance of comprehending human behaviour to develop precise tools for cyber risk mitigation strategies within the maritime domain [11-13]. In this regard, one important aspect within behaviour science is the concept of risk perception, which investigates how various factors influence the perception of technological risk across different contexts [14]. It is widely recognized that action-related decisions build on individual risk perceptions, and that these perceptions play a major role in prompting protective action towards cyber risks [15, 16]. Consequently, with the new cyber threat landscape that modern vessels must navigate today, it is of utter importance to help the crew prevent and handle cyber incidents. To do this effectively, it is vital to investigate maritime decision makers', such as deck officers, cyber risk perceptions towards IT and OT systems [17, 18]. The nature of IT and OT is different, and cyber risk management strategies must consider this distinction, especially to strengthen maritime OT-security and facilitate good cyber security behaviour [3, 9].

Motivated by a previous qualitative study that explored factors influencing deck officers' perception of cyber risks [19], this paper aims to investigate variations and causal relationships in cyber risk perception within this maritime context. The objective of this study is twofold: to measure deck officers' cyber risk perception and develop predictive statistical models to predict their perception of cyber risks towards IT and OT systems. To achieve this, a survey was conducted among deck officers working on offshore vessels within Norwegian shipping companies. The survey included measures of cyber risk perception, perceived benefit, cyber security training, experience with cyber-attacks, and trust towards different stakeholders within the maritime domain. The results have potential to further inform decision-making processes and facilitate development of targeted and preventive measures to enhance maritime cyber security and safety.

The remaining sections of this paper are organized as follows: first, theoretical aspects and previous research is presented, followed by the hypotheses investigated in this paper. Subsequently, the methodology is presented before the results are given and discussed. Finally, the limitations are addressed before concluding the paper, which also includes suggestions for further research.

2 Theoretical aspects

2.1 Maritime cyber security and cyber risks

The unique characteristics of the maritime domain, such as global operations, long supply chains, operational and demanding working environments, and diverse stakeholders, pose significant challenges in building and maintaining robust cyber security [5]. The offshore industry is experiencing rapid changes, driven by simultaneous efforts to achieve the green shift while aiming to reduce operational costs. This has led to a growing emphasis on digitalization and automation as essential marked strategies to maintain relevance [20]. Vessels, equipped with advanced technologies and automated systems, are connected through the Internet of Things (IoT), satellite communications, and cloud-based services. The IT-infrastructure is becoming more advanced, and the previous air gap isolating operational technology is closing as propulsion, machinery and navigational systems becomes more networked and connected [3]. This complexity and interconnectedness increases the cyber-attack surface, leaving vessels and crew exposed to cyber risks caused by threats exploiting cyberspace [21].

Maritime cyber security can be understood as the measures and practices implemented to protect vessels, ports, shipping companies and related infrastructures from cyber risks [9]. By use of von Solms' and van Niekerk's [22] definition of cyber security, this understanding involves the protection of cyberspace itself, the electronic information, the IT and OT systems that support cyberspace, and the users of cyberspace. The users, in this context the crew, are vital assets that needs protection and safeguarding at sea. As emphasized in earlier research, safety and security are intertwined with each other, making maritime cyber risks potential safety risks and vice versa [11].

Research within maritime cyber security has increased over the last decade, and several recent studies focus on aspects related to cyber security awareness [6]. These studies often focus on cyber preparedness in maritime companies [23], seafarers' level of cyber security awareness [24], or how training frameworks can be developed to enhance awareness and knowledge [12, 25]. While such studies are centred around the human aspect of cyber security, they often fell short of addressing the underlying behavioural processes such as risk perception.

Despite the growing interest and awareness of cyber risks and threats in the maritime sector, findings of Chubb et al. [26] suggest that seafarers and other industry professionals are still struggling with comprehending cyber risks and the implementation of mitigating measures. Some may underestimate the potential impact of cyber incidents due to a lack of training and experience with cyber-attacks, while others may be overwhelmed by the complexities of cyber threats and uncertain about the appropriate risk mitigation strategies [5, 24]. Understanding cyber risk perception and factors influencing them, can help foster a proactive and resilient cyber risk management approach within maritime companies. This study includes measures of cyber security training and experience with cyber-attacks to investigate their causal relationship to deck officers' perception of cyber risks.

2.2 IT and OT systems

Offshore vessels rely extensively on a diverse range of information technology (IT) and operational technology (OT) systems to support their operational activities [3]. IT systems encompass the traditional computing and networking infrastructure used for administrative tasks, communication, data management, and business operations within shipping companies, their vessels, and ports. These systems often handle sensitive information such as financial data, crew details, and cargo manifests. On the other hand, OT systems refer to the hardware

and software that control, monitor, and automate the physical processes and machinery in maritime operations, such as navigational systems, engine controls, cargo handling equipment, and safety mechanisms [27].

The key difference between IT and OT systems lies in their primary functions and scope of influence. While IT systems are predominantly focused on data management and administrative functions, OT systems are specifically designed to interact with and control physical assets and processes [9]. These systems are vital for ensuring the safe and efficient operation of vessels. However, as mentioned above, the integration and digitalization of these systems introduce new cyber risks.

Reviewed literature shows the omnipresence of cyber risks towards modern vessels [5]. Several recent papers provide records of inherent system vulnerabilities, possible cyber-attack vectors and significant previous cyber-attacks against vessels and maritime industry [1, 2, 4, 6, 7, 27]. It is a clear trend that connectivity and interconnection affect the security level of maritime infrastructures negatively. Moreover, a lack of proper cyber security training and more sophisticated cyber-attack methods increases the probability of successful cyber-attacks towards vessels and maritime industry [6]. Additionally, studies show that there is a lack of OT-security expertise within shipping companies, and that it remains ambiguity about the allocation of responsibility for securing the operational technology [26].

Research within maritime cyber security has increased over the years. Recently there has been a shift in focus from mainly looking at cyber risks towards information technologies, to a greater interest in cyber risks and threats towards operational technologies as well [3, 26, 28]. Even so, few papers address human behaviour within maritime cyber security, regardless of the well-established fact that humans play an important role in cyber security and protection of all technical systems [8, 11]. How deck officers perceive cyber risks towards IT and OT systems will influence their behaviour and cyber security compliance [19]. Since the two system categories have fundamentally distinct functions and history of digitalization, different factors might influence the officer's perception of risks towards these systems. Therefore, the objective in this study is to measure their level of cyber risk perception towards IT and OT systems, and to test the causal relationship between their perceptions and independent variables as perceived benefit and trust.

2.3 Risk perception

Since the 1970s, researchers have been studying how risk perceptions are formed, trying to explain how people reconstruct previously assimilated risk through subjective judgments [29-31]. How people perceive risk is important because it influences individual behaviour as well as the acceptance and commitment to technology, policies, and norms [32]. Each technology has its specific risk factors that need to be studied in their own right and context [33], especially since factors explaining people's perception of risk varies from population to population and from profession to profession [34, 35].

As shown in figure 1, there are multiple paradigms within risk perception research, and Siegrist and Árvai (2020) group these within three general approaches: hazard characteristics, characteristics of risk perceivers, and heuristics. Within these approaches, studies of risk perception related to perceived benefit, trust, and the availability heuristic can be found. These factors have been identified as predictive factors of cyber risk perceptions in various research fields [11, 19].

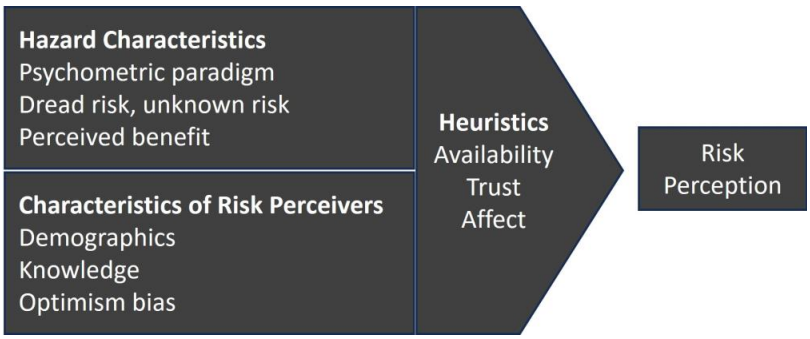


Figure 1: Paradigms and influential factors in risk perception (adapted from Siegrist and Árvai, 2020) [32].

2.3.1 Perceived benefit of technology

The studies of Starr (1969) and Fischoff et al. (1979) has been the inspiration for numerous of perceived risk and benefit studies within the psychological paradigm of risk perception [36]. Starr advocated for a "revealed preference" approach where use of risk and benefit data could be used to reveal patterns of acceptable risk-benefit trade-offs [37]. Some years later, in the wake of the debate over Starr's approach, Fischoff et al. [31] developed the "expressed preference" approach which indicates that society may accept higher levels of risk with more beneficial activities and tolerate higher risk levels for voluntary activities [38]. This coincides with several studies finding an inverse correlation between levels of cyber risks towards information technologies and internet related activities perceived as beneficial [15, 38-40].

The causal relationship between perceived risk and benefit have been questioned and it is postulated that risk and benefit perceptions may be influenced by other variables or causal relationships, as within the psychometric paradigm [29, 41]. This study will investigate to what extent perceived system benefit has a causal relationship with deck officers cyber risk perception.

2.3.2 Trust

An often used definition of trust within risk perception and management: *"Trust is a psychological state compromising the intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another"* [42]. According to Siegrist [35], trust is an important concept for a better understanding of perceptions or decisions made in the risk domain, and the function of trust can be a mechanism for reduced complexity that enables people to maintain their capacity to act in a complex environment. This coincides with a study indicating that the concept of trust could be of relevance to deck officers' perception of cyber risks and their vessels' cyber defence [19].

One way of classifying trust mechanisms is by looking at trust as the result of social trust and confidence. This conceptual framework of trust postulates that social trust is related to the judgement of similarities in intentions and values, whereas confidence is based on past experiences suggesting that future events will occur as expected [43]. Previous studies using this framework often ask participants to assess their trust in an industry or such, but it can be unclear to what extent the participants rely on competence or value aspects when answering such questions [44]. Because social trust and confidence often is found to be strongly correlated [35], they will be combined into one construct in this study [45].

The importance of trust is somewhat controversial, and previous research have found various degrees of correlation between trust measurements and risk perceptions of technology [46]. It seems that degree of knowledge about the technology and risks involved, the perceived importance of the issue, and the methods used to measure the constructs of trust is important for the observed correlation between trust and risk perception [35]. Other research findings question if the effect of trust is direct or indirect, and that trust influences both risk and benefit perceptions. Social trust has been found to decrease risk perceptions and increase benefits association [41, 47].

2.3.3 The availability heuristic

People often rely on heuristics when making decisions, meaning they replace a target attribute that is not readily accessible (e.g., the objective probability of a cyber-attack) with a heuristic that comes to mind more easily (e.g., the number of concrete examples of cyber-attacks that can be recalled) [32, 48]. In the risk domain, a major part of research focus on the availability heuristic [35], which is when people use the "ease with which instances of occurrences can be brought to mind" [49].

If people rely on the availability heuristic, they tend to perceive threats or risk events as high risk when they find it easy to imagine, recall or conceptualise the occurrence of such threats or events [50, 51]. How heuristics are used to evaluate information and how these processes influence certain cognitive biases, has played an important role in the discussion of risk perception [30]. Nevertheless, how the availability heuristic should be operationalized or measured is undetermined, and it may not be fully clear in which situations and contexts people actually rely on this heuristic [32].

3 Purpose of study and hypotheses

The aim of the research presented in this paper is to measure deck officers' cyber risk perceptions and develop statistical models for prediction of their perception of cyber risks towards their vessels IT and OT systems. Informed by previous research and theory within the fields of maritime cyber security and risk perception, the following two hypotheses were developed:

- H1: Deck officers perceive lower cyber risks towards OT systems than IT systems.
- H2: There is a difference in how the independent variables perceived benefit, trust, cyber security training, and experience with cyber-attacks predict deck officers' cyber risk perception towards their vessels IT and OT systems.

This study was motivated by a previous qualitative study conducted to explore and describe factors influencing deck officers' perception of cyber risks [19]. Several main themes that emerged from those in-depth interviews, directly inspired the hypotheses development in this study. For instance, the qualitative findings implied that deck officers rely on trust in other stakeholders for cyber defence. Furthermore, the officers emphasized having limited cyber security knowledge and training, and they described IT and OT systems differently with regard to cyber risks and perceived benefits [19]. By grounding the hypotheses in the real-

world experiences of deck officers, layers of context and depth were added to the research design, ensuring relevance to practical challenges faced by maritime decision makers.

4 Method

To investigate the hypotheses, a survey was conducted among deck officers working on offshore vessels within Norwegian shipping companies. The survey included measures of cyber risk perception, perceived benefit, and trust towards different stakeholders in relation to their vessels IT and OT systems. Participants were also asked about their experience with cyber-attacks and amount of cyber security training. The constructs in the questionnaire were developed based on previous research within maritime cyber security and cyber risk perception [11, 19]. Wilcoxon signed-rank test was used to compare the level of perceived cyber risk towards IT and OT systems. Then, hierarchical regression analyses were performed to test the independent variables prediction of cyber risk perception.

4.1 Participants

The participants in this study were selected to gain insights into cyber risk perception in the offshore industry. The selection criteria were deck officers employed on offshore vessels, which are vessels that specifically serve operational purposes such as oil exploration and construction work at the high seas [52]. Offshore vessels operate in a critical environment and utilize highly technical systems, making cyber risk management of utmost importance [3]. To ensure adequate representation, an online survey was distributed to eleven of the largest offshore companies operating in Norway. These companies were responsible for distributing the survey among their deck officers working on offshore vessels during the designated period between October and December 2022.

To ensure sample representativeness, efforts were made to recruit participants who were representative of the target population of deck officers working on offshore vessels. Although the study did not employ random sampling, the sample characteristics closely mirrored those of the broader population in terms of demographic and professional attributes. This enhances the external validity and generalizability of the findings to the wider population [53].

Prior to participating in the study, the participants were provided with information regarding the purpose of the research. They were explicitly informed that the survey was anonymous, ensuring that their responses could not be traced back to them. Participants were requested to confirm their voluntary consent to participate, thereby acknowledging their understanding of the study's objectives. To address potential concerns or seek additional information or

support, participants were also provided with contact information of the researchers. These measures were implemented to uphold ethical standards and to safeguard participant confidentiality and privacy throughout the research process.

4.2 Questionnaire

The questionnaire used in this study consisted of five sections: (1) demographic information, (2) perception of system benefits, (3) experience with cyber-attacks and cyber security training, (4) perception of cyber risks, and (5) trust towards different stakeholders. See appendix for an overview of the questionnaire wording, which was distributed in both English and Norwegian to the participants.

The first section included questions about age range, gender, educational level, years of experience working at sea, and what rank they currently were holding on their offshore vessel. Section two included questions about assessing the benefits of systems deck officers depend on in their everyday working life. Participants were asked to rate the level of benefit on a scale ranging from 1 (no benefit at all) to 5 (very high benefit) for systems commonly found on the bridge of an offshore vessel. They also got the option of choosing "Don't know/Don't use this" when assessing the systems.

The third section had the topics experience with cyber-attacks and cyber security training. The first questions were related to the participants experience with cyber-attacks towards their vessel and shipping company, together with how many times they have heard about others being victim of a cyber-attack. Then the participants were asked to rate how often they have conducted different types of cyber security training (e.g., computer-based training, security drills and tabletops).

Section four included questions about assessing the level of cyber risks towards the same type of systems they rated in section two. Participants were asked to rate the level of cyber risk on a Likert scale ranging from 1 (no cyber risk at all) to 5 (very high cyber risk) or select the option "Don't know/Don't use this". The systems listed were the same as for perceived benefit, and they were presented in a random order as shown in the appendix.

Section five included questions about social trust and confidence, which forms the construct trust, in stakeholders related to securing the onboard systems and performing the cyber security tasks they are responsible for. Participants were asked to rate their level of trust on a scale ranging from 1 (no trust at all) to 5 (very high trust). The stakeholders they were asked

about was their crew, management, IT-department, suppliers of onboard systems, their government, and the International Maritime Organisation (IMO).

A panel of academic experts and a small group of former deck officers with relevant expertise were involved in the review process of the questionnaire. Their valuable insights and feedback helped refine the questionnaire to ensure its suitability and relevance to the study context. Prior to the main data collection, a pilot test of the questionnaire was conducted. A subset of participants, similar to the target population, were invited to complete the questionnaire and provide feedback. This pilot testing allowed for the identification of potential ambiguities or difficulties in item interpretation. Based on the feedback received, adjustments were made to improve the clarity of the questionnaire items, enhancing the face validity and content validity [53]. The pilot study was conducted with seven participants, and they were not included in the final sample.

The survey was administered online using the Nettskjema tool, specifically designed to meet privacy requirements in Norway [54]. The online format allowed for efficient data collection and facilitated wider accessibility for participants. The survey was accessible to the participants between the 19th of October and the 31st of December 2022, providing a designated time frame for response submission.

4.3 Statistical analyses

Significance level of $p < 0.05$ was used as limit, and all analyses were performed in version 28 of SPSS. There were no missing data as the electronic survey required mandatory answers to all the questions. Even so, the option "Don't know/Don't use this" was given the value 0 in the dataset and treated as a missing value for the constructs cyber risk perception and perceived benefit.

Wilcoxon signed-rank test was used to test for significant discrepancies between deck officers' perception of cyber risk towards IT and OT systems. This test was appropriate since it allows for testing of two conditions when the scores came from the same participants and since the statistical data is not normally distributed [53].

Two separate hierarchical linear regression analyses were performed to investigate the causal relationships between the independent variables and the dependent variables cyber risk perception towards IT systems and cyber risk perception towards OT systems. Reliability and validity of the measurements were investigated together with multicollinearity tests.

Evaluation of increase or decrease in R^2 between the steps in regression analyses was used to determine significance between two consecutive steps in the analyses.

5 Results

5.1 Descriptive statistics

A total of 293 respondents participated in the study. Among the respondents, 96 % identified as male (N = 282), while 2.5 % identified as female (N = 7). An additional 1.5 % of participants chose to identify as "other" or preferred not to disclose their gender (N = 4). Given the male-dominated nature of the offshore industry [55], the high percentage of male participants aligns with expectations. In terms of age distribution, 60.4 % of participants fell within the age range of 30-49 years. Detailed statistical information about the sample can be found in Table 1.

Table 1
Basic statistics of the sample.

	Options	**%**	**n**
Gender	Other/Don't want to say	1.4	4
	Male	96.2	282
	Female	2.4	7
Age	19-29	15.4	45
	30-39	27.6	81
	40-49	32.8	96
	50-59	20.8	61
	60-69	3.4	10
Rank	Second mate	40.6	119
	Chief mate	25.6	75
	Captain	33.8	99
Education*	Vocational school	49.5	148
	Bachelor's degree	44.0	129
	Master's degree	14.7	43

*Participants could choose more than one option in this question.

Table 2 gives an overview of the average level of cyber risk and benefit the deck officers perceived of each system in the questionnaire, together with statistics of how many participants answering "Don't know/Don't use this". One of the IT systems (passenger servicing and management systems) scored high on "Don't know/Don't use this" (39.2 % under perceived benefit and 43.3 % when assessing cyber risks), so it was excluded in the analyses.

Table 2
Descriptive statistics of IT and OT systems

	Mean cyber risk	**N***	**%***	**Mean benefit**	**N****	**%****
IT system						
E-mail	4.38	3	1.0	4.82	1	0.3
Passenger servicing and management systems***	3.03	**127**	**43.3**	3.69	**115**	**39.2**

Remote access for monitoring	3.48	39	13.3	3.62	54	18.4
Client reporting systems	3.17	67	22.9	3.68	56	19.1
SafeSeaNet	3.02	46	15.7	4.30	44	15.0
Internal reporting system	2.86	13	4.4	4.23	3	1.0
OT system						
Power management systems (PMS)	2.64	18	6.1	4.52	6	2.0
Electronic Chart Display and Information System (ECDIS)	2.93	3	1.0	4.92	1	0.3
Radar	2.10	3	1.0	4.92	1	0.3
Dynamic Position System (DP-system)	2.67	4	1.4	4.97	4	1.4
Remote access for maintenance	3.51	27	9.2	4.09	31	10.6
Cargo and loading management systems	2.01	27	9.2	4.33	19	6.5

*Participants who chose "I don't know/Don't use this" when assessing cyber risks **Participants who chose "I don't know/Don't use this" when assessing system benefits ***System excluded from the analyses

5.2 Wilcoxon signed-rank test

Wilcoxon signed-rank test was conducted to examine significant discrepancies in the deck officers' levels of cyber risk perception towards IT and OT systems. Because one IT system was excluded from the analysis, summative indexes with mean values were used in this test (Table 3). The result is conveyed in Table 4 and revealed that deck officers perceive a significant lower cyber risk towards OT systems (Mean = 2.69) than IT systems (Mean = 3.44), z = -11.97, p = 0.00, r = -0.703. This confirmed H1 and the divide between these two system categories were kept when performing the regression analysis.

Table 3
Statistics of variables used in the Wilcoxon signed-rank test

	Information	Min.	Max.	N	SD	Mean
Perceived cyber risk IT systems	Mean values of 5 ordinal variables	1.20	5.00	291	.807	3.44
Perceived cyber risk OT systems	Mean values of 6 ordinal variables	1.00	5.00	290	.955	2.69

Table 4
Results of Wilcoxon signed-rank test comparing perceived cyber risk towards OT and IT systems

N	290
T	3279
α	1334.368
z	-11.970
p (2-sided)	.000
r (z/√N)	-.703

5.3 Reliability and validity of measurements

Summative indexes were created to represent the measured constructs by summing the scores of the measured items within each latent variable. An overview of the variables is shown in Table 5. The measured items within the variables cyber risk perception, perceived benefit, and trust are assumed to be indicators of the underlying latent variables, and these items are expected to be correlated [56]. This is not the case with the items within cyber security training and experience with cyber-attacks, which are considered as formative measurements [57].

Table 5
Statistics of variables used in the regression analysis.

	Information	Range	Min.	Max.	N	SD	Mode	α
Perceived cyber risk IT systems**	S.I* with 5 ordinal variables	22	3	25	291	4.43	17	.770
Perceived cyber risk OT systems**	S.I* with 6 ordinal variables	27	3	30	290	5.92	14	.880
Perceived benefit	S.I* with 11 ordinal variables	32	23	55	293	6.03	55	.753
Trust	S.I* with 12 ordinal variables	48	12	60	293	7.82	48	.897
Cyber security training	S.I* with 8 ordinal variables	30	5	35	293	5.91	17	
Experience cyber-attack own vessel	Ordinal variable	4	0	4	293	.904	1	
Experience cyber-attack company	Ordinal variable	4	0	4	293	1.02	1	
Hear about cyber-attack others	Ordinal variable	4	0	4	293	1.09	3	

*Summative Index, **Dependent variable

Internal consistency is often used as a reliability indicator of measurements expected to correlate [56]. Cronbach's alpha coefficient was utilized to assess the reliability of the applicable variables. The reliability analysis results, presented in Table 5, demonstrate the internal consistency of the variables measuring cyber risk perception, perceived benefit, and trust, which all show acceptable levels with Cronbach's alpha values > 0.7. Further, the validity of the measurement instruments was a key consideration. The questionnaire items were developed based on a review of existing literature on risk perception, benefit, and trust [19, 41, 44, 50, 58], ensuring that the constructs of interest were captured.

5.4 Hierarchical regression analysis

Hierarchical regression analysis was performed to test H2. Two separate analyses were conducted for cyber risk perception towards IT and OT systems. Because of theoretical considerations, the first step in the hierarchy included the independent variables perceived

benefit and trust. The variables cyber security training and experiences with cyber-attacks were added in the second step.

The regression models with cyber risk perception towards IT systems as dependent variable are conveyed in Table 6. *Perceived benefit* significantly related to cyber risk perception of IT systems in both models ($\beta_1 = 0.233$, $p < 0.001$; $\beta_2 = 0.198$, $p < 0.001$). *Trust*, *cyber security training*, and the three *experience with cyber-attacks* variables were not significant in both steps ($p > 0.05$). Step 1 accounted for 8.5 % of the variance ($R^2 = 0.085$). The change in R^2 was not significant in step 2 ($R^2 = 0.101$; $\Delta R^2 = 0.016$, $p = 0.296$), and there was a decrease in the F value ($F_1 = 13.380$; $F_2 = 5.299$), indicating that the addition of the variables in Step 2 led to a decrease in model fit. The F-test is a component of analysis of variance (ANOVA) and is utilized to determine the significance of the overall model [53].

Table 6
Results of hierarchical regression analysis with Cyber Risk Perception of IT systems as dependent variable

	b	SE B	β	p	95 % CI Lower	Upper
Step 1						
Constant	6.800	2.071		.001	2.724	10.875
Perceived Benefit	.233	.043	.305	<.001	.138	.309
Trust	-.041	.033	-.072	.223	-.106	.025
Step 2						
Constant	6.889	2.142		.001	2.673	11.104
Perceived Benefit	.198	.045	.270	<.001	.109	.286
Trust	-.052	.034	-.093	.126	-.120	.015
Cyber security training	.083	.046	.110	.072	-.008	.173
Experience cyber-attacks own vessel	.148	.321	.030	.645	-.484	.781
Experience cyber-attacks own company	-.324	.282	-.075	.251	-.879	.230
Heard about cyber-attacks others	.143	.253	.035	.571	-.355	.641

Note: $R^2 = .085$ with $p < .001$ for Step 1; $\Delta R^2 = .016$ with $p = .296$ for Step 2

The regression models with the dependent variable of cyber risk perception towards OT systems is presented in Table 7. *Perceived benefit* significantly related to the dependent variable in both steps ($\beta_1 = 0.211$, $p < 0.001$; $\beta_2 = 0.147$, $p = 0.015$), and *trust* was not significant in neither of the models ($p > 0.05$). *Cyber security training* ($\beta = 0.142$, $p = 0.020$), *experience with cyber-attacks towards own vessel* ($\beta = 0.966$, $p = 0.024$) and *company* ($\beta = -1.235$, $p = 0.001$), and *heard about cyber-attacks towards others* ($\beta = 0.749$, $p = 0.027$) significantly predicted cyber risk perception towards OT systems. The first step accounted for 4.3 % of the variance ($R^2 = 0.043$), and the change in R^2 was significant and accounted for 11.8 % of the variance in the second step ($R^2 = 0.118$; $\Delta R^2 = 0.074$, $p < 0.001$). Even so, there

was a slight decrease in the F value (F_1 = 6.486; F_2 = 6.292), indicating that the model fit did not improve.

Table 7
Results of hierarchical regression analysis with Cyber Risk Perception of OT systems as dependent variable

	b	SE B	β	p	95 % CI Lower	Upper
Step 1						
Constant	7.197	2.835		.012	1.616	12.778
Perceived Benefit	.211	.059	.216	<.001	.095	.328
Trust	-.027	.046	-.036	.552	-.117	.063
Step 2						
Constant	7.236	2.841		.011	1.644	12.829
Perceived Benefit	.147	.060	.150	.015	.029	.264
Trust	-.053	.045	-.070	.248	-.142	.037
Cyber security training	.142	.061	.142	.020	.023	.262
Experience cyber-attacks own vessel	.966	.427	.147	.024	.126	1.805
Experience cyber-attacks own company	-1.235	.374	-.215	.001	-1.972	-.499
Heard about cyber-attacks others	.749	.336	.138	.027	.088	1.410

Note: R^2 = .043 with p = .002 for Step 1; ΔR^2 = .074 with p < .001 for Step 2

5.5 Multicollinearity

Multicollinearity arises when independent variables have high correlation between themselves, leading to a lack of ability to predict the values of dependent variables [53]. To assess the presence of multicollinearity, both variance inflation factor (VIF) and correlation analysis were conducted. The results, as shown in Table 8 and 9, indicate that all variables have VIF values below three, suggesting low levels of multicollinearity. Moreover, the tolerance levels are above 0.2, indicating that a substantial proportion of variance in each variable is not shared with other predictors. However, the correlation analysis reveals significant correlations between multiple variables (Table 10 and 11). Most correlations are moderate (between 0.2 and 0.4) or weak (>0.2), except for the correlation between experience with cyber-attacks towards own vessel and company, which demonstrates a correlation coefficient of 0.462 and 0.461. Although the presence of this medium-high correlation is not very surprising and suggests the potential for multicollinearity, the overall VIF values and tolerance levels indicate that the multicollinearity issue in the model might be within acceptable limits. Even so, this could introduce challenges in the regression analysis by reducing the statistical significance of experience with cyber-attacks towards own vessel and company, since they might explain overlapping portions of variance in the dependent variables [56].

Table 8
Results of multicollinearity analysis

Variables	Tolerance	VIF
Step 1		
Perceived Benefit	.908	1.101
Trust	.908	1.101
Step 2		
Perceived Benefit	.840	1.190
Trust	.861	1.162
Cyber security training	.848	1.179
Experience cyber-attack own vessel	.737	1.357
Experience cyber-attack own company	.737	1.357
Heard about cyber-attack others	.811	1.233

a. Dependent variable: Cyber risk perception IT systems

Table 9
Results of multicollinearity analysis

Variables	Tolerance	VIF
Step 1		
Perceived Benefit	.908	1.101
Trust	.908	1.101
Step 2		
Perceived Benefit	.840	1.191
Trust	.861	1.162
Cyber security training	.848	1,179
Experience cyber-attack own vessel	.737	1.357
Experience cyber-attack own company	.737	1.357
Heard about cyber-attack others	.810	1.234

a. Dependent variable: Cyber risk perception OT systems

Table 10
Correlation analysis with Cyber Risk Perception IT systems as dependent variable

	Cyber Risk Perception IT	Perceived Benefit	Trust	Cyber security training	Experience cyber-attack own vessel	Experience cyber-attack own company	Heard about cyber-attack others
Cyber Risk Perception IT	1.000						
Perceived Benefit	.283**	1.000					
Trust	.020	.303**	1.000				
Cyber security training	.172*	.285**	.206**	1.000			
Experience cyber-attack own vessel	.032	.040	.032	.156*	1.000		
Experience cyber-attack own company	-.039	-.050	-.125*	.125*	**.462****	1.000	

Heard about cyber-attack others	.091	.140*	-.050	.234**	.331**	.306**	1.000

*p < 0.05. **p < 0.01

Table 11
Correlation analysis with Cyber Risk Perception OT systems as dependent variable

	Cyber Risk Perception OT	**Perceived Benefit**	**Trust**	**Cyber security training**	**Experience cyber-attack own vessel**	**Experience cyber-attack own company**	**Heard about cyber-attack others**
Cyber Risk Perception OT	1.000						
Perceived Benefit	.205**	1.000					
Trust	.029	.303**	1.000				
Cyber security training	.199**	.285**	.205**	1.000			
Experience cyber-attack own vessel	.120*	.040	.033	.157*	1.000		
Experience cyber-attack own company	-.085	-.050	-.125*	.126*	**.461****	1.000	
Heard about cyber-attack others	.179**	.140*	-.051	.234**	.332**	.307**	1.000

*p < 0.05. **p < 0.01

5.6 Summary of results

The statistical analyses gave the following results:

- The result from the Wilcoxon signed-rank test supports H1 and shows that deck officers perceive significantly lower cyber risks towards operational technology than informational technology.
- The results from the hierarchical regression analyses support H2 regarding perceived benefit, cyber security training, and experience with cyber-attacks. Figure 2 visualizes the second step of the regression analyses, showing the difference in significance levels and beta values, suggesting that these independent variables influence deck officers' cyber risk perception differently with respect to IT and OT systems.
- The results from the regression analyses do not support H2 regarding trust. Figure 2 shows that trust was not a significant predictor of deck officers' cyber risk perception in either of the regression models.
- Perceived benefit of systems was positively significant for predicting cyber risk perception towards both IT and OT systems, with quite similar beta values. However, this independent variable explains more of the variance in perception of cyber risks towards IT systems than OT systems.

- The amount of cyber security training positively predicts deck officers' perception of cyber risks towards OT systems but was not a significant predictor towards IT systems.
- Previous experience with cyber-attacks towards own vessel and company were significantly related to cyber risk perception of OT systems but not of IT systems. Figure 2 shows that deck officers with experience of cyber-attacks towards own vessel have an increase in their cyber risk perception, and a decrease in their cyber risk perception if they have experience with cyber-attacks towards own company.
- If deck officers have heard about other vessels or companies being victims of cyber-attacks, it positively predicts their cyber risk perception of OT systems.

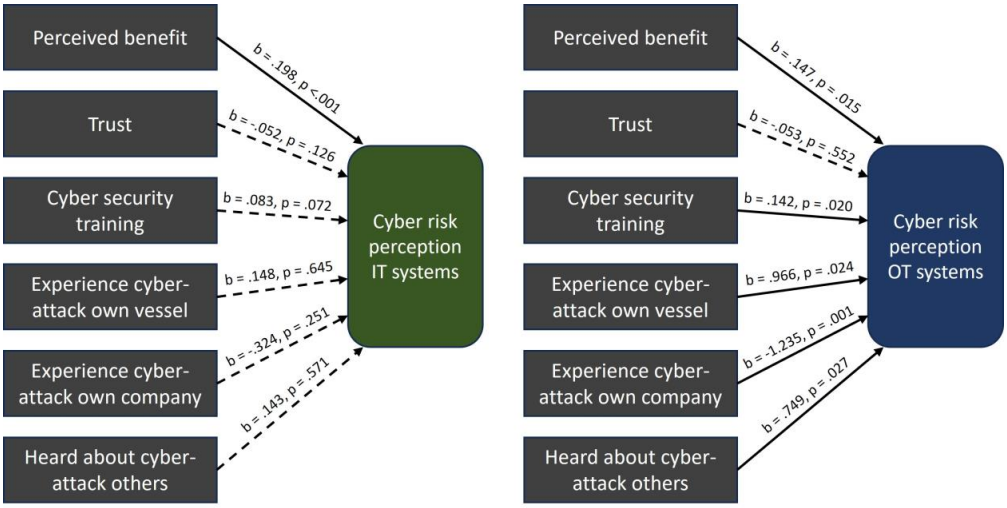


Figure 2: Results of the causal relationship between the independent variables and cyber risk perception in the second step of the hierarchical regression analyses. Dotted line indicates no significant relationship. Beta value and significance level are given for each independent variable.

6 Discussion

The aim of this research is to study deck officers' cyber risk perception. The goals were to measure if (1) deck officers perceive lower cyber risks towards OT systems than IT systems and investigate if (2) there is a difference in how perceived benefit, trust, cyber security training, and experience with cyber-attacks predict their perception of cyber risks towards IT and OT systems. In this section, the results are reviewed in relation to these goals. Additionally, implications of the work are discussed, recommendations are made, future research areas identified, and limitations considered.

6.1 Level of cyber risk perception towards IT and OT systems

Historically, operational technology on vessels have been isolated from the internet and shielded from cyber threats. This air gap is not the case anymore, and over the past years there has been an extensive increase in cyber-attack vectors and cyber risks towards all maritime systems [3]. Even so, the Wilcoxon signed-rank test result in Table 4 show that deck officers perceive significantly lower cyber risks towards OT systems than IT systems. This discrepancy in level of cyber risk perception might be explained by the systems nature and primary functions since administrative systems are more associated with cyber-attacks and security needs than operational systems [26]. Moreover, there is no obligation of reporting maritime cyber-attacks to the authorities, and the fear of reputation loss might deter the shipping companies from reporting cyber incidents [5]. Therefore, if deck officers only rely on the available examples of previous cyber-attacks to inform their risk perceptions, it might lead to an underestimation of cyber risks towards their operational technology [50].

Another aspect concerns how the officers assessed cyber risks when answering the questionnaire. If potential consequences of cyber-attacks towards their vessels operational technology seems somewhat abstract, they might think of probability more than fatal consequences when assessing the level of cyber risk towards OT systems [17]. Media coverage of cyber-attacks with fatal consequences for maritime companies are mostly related to attacks on IT-infrastructure [7]. This could be substantiated with findings indicating that vessels are not perceived as attractive targets for cyber criminals, and that the onboard crew feels in control of their operational technology [19]. Nevertheless, the significant differences in cyber risk perception levels towards IT and OT systems demonstrate the importance of investigating what factors influence these perceptions.

6.2 Factors influencing cyber risk perception

Previous research has explored the predictive power of factors for perceived risk in cyber security. However, it has not been investigated in a maritime context before [8, 11]. It is essential to gain insight into specific contexts where people use technology, as factors explaining perception of risk varies from population to population and from profession to profession [35]. The results of the two regression models in this study show a difference in predictive power and significance of independent variables. This substantiates the notion that deck officers perceive cyber risks differently towards IT- versus OT systems, and that factors influence these perceptions at varying degrees. Knowledge of this will impact how the maritime industry should develop training programs, policies, risk communication and design

technology to improve cyber security behaviour and compliance [18, 59]. The next sub-sections discuss the findings related to perceived benefit, trust, cyber security training and experience and familiarity with cyber-attacks.

6.2.1 Perceived benefit

Both regression models utilised in the analyses demonstrated that perceived benefit significantly enhances deck officers cyber risk perception. Interestingly, this result contrasts with prior research, which often finds an inverse relationship between perceived cyber risk and benefit [15, 40]. When examining the benefit scores presented in Table 2, it is evident that deck officers perceive high levels of benefit for all systems. Moreover, Table 5 show that the mode for perceived benefit across all systems is the maximum value of 55. These observations indicate that perceived benefit towards IT and OT systems are generally high and might be assessed differently in comparison to alternative contexts and other forms of information technology. A possible explanation for this could stem from the operational and demanding working environment aboard vessels [60]. Deck officers rely extensively on both IT and OT systems to perform their work duties in a safe and efficient manner, leaving them with no viable substitutes for these systems [33]. This might coincide with the notion that, when perceived benefit is high enough, users are more inclined to accept a certain level of associated risk [31, 38].

Preceding studies have asked participants to evaluate the specific risks or benefits of activities associated with the technologies in question [15, 33, 61]. It is plausible that the deck officers would assess cyber risks or benefits of specific tasks, such as navigation with radar or communication by email, in a different manner compared to assessing the overall system cyber risks or benefits of radar and email. Nevertheless, it is important to note that the findings indicate a generally high level of perceived system benefits, and that this perception might, to some extent, contribute to an elevation in deck officers' cyber risk perception. By considering this in cyber risk communication and cyber security training programs, it could provide a more balanced perspective of both system benefits, potential risks, and system vulnerabilities. Consequently, this could facilitate more informed decision making regarding cyber risk management and strengthened incident response [4, 59].

6.2.2 Trust

Trust did not emerge as a significant predictor of cyber risk perception towards either IT- or OT systems. In assessing trust towards various stakeholders (comprising the crew, company

management, IT-department, suppliers, government, and IMO) working with securing these systems, the concepts of social trust and confidence were used. Social trust is related to shared intentions and values, and the results may imply that deck officers perceive a lack of alignment in intentions and values between themselves and the stakeholders concerning cyber security matters [35, 58]. Alternatively, it could suggest that the stakeholders are a highly diverse group, making it challenging to identify a collective set of shared values between them.

Confidence, on the other hand, hinges on past experiences over time and the perceived knowledge of stakeholders about the technologies in question [62]. If deck officers have limited cyber security related interactions with the stakeholders, the officers may not have sufficient information or experiences for the development of confidence-based judgements. Overall, the participants might lack substantial positive or negative experience with stakeholders' management of cyber risks towards the onboard systems. This potential absence of experiences to anchor their value and confidence judgements might contribute to the lack of statistically significance of trust.

Furthermore, the divergence between the results observed in this quantitative study and the implications drawn from the previous qualitative study, which underscored the significance of trust in others for cyber defence [19], can be attributed to the complex nature of trust mechanisms. Consequently, trust within maritime cyber security could be evaluated differently regarding value perspectives and importance attributed to stakeholders' knowledge [35, 63]. The results are also influenced by how social trust and confidence were operationalized in the questionnaire. It is possible that the questions did not fully capture the nuances of how deck officers perceive trust in this context, or that trust has an indirect impact on cyber risk perceptions. Future research should explore these trust dynamics and possible correlations comprehensively. Furthermore, it may be worthwhile to investigate the relevance of trust dimensions within security research as well, such as self-efficacy and control, technical trust, and the potential impact of limited personal interaction [64].

6.2.3 Cyber security training

The results show that the amount of cyber security training deck officers receive, positively predicts their cyber risk perception towards OT systems but has no significant impact on their perception of cyber risks towards IT systems. Since knowledge-building within maritime cyber security can be seen as novel, the main part of this training has been theoretical and

focusing on IT-security [19, 26]. However, maritime personnel depend on operational training and drills to ensure effective crisis management aboard vessels [13]. Since operational technology can be deemed more critical to vessels' operations, increased training related to securing this technology may enhance the deck officers' awareness of OT systems vulnerabilities. Together with a focus on good security behaviours and positive stimuli, this training might lead to more compliant security behaviour, reducing the gap between perceived importance of cyber security and actual cyber-practices [24, 65].

Furthermore, the effectiveness of security methods depends on individuals implementing and using them [61], which in turn makes it important how deck officers comprehend the information given to them about potential cyber risks and threats [65]. Previous research show that people tend to react to the effects of cyber-attacks and not the attack itself [18]. Maybe training programs targeting OT systems are more likely to give deck officers tools to comprehend potential consequences of cyber incidents and handle cyber risks more efficiently, which in turn enhances their cyber risk perception. These findings imply the necessity for an evaluation of the content and effectiveness of current cyber security training programs, as well as highlighting the need for tailored training approaches focusing on operational aspects of vessels' cyber security. Consequently, these results open for further exploration of the relationship between cyber risk perception, training, and the specific characteristics of IT and OT systems in the maritime domain.

6.2.4 Experience and familiarity with cyber-attacks

The results regarding deck officers' previous experience and familiarity with cyber-attacks provide insights into how personal experiences and external information might shape their cyber risk perception. Again, the results were significant for predicting cyber risk perception towards OT systems but not for IT systems, which further underpins the difference in factors influencing perception of cyber risks towards information and operational technologies.

The observed increase in cyber risk perception towards OT systems among deck officers who have experienced a cyber-attack towards their own vessel, coincides with previous studies finding that personal experience heightens risk perceptions [17, 66]. This increase might be attributed to the availability heuristic, since people tend to perceive risks as high if they find it easy to recall the occurrence of associated events [32, 48, 50]. Conversely, the significant decrease in cyber risk perception among those with experience of cyber-attacks towards their

shipping company, could reflect a belief in organizational learning and the company's ability to handle another attack [26].

Furthermore, the positive correlation between familiarity of cyber-attacks towards other vessels or shipping companies and cyber risk perception of OT systems show the influence of external information and mass media [48, 49]. This indicates that deck officers' cyber risk perception is not only influenced by their own experiences, but also by cyber incidents within the maritime industry known through storytelling or media. Even so, the official number of cyber-attacks towards OT systems are much lower than towards IT systems [7], making it important to establish reporting systems for maritime cyber incidents and develop effective awareness campaigns and risk communication tools [67]. More statistical data on maritime cyber incidents would further inform deck officers cyber risk perceptions and support decision making related to cyber risk management [5].

6.3 Implications and practical recommendations

Implications drawn from this empirical study pave the way for strategic recommendations to bridge the gap between theory and practice within maritime cyber security. The findings demonstrate the importance of considering the particularities within maritime cyber risk perception and the essential role of the factors influencing these perceptions. Table 12 summarizes the implications as practical recommendations that can empower operational decision makers to enhance their cyber risk management efforts forward.

Table 12
Practical recommendations

Acknowledge the difference between IT and OT systems.	The nature of information and operational technology is different, and this influence cyber risk perceptions. Acknowledgement of this difference can aid the process of implementing and revising cyber risk management strategies.
Increased collaboration between maritime stakeholders.	Increase stakeholders' communications related to cyber security decisions and actions. Emphasize the need for open dialogues, feedback sharing and joint efforts to address cyber risks within the maritime value chain.
Specific risk communication tools for IT and OT systems.	Develop specific risk communication tools for IT and OT systems with strategies that provide relevant and timely information about cyber incidents. Give transparent and contextually rich information about incidents involving vessels, shipping companies and other maritime companies. Focus on rewarding compliance and good security behaviour.
Tailored cyber security training programs with operational focus.	Revise current cyber security training programs to ensure a focus on operational training and OT systems. Consider the importance of continuous training and learning approaches to strengthen management strategies and cyber incident responses.
Cyber incident reporting system.	Work to establish structured incident reporting mechanisms to capture cyber incidents, impacts and lessons learned. More comprehensive data of industry-wide incident trends will support more efficient and accurate decision-support tools for cyber risk assessments.
Substantiated and holistic cyber security policies.	Create holistic policies to substantiate these cyber security recommendations. Highlight the importance of policymaking for enhanced decision making and cyber risk management.

6.4 Limitations

This study has some methodological limitations which must be considered. Since the participants in the sample is working within the offshore segment, it might not be possible to generalize the findings to the broader population of deck officers within the maritime industry. Offshore vessels are technically advanced, using a more diverse range of both IT and OT systems than for example tankers, dry bulk vessels or ferries [52].

The current study has a cross-sectional design, so it only captures a snapshot of participants' perceptions and experiences at a specific point in time. Longitudinal research may better test and assess the stability of cyber risk perceptions over time [53]. Furthermore, when using questionnaires there is the potential for self-reporting bias. This means participants might provide responses they believe to be socially correct or that align with their roles, possibly resulting in the self-reporting measures not fully capturing the participants' actual perceptions or experiences [56]. Other potential biases in this study could be related to the questionnaire wording or how the constructs were measured and operationalized. Future studies should carefully consider how to measure trust, and investigate the causal, and possible confounding, relationship between trust and perceived benefit.

The explanation percentages in both regression models were low, suggesting that other variables might be more important in explaining deck officers cyber risk perception. This could be because people's perception of cyber risks might deviate from their perception of offline risks, e.g., risks related to gene technology and nuclear power. These offline risks can be replaced with other solutions or avoided if preferred, but IT and OT systems are not replaceable and deck officers depend on these technologies to do their job [33]. This distinction between offline and online risks might cause differences in how attitudes and risk responses are developed. Consequently, it is quite plausible that other variables and mechanisms are affecting people's perceptions of risks in cyberspace versus real life.

7 Conclusion

The empirical evidence in this study show that deck officers perceive cyber risks towards information and operational technology differently. Moreover, the varied influence of perceived benefit, trust, cyber security training, and experience with cyber-attacks provide insights into the intricate interplay of variables influencing cyber risk perceptions. The implications of these distinct findings for IT and OT systems calls attention to the necessity of tailored risk communication tools, cyber security training programs, reporting systems, and

holistic cyber security policies within the maritime domain. Future research should analyse the long-term effects of such cyber security interventions, as understanding the causes and effects of the recommended security measures will be crucial.

In conclusion, this study marks a significant stride towards comprehending maritime decision-makers' cyber risk perceptions of technological systems used in highly operational work environments. This previously unexplored perceptive provides an understanding of that human cognition not only distinguishes cyber risks between different contexts but also among different system categories. The hope is that insights provided from this study stimulate further investigations into the complex relationship between human behaviour and maritime technologies within the realm of cyberspace. Capturing a wider understanding of these dynamics will aid in the ongoing efforts to maintain vessel security and safety in this new cyber threat landscape.

Statements and declarations

Funding This study was funded by the Grant from the Research Based Innovation Centre "SFI Marine Operation in Virtual Environment (SFI-MOVE)" by the Norwegian Research Council under Project 237929.

Conflict of interest The authors have no relevant financial or non-financial interests to disclose.

Data availability The datasets generated and analysed during the current study are not publicly available due to individual privacy concerns, but are available from the corresponding author on reasonable request.

References

1. NORMACyber: NORMA Cyber Annual Threat Assessment 2023 (2023). Available from: https://www.normacyber.no/news/48o1qpgi66klzqspdg7jg3kwta3172.
2. Tam K, Jones K.: Situational awareness: Examining factors that affect cyber-risks in the maritime sector (2019). Available from: https://pearl.plymouth.ac.uk/handle/10026.1/14948.
3. DNV: Maritime Cyber Priority 2023 (2023). Available from: https://www.dnv.com/cybersecurity/cyber-insights/maritime-cyber-priority-2023.html.
4. Kuhn K, Bicakci S, Shaikh SA.: COVID-19 digitization in maritime: understanding cyber risks. WMU Journal of Maritime Affairs. 20(2), 193-214 (2021). https://doi.org/10.1007/s13437-021-00235-1

5. Schinas O, Metzger D.: Cyber-seaworthiness: A critical review of the literature. Marine Policy. 151105592 (2023). https://doi.org/10.1016/j.marpol.2023.105592
6. Ben Farah MA, Ukwandu E, Hindy H, Brosset D, Bures M, Andonovic I, et al.: Cyber security in the maritime industry: a systematic survey of recent advances and future trends. Information. 13(1), 22 (2022). https://doi.org/10.3390/info13010022
7. Meland PH, Bernsmed K, Wille E, Rødseth ØJ, Nesheim DA.: A Retrospective Analysis of Maritime Cyber Security Incidents. 519-30 (2021). https://doi.org/10.12716/1001.15.03.04
8. Bolbot V, Kulkarni K, Brunou P, Banda OV, Musharraf M.: Developments and research directions in maritime cybersecurity: A systematic literature review and bibliometric analysis. International Journal of Critical Infrastructure Protection. 39100571 (2022). https://doi.org/10.1016/j.ijcip.2022.100571
9. Kessler GC, Shepard SD.: Maritime Cybersecurity - A Guide for Leaders and Managers. Second Edition ed. Great Britain: Amazon (2022)
10. Erstad E, Ostnes R, Lund MS.: An Operational Approach to Maritime Cyber Resilience. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 1527-34 (2021). https://doi.org/10.12716/1001.15.01.01
11. Larsen MH, Lund MS.: Cyber Risk Perception in the Maritime Domain: A Systematic Literature Review. IEEE Access. 9144895-905 (2021). https://doi.org/10.1109/ACCESS.2021.3122433
12. Erstad E, Lund MS, Ostnes R.: Navigating through cyber threats, a maritime navigator's experience. Applied Human Factors and Ergonomics International (AHFE International). 5384-91 (2022). https://doi.org/10.54941/ahfe1002205
13. Erstad E, Hopcraft R, Vineetha Harish A, Tam K.: A human-centred design approach for the development and conducting of maritime cyber resilience training. WMU Journal of Maritime Affairs. 22(2), 241-66 (2023). https://doi.org/10.1007/s13437-023-00304-7
14. Spencer T.: Risk Perception. Hauppauge: Nova Science Publisher (2016)
15. Van Schaik P, Renaud K, Wilson C, Jansen J, Onibokun J.: Risk as affect: The affect heuristic in cybersecurity. Computers & Security. 90101651 (2020). https://doi.org/10.1016/j.cose.2019.101651
16. Sjöberg L, Moen B-E, Rundmo T.: Explaining risk perception. An evaluation of the psychometric paradigm in risk perception research. Rotunde publikasjoner Rotunde. 8455-76 (2004).
17. Van Schaik P, Jeske D, Onibokun J, Coventry L, Jansen J, Kusev P.: Risk perceptions of cyber-security and precautionary behaviour. Computers in Human Behavior. 75547-59. (2017). https://doi.org/10.1016/j.chb.2017.05.038
18. Bada M, Nurse JR.: The social and psychological impact of cyberattacks. Emerging Cyber Threats and Cognitive Vulnerabilities. Academic Press. 73-92 (2020). https://doi.org/10.1016/B978-0-12-816203-3.00004-6
19. Larsen MH, Lund MS, Bjørneseth FB.: A model of factors influencing deck officers' cyber risk perception in offshore operations. Maritime Transport Research. 3100065 (2022). https://doi.org/10.1016/j.martra.2022.100065
20. Haugli-Sandvik M, Pareliussen B, Bjørneseth FB.: Kommunikasjon og distribuert situasjonsbevissthet i maritime fjernoperasjoner. Nyskaping: Fjordantologien 2023. Universitetsforlaget. 269-85 (2023). https://doi.org/10.18261/9788215069371-23-15
21. Refsdal A, Solhaug B, Stølen K.: Cyber-risk management. Springer. 9-47 (2015). https://doi.org/10.1007/978-3-319-23570-7_5
22. Von Solms R, Van Niekerk J.: From information security to cyber security. Computers & Security. 3897-102 (2013). https://doi.org/10.1016/j.cose.2013.04.004

23. Lee AR, Wogan HP., Editors: All at sea: The modern seascape of cybersecurity threats of the maritime industry. OCEANS 2018 MTS/IEEE Charleston (2018). IEEE.
24. Knight V, Sadok M., Editors: Is cyber-security the new lifeboat? An exploration of the employee's perspective of cyber-security within the cruise ship industry. 7th International Workshop on Socio-Technical Perspective in IS Development (2021). CEUR Workshop Proceedings.
25. Potamos G, Theodoulou S, Stavrou E, Stavrou S., Editors: 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 (2023). Springer.
26. Chubb N, Finn P, Ng D.: The Great Disconnect (2022). Available from: https://safety4sea.com/wp-content/uploads/2022/03/Thetius-hfw-cyberowl-Great-disconnect-cyber-risk-management-2022_03.pdf
27. Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M.: Cybersecurity Challenges in the Maritime Sector. Network. 2(1), 123-38 (2022). https://doi.org/10.3390/network2010009
28. Alcaide JI, Llave RG.: Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia. 45547-54 (2020). https://doi.org/10.1016/j.trpro.2020.03.058
29. Slovic P.: Perception of risk: Reflections on the psychometric paradigm. Theories of Risk. New York, Praeger (1990)
30. Kahneman D, Slovic SP, Slovic P, Tversky A.: Judgment under uncertainty: Heuristics and biases. Cambridge university press (1982)
31. Fischhoff B, Slovic P, Lichtenstein S, Read S, Combs B.: How safe is safe enough? A psychometric study of attitudes towards technological risks and benefits. Policy sciences. 9(2), 127-52 (1978). https://doi.org/10.1007/BF00143739
32. Siegrist M, Árvai J.: Risk perception: Reflections on 40 years of research. Risk Analysis. 40(S1), 2191-206 (2020). https://doi.org/10.1111/risa.13599
33. Sjöberg L, Fromm J.: Information technology risks as seen by the public. Risk Analysis. 21(3), 427-42 (2001). https://doi.org/10.1111/0272-4332.213123
34. Siegrist M, Keller C, Kiers HA.: A new look at the psychometric paradigm of perception of hazards. Risk Analysis: An International Journal. 25(1), 211-22 (2005). https://doi.org/10.1111/j.0272-4332.2005.00580.x
35. Siegrist M.: Trust and risk perception: A critical review of the literature. Risk analysis. 41(3), 480-90 (2021). https://doi.org/10.1111/risa.13325
36. Slovic P.: Perception of risk. Science. 236(4799), 280-5 (1987). https://doi.org/10.1126/science.3563507
37. Starr C.: Social benefit versus technological risk. Science. 1232-8 (1969)
38. LeBlanc D, Biddle R., Editors: Risk perception of internet-related activities. 2012 Tenth Annual International Conference on Privacy, Security and Trust (2012). IEEE.
39. Farahmand F, Spafford EH.: Understanding insiders: An analysis of risk-taking behavior. Information systems frontiers. 15(1), 5-15 (2013). https://doi.org/10.1007/s10796-010-9265-x
40. Frewer LJ, Howard C, Shepherd R.: Understanding public attitudes to technology. Journal of Risk Research. 1(3), 221-35 (1998). https://doi.org/10.1080/136698798377141
41. Siegrist M, Cvetkovich G, Roth C.: Salient value similarity, social trust, and risk/benefit perception. Risk analysis. 20(3), 353-62 (2000). https://doi.org/10.1111/0272-4332.203034

42. Rousseau DM, Sitkin SB, Burt RS, Camerer C.: Not so different after all: A cross-discipline view of trust. Academy of management review. 23(3), 393-404 (1998). https://doi.org/10.5465/amr.1998.926617
43. Earle TC, Siegrist M.: On the relation between trust and fairness in environmental risk management. Risk Analysis: An International Journal. 28(5), 1395-414 (2008). https://doi.org/10.1111/j.1539-6924.2008.01091.x
44. Van Kleef E, Fischer AR, Khan M, Frewer LJ.: Risk and benefit perceptions of mobile phone and base station technology in Bangladesh. Risk Analysis: An International Journal. 30(6), 1002-15 (2010). https://doi.org/10.1111/j.1539-6924.2010.01386.x
45. Siegrist M, Earle TC, Gutscher H.: Test of a trust and confidence model in the applied context of electromagnetic field (EMF) risks. Risk Analysis: An International Journal. 23(4), 705-16 (2003). https://doi.org/10.1111/1539-6924.00349
46. Visschers VH, Siegrist M.: How a nuclear power plant accident influences acceptance of nuclear power: Results of a longitudinal study before and after the Fukushima disaster. Risk Analysis: An International Journal. 33(2), 333-47 (2013). https://doi.org/10.1111/j.1539-6924.2012.01861.x
47. Slovic P.: Perceived risk, trust, and democracy. Risk analysis. 13(6), 675-82 (1993). https://doi.org/10.1111/j.1539-6924.1993.tb01329.x
48. Kahneman D.: Thinking, fast and slow. Macmillan (2011)
49. Tversky A, Kahneman D.: Judgment under Uncertainty: Heuristics and Biases: Biases in judgments reveal some heuristics of thinking under uncertainty. Science. 185(4157), 1124-31 (1974). https://doi.org/10.1126/science.185.4157.1124
50. De Smidt G, Botzen W.: Perceptions of corporate cyber risks and insurance decision-making. The Geneva Papers on Risk and Insurance-Issues and Practice. 43(2), 239-74 (2018). https://doi.org/10.1057/s41288-018-0082-7
51. Tversky A, Kahneman D.: Availability: A heuristic for judging frequency and probability. Cognitive psychology. 5(2), 207-32 (1973). https://doi.org/10.1016/0010-0285(73)90033-9
52. Karan C.: What are Offshore Vessels?. Marine Insight (2019). Available from: https://www.marineinsight.com/types-of-ships/what-are-offshore-vessels/. Last accessed: 07.08.23
53. Field A.: Discovering statistics using IBM SPSS statistics 5ed. London. Sage Publications Ltd. (2018)
54. Gulbrandsen A.: Informasjonssikkerhet og risikovurdering for Nettskjema. University of Oslo (2017). Available from: https://www.uio.no/tjenester/it/adm-app/nettskjema/mer-om/informasjonssikkerhet/. Last accessed: 02.08.23
55. IMO: Women in Maritime (2023), Available from: https://www.imo.org/en/ourwork/technicalcooperation/pages/womeninmaritime.aspx. Last accessed: 07.08.23
56. Ringdal K.: Enhet og Mangfold. 4 ed. Bergen: Fagbokforlaget (2018)
57. Diamantopoulos A, Winklhofer HM.: Index construction with formative indicators: An alternative to scale development. Journal of marketing research. 38(2), 269-77 (2001). https://doi.org/10.1509/jmkr.38.2.269.188
58. Siegrist M.: The influence of trust and perceptions of risks and benefits on the acceptance of gene technology. Risk analysis. 20(2), 195-204 (2000). https://doi.org/10.1111/0272-4332.202020
59. Farahmand F, Dark M, Liles S, Sorge B., Editors: Risk perceptions of information security: A measurement study. 2009 International Conference on Computational Science and Engineering (2009). IEEE.

60. Hystad S, Nielsen M, Eid J.: The impact of sleep quality, fatigue and safety climate on the perceptions of accident risk among seafarers. European review of applied psychology. 67(5), 259-67 (2017). https://doi.org/10.1016/j.erap.2017.08.003
61. Huang D-L, Rau P-LP, Salvendy G.: Perception of information security. Behaviour & Information Technology. 29(3), 221-32 (2010). https://doi.org/10.1080/01449290701679361
62. Earle TC, Siegrist M, Gutscher H.: Trust, Risk Perception and the TCC Model of Cooperation 1. Trust in cooperative risk management. Routledge. 1-50 (2012)
63. Earle TC.: Trust in risk management: A model-based review of empirical research. Risk Analysis: An International Journal. 30(4), 541-74 (2010). https://doi.org/10.1111/j.1539-6924.2010.01398.x
64. Flowerday S, Von Solms R., Editors: Trust: An element of information security. IFIP International Information Security Conference (2006). Springer.
65. He W, Zhang Z.: Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce. 29(4), 249-57 (2019). https://doi.org/10.1080/10919392.2019.1611528
66. Kostyuk N, Wayne C.: The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. Journal of Global Security Studies. 6(2), ogz077 (2021). https://doi.org/10.1093/jogss/ogz077
67. Tsohou A, Karyda M, Kokolakis S.: Analyzing the role of cognitive and cultural biases in the internalization of information security policies: Recommendations for information security awareness programs. Computers & security. 52128-41 (2015). https://doi.org/10.1016/j.cose.2015.04.006

Appendix

Questionnaire with wording, sequence of questions and options:

Variables	Information and question wording	Scaled items	Options/Scales with values in dataset
Age			19-29 30-39 40-49 50-59 60-69
Gender			Male Female Other/ Do not want to say
Rank	What is your current rank?		Captain. Chief mate. Second mate.
Sailing years	How many years of sailing experience do you have?		Free text reply
Education	What education do you have?		Vocational school Bachelor's degree Master's degree
Perceived benefit	As deck officer, you depend on technological systems in your everyday working life. Consider the level of benefit the systems below have for conducting your job.	Power management systems (PMS). E-mail. Electronic Chart Display and Information System (ECDIS). Radar. Passenger servicing and	1. Very low benefit 2. 3. 4. 5. Very high benefit 0. Don't know/Don't use this

	On a scale from one to five, where five is very high benefit, how do you assess the benefits of the following systems for your job as a deck officer?	management systems. Remote access for maintenance. Dynamic Position System (DP-system). Client reporting systems. Remote access for monitoring. SafeSeaNet. Cargo and loading management systems. Internal reporting system.	
Experience with cyber-attacks	How many times have you experienced a cyber-attack towards any of the vessels you have worked on? How many times have you experienced a cyber-attack towards shipping companies you have worked for? How many times have you heard about other shipping companies or vessels being victim of a cyber-attack?		1. Never 2. One time 3. A few times (about 2-5) 4. Many times (6+ times) 0. I don't know
Cyber security training	How often have you conducted the following cyber security training?	Computer based training (E.g., Seagull CBT). External course. Internal course. Security drills. Tabletops. Phishing campaigns on email. Awareness campaigns on email. Another form for cyber security training.	1. Never 2. Once 3. Yearly 4. Twice a year 5. Monthly 0. I don't know
Perceived cyber risk	Cyber risks are caused by threats like malicious software or hackers. These threats exploit cyberspace and may cause cyber incidents towards the systems on board your vessel. On a scale from one to five, where five is very high risk, how do you assess the cyber risks towards the following systems?	Power management systems (PMS). E-mail. Electronic Chart Display and Information System (ECDIS). Radar. Passenger servicing and management systems. Remote access for maintenance. Dynamic Position System (DP-system). Client reporting systems. Remote access for monitoring. SafeSeaNet. Cargo and loading management systems. Internal reporting system.	1. Very low cyber risk 2. 3. 4. 5. Very high cyber risk 0. Don't know/Don't use this
Confidence	Consider your level of trust in the institution or persons competence to perform the cyber security related tasks they are responsible for. What is your level of trust in the following institutions or persons ability to contribute to the	Your crew. Management in your shipping company. IT-department in your shipping company. Suppliers of onboard systems. Government. IMO (International Maritime Organization).	1. No trust at all 2. 3. 4. 5. Very high trust

	securing of the onboard systems against cyber risks?		
Social trust	Consider your level of trust in that the institutions or persons don't want to harm you, but are acting in your best interest when performing the cybersecurity tasks they are responsible for. What is your level of trust in the following institutions or persons that they are acting in your best interest when it comes to securing the onboard systems against cyber risks?	Your crew. Management in your shipping company. IT-department in your shipping company. Suppliers of onboard systems. Government. IMO (International Maritime Organization).	1. No trust at all 2. 3. 4. 5. Very high trust

Appendix 1: Protocol systematic literature review

PROTOCOL LITERATURE REVIEW (2021)

This literature review is planned and executed following *A guide to conducting a systematic literature review of information systems research* by Okoli and Schabram (2010). The current document reflects the planning and execution of the eight steps in the guide and will be presented under the phases of planning, selection, extraction, and execution.

PLANNING

1. Purpose of the literature review

This literature review is a part of the PhD project "Perception of cyber risks in offshore operations" and will answer the following research question: What is the current state of research in the field of cyber risk perception in general and in the maritime domain specifically?

To do this, the literature review will answer the following sub-questions:

Question 1: What are the main dimensions within the psychometric paradigm and the cognitive biases related to cyber risk perception?

Question 2: What is the current state of research within the field of maritime cyber risk perception, and what recommendations can be given to advance research within this field?

2. Protocol and training

This protocol is the result of planning and training and will be used as a dynamic tool throughout the process of working with this SLR.

SELECTION

3. Searching for the literature

To search for literature, digital databases accessible to the researcher were chosen as the main sources of information. The chosen databases reflect the multidisciplinary nature of this literature review, which includes research fields such as psychology, behavioural science, social science, information security/cybersecurity, engineering, economy, and health science.

Chosen databases:

- SpringerLink
- Science direct
- PsycINFO
- Web of Science

- SAGE journals
- IEEE Xplore: digital library
- EBSCO (Academic Search Complete, CINAHL Complete, EconLit with Full Text, Psychology and Behavioral Sciences Collection, Sociology Source Ultimate)
- Taylor & Francis Online

Key words used in the search:

- Risk perception
- Cyber threat
- Cyber risk
- Cyber security
- Information security
- Security risk
- Risk
- Maritime
- Marine
- Offshore
- Cyberpsychology
- Policy

The researcher decided to limit the use of Boolean Operators to AND. The search strings including the key words were as follows:

- “Risk perception” AND “security risk” AND “information security”
- “Risk perception” AND “cyber risk” AND “cyber security”
- “Risk perception” AND “cyber threats”
- “Risk perception” AND “risk” AND “information security”
- “Risk perception” AND “risk” AND “cyber security”
- “Perception of cyber risk”
- “Maritime” AND “security” AND “risk perception” AND “information”
- “Perception of risk” AND “cyber risk”
- “Perception of risk” AND “cyber threats”
- “Cyber risk” AND “risk perception” AND “policy”
- “Maritime” AND “information security” AND “risk” AND “perception”
- “Risk perception” AND “information security”
- “Maritime” AND “information security” AND “risk perception”
- “Marine” AND “cyber risk” AND “risk perception”
- “Risk perception” AND “cyber security”
- “Maritime” AND “cyber risk”
- “Offshore” AND “cyber risk” AND “risk perception”
- “Offshore” AND “cyber security” AND “risk perception”
- “Cyberpsychology” AND “risk perception” AND “cyber”

- “Cyberpsychology” AND “risk” AND “perception”
- “Cyberpsychology” AND “risk perception” AND “information security”

4. Practical screening (screening for inclusion)

Inclusion and exclusion criteria used to evaluate which papers should be included:

- Risk perception research within the psychometric paradigm, or research developed from this paradigm
- Broad review of perception of cyber risks/security risks
- No limited period
- Peer-reviewed articles in English
- Both journal articles and conference papers
- The paper must be peer-reviewed and published in a conference proceeding or journal.
- The paper must contain research related to perception of cyber risks.
- The paper must be written in English.
- Grey literature, such as blogs and government documents, are not assessed.

EXTRACTION

5. Quality appraisal (screening for exclusion)

For the list of potential papers, the following criteria should be used to ensure quality:

- The paper must present empirical data related to risk perception research within the psychometric paradigm, research developed within this paradigm, or research related to cognitive biases and risk perception.
- Papers focusing on risk perception research within other theoretical frameworks than the psychometric paradigm, such as protection motivation theory, are not included.
- Papers focusing on gender or geographical factors are not included.
- The purpose of the paper must be within the following categories:
    - How policies should be outlined
    - Risk communication
    - Risk mitigation measures or demand for risk mitigation
    - Prediction of security behaviour

6. Data extraction

When the final list of papers is ready, information should be systematically taken from each article to serve as the raw material for the synthesis stage. The following are proposed categories for the data extraction:

- Context data: Information about the purpose of the study
- Methodology: Information about methodology and data collection methods
- Research questions: The research questions or hypothesis outlined in the study
- Qualitative data: Findings and conclusions relevant for this SLR’s research questions

EXECUTION

7. Analysis of findings

The studies collected in this review will consist of both quantitative and qualitative analyses and will be analysed by conducting a qualitative synthesis. This will be the foundation for the result section in the literature review.

8. Writing the review

Purposed structure of the review:

- Title
- Authorship
- Executive summary or structured abstract
    - Context, objectives, methods, results, conclusions
- Background
    - Justification of the need for the review
- Review questions
- Review methods
    - Data sources and search strategy, study selection, study quality assessment, data extraction, data synthesis
- Included and excluded studies
    - Inclusion and exclusion criteria, list of excluded studies with rationale for exclusion
- Results
- Discussion
    - Principal findings, strength and weaknesses, meaning of findings
- Conclusions and recommendations
- Acknowledgements
- References and appendices

Appendix 2: Interview guide

Theme	Interview questions
Information before tape recording	Talk about the topic of conversation (background, purpose). Explain what the interview will be used for, the interviewee's rights, confidentiality, and anonymity. Ask if anything is unclear, and if the interviewee has any questions. Inform, obtain consent, and start the recording.
Personal information	Education. Years of experience at sea. Current position and type of vessel.
Cyber risk	What do you think of when I say cyber risks at sea?
Experience with cyber incidents	Can you tell me about a cyber incident that you have experienced at work? Do you have any thoughts on what a cyber incident on your vessel might be? Have you heard about other vessels experiencing a cyber threat?
Procedures and training	In what way do you work with cybersecurity on board your vessel? What actions should be taken if a cyber incident occurs? How do you think other vessels and shipping companies work with cybersecurity?
Crew/organisation/shipping company	Do you find that your crew are concerned about how on-board systems can be prone to cyber risks? How does the shipping company communicate with you about cybersecurity and potential cyber risks?
Cyber risk in operation	How do you experience the risk of a cyber incident occurring during an operation? Do you have any thoughts about what may affect your perception of cyber risks at work?
Connectivity on board	In what way can you use your own devices on board? Is the shipping company concerned about what is important for the crew regarding access to the internet? Do you think there are any challenges associated with using your own devices on board?
Summary	Is there anything you are especially concerned about regarding the topics we have talked about? Why is this important? What should/could be done? Quickly summarise the interview, and ask if I have understood the interviewee correctly and if they have anything to add.

Appendix 3: Sikt assessment of processing of personal data

Sikt

Notification form / Cyberrisiko i Offshoreoperasjoner / Assessment

Assessment of processing of personal data

Reference number	Assessment type	Date
673927	Standard	03.09.2020

Title
Cyberrisiko i Offshoreoperasjoner

Data controller (institution responsible for the project)
Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Project leader
Marie Haugli Larsen

Project period
21.09.2020 - 30.09.2023

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 30.09.2023.

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 03.09.2020, samt i meldingsdialogen mellom innmelder og NSD. 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 30.09.2023.

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 viderebehandles 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 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 eventuelt rådføre dere med behandlingsansvarlig institusjon.

OPPFØLGING AV PROSJEKTET
NSD vil følge opp underveis (hvert annet år) og ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet/pågår i tråd med den behandlingen som er dokumentert.

Lykke til med prosjektet!

Kontaktperson hos NSD: Maren Urheim
Tlf. Personverntjenester: 55 58 21 17 (tast 1)

Sikt

Notification form / Cyberrisiko i Offshoreoperasjoner / Assessment

Assessment of processing of personal data

Reference number	Assessment type	Date
673927	Standard	10.10.2022

Title
Cyberrisiko i Offshoreoperasjoner

Data controller (institution responsible for the project)
Norges teknisk-naturvitenskapelige universitet / Fakultet for ingeniørvitenskap / Institutt for havromsoperasjoner og byggteknikk

Project leader
Marie Haugli Larsen

Project period
21.09.2020 - 31.12.2024

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 31.12.2024.

Notification Form

Comment
Personvernombudet har vurdert endringen registrert 21.9.2022.

Vi har registrert at ny sluttdato for behandlingen av personopplysninger er 31.12.2024 (tidligere 30.9.2022).

Prosjektet skulle opprinnelig vare i tre år, og prosjektperioden forlenges med dette til noe over fire år. Personopplysningene er av lite omfang og lav grad av sensitivitet, og det er til dels tatt høyde for forsinkelser i informasjonsskrivet («skal etter planen innen utgangen av september 2023»). Alt tatt i betraktning, vurderer vi at forlengelsen må antas å falle innenfor deltakernes rimelige forventninger, og at behandlingen av personopplysningene kan fortsette med grunnlag i innhentede samtykker. Vi bemerker at dersom det blir aktuelt med ytterligere forlengelse, må det påregnes å gi oppdatert informasjon til de registrerte.

Det er dermed 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. Behandlingen kan fortsette.

OPPFØLGING AV PROSJEKTET
Vi vil følge opp ved planlagt avslutning for å avklare om behandlingen av personopplysningene er avsluttet.

Lykke til videre med prosjektet!

Appendix 4: Information sheet and consent form

Request for participation in the research project "Cyber risk in offshore operations"

This is an inquiry requesting you to participate in a research project to recount your experiences with the above topic. This letter provides information about the aim of the project and what participation will mean for you.

Background and purpose
In this study, I hope to find out how deck officers experience cyber risk in offshore operations. Therefore, I would like to interview deck officers to gain knowledge about their experiences related to this topic.

The project is a doctoral thesis, to be completed at the Institute for Ocean Operations and Construction Engineering at NTNU in Ålesund.

Who is responsible for the research project?
NTNU in Ålesund is responsible for the project.

Why are you being asked to participate?
You are being asked to participate because you are in the target group for this research project. You can participate in the study if you are a sailing deck officer offshore.

What does participating mean for you?
I will conduct an interview with you that will take approx. 30–60 minutes. This interview is intended as a conversation in which you can talk freely about your experiences related to the above topic. The questions focus on your experience and what you are interested in. Our conversation will be audio-recorded.

Participation is voluntary
Participation in the project is voluntary. If you choose to participate, you can withdraw your consent at any time without giving any reason. There will be no negative consequences for you if you do not want to participate or later choose to withdraw.

Your privacy: how I store and use your information
I will only use the information about you for the purposes that I have described in this statement. I process the information confidentially and in accordance with privacy regulations.

The information from you, as well as from the other interviewees, will only be used as basic material in my doctoral thesis. Personal information will be kept separate from other data, and only I will have access to it. The audio recording and transcription will be password-protected and stored on an external hard drive, which will be kept securely. In working with the data, I will use fictitious names for interviewees. It will not be possible to recognise you in the finished publication.

What happens to your information when I end the research project?
The project is scheduled to be completed by the end of September 2023. All data will then be deleted, and printed interviews will be shredded.

Your rights
As long as you can be identified in the data material, you have the right to:

- access personal data registered about you;
- have personal data about you corrected;
- have personal data about you deleted;
- be given a copy of your personal data (data portability); and
- send a complaint to the data protection officer or the Norwegian Data Protection Authority about the processing of your personal data.

What gives me the right to process personal data about you?
We process information about you based on your consent.

On behalf of NTNU, the NSD – Norwegian Center for Research Data AS has assessed that the processing of personal data in this project is in accordance with the privacy regulations.

Where can you find out more?
If you have questions about the study or wish to make use of your rights, please contact:

- Frøy Birte Bjørneseth (supervisor), NTNU in Ålesund, telephone: 99535333 or email: froy.b.bjornseth@ntnu.no
- Marie Haugli Larsen (PhD candidate), telephone: 45061300 or email: marie.h.larsen@ntnu.no
- Our data protection officer: Thomas Helgesen, telephone: 93079038
- NSD – Norwegian Center for Research Data AS, telephone: 55582117 or email: personvernombudet@nsd.no or.

Best regards,

Marie Haugli Larsen

Declaration of consent

I have received and understood the information about the project *"*Cyber risk in offshore operations" and have had the opportunity to ask questions. I agree to:

☐ to participate in the interview survey

I agree to my data being processed until the project is finished at approximately the end of September 2023.

(Signed by project participant, date)

Appendix 5: Online questionnaire

Cybersikkerhet på offshoreskip

Language *

- ◯ Norwegian (Bokmål)
- ◯ English

Information about research project and consent to participate

Background and purpose

The purpose of this study is to map:

- Benefits of onboard systems.
- Cyber security training.
- Cyber risks towards systems on offshore vessels
- Trust in others related to system security.

The survey takes approx. 5 minutes to finish, and you will be asked to give your opinion (it is not a knowledge test).

This study is part of a doctoral thesis, to be completed at the Department of Ocean Operations and Civil Engineering at NTNU in Ålesund.

Why are you asked to participate?

The target group of this project is deck officers working offshore.

Your privacy

This survey is anonymous, and your answers can not be traced back to you.

It is voluntary to participate in this survey.

If you have questions, please contact:

Marie Haugli-Sandvik, phone: 45061300 or email: marie.h.sandvik@ntnu.no

I have read and understood the information about this research project. *

- ◯ I consent to participate in this survey

Are you currently working as a deck officer on a vessel in the offshore industry? *

- ◯ Yes
- ◯ No

Age *

- ○ 19-29
- ○ 30-39
- ○ 40-49
- ○ 50-59
- ○ 60-69

Gender *

- ○ Male
- ○ Female
- ○ Other/ Do not want to say

What is your current rank? *

- ○ Captain
- ○ Chief mate
- ○ First mate
- ○ Second mate
- ○ Third mate

How many years of sailing experience do you have?

[ ]

What education do you have? (Multiple answers possible) *

- ☐ Vocational school
- ☐ Bachelor's degree
- ☐ Master's degree

System benefits

As deck officer, you depend on technological systems in your everyday working life. Consider the level of benefit the systems below have for conducting your job.

How do you assess the benefits of the following systems for your job as a deck officer?

	1 No benefit at all	2	3	4	5 Very high benefit	Don't know/Don't use this
Power management systems (PMS) *	○	○	○	○	○	○
E-mail *	○	○	○	○	○	○
ECDIS (Electronic Chart Display and Information System) *	○	○	○	○	○	○
Radar *	○	○	○	○	○	○
Passenger servicing and management systems *	○	○	○	○	○	○
Remote access for maintenance *	○	○	○	○	○	○
Dynamic Position System (DP) *	○	○	○	○	○	○
Client reporting systems *	○	○	○	○	○	○
Remote access for monitoring *	○	○	○	○	○	○
SafeSeaNet *	○	○	○	○	○	○
Cargo and loading management systems *	○	○	○	○	○	○
Internal reporting systems *	○	○	○	○	○	○

Experience with cyber attacks

How many times have you experienced a cyber-attack towards any of the vessels you have worked on? *

- ○ Never
- ○ One time
- ○ A few times (about 2-5)
- ○ Many times (6+ times)
- ○ I don't know

How many times have you experienced a cyber-attack towards shipping companies you have worked for? *

- ○ Never
- ○ One time
- ○ A few times (about 2-5)
- ○ Many times (6+ times)
- ○ I don't know

How many times have you heard about other shipping companies or vessels being victim of a cyber-attack? *

- ○ Never
- ○ One time
- ○ A few times (about 2-5)
- ○ Many times (6+ times)
- ○ I don't know

Cyber security training

How often have you conducted the following cyber security training?

	Never	Once	Yearly	Twice a year	Monthly	I don't know
Computer based training (E.g. Seagull CBT) *	○	○	○	○	○	○
External course *	○	○	○	○	○	○
Internal course *	○	○	○	○	○	○
Security drills *	○	○	○	○	○	○
Tabletops *	○	○	○	○	○	○
Phishing campaigns on email *	○	○	○	○	○	○
Awareness campaigns on email *	○	○	○	○	○	○
Another form for cyber security training *	○	○	○	○	○	○

If you have recieved another form for cyber security training, what training was that?

Cyber risks towards onboard systems

Cyber risks is caused by threats like malicious software or hackers. These threats exploits cyberspace, and may cause cyber incidents towards the systems on board your vessel.

On a scale from one to five, where five is very high risk, how do you assess the cyber risks towards the following systems?

	1 No cyber risk at all	2	3	4	5 Very high cyber risk	Don't know/Don't use this
Power management systems (PMS) *	○	○	○	○	○	○
E-mail *	○	○	○	○	○	○
ECDIS (Electronic Chart Display and Information System) *	○	○	○	○	○	○
Radar *	○	○	○	○	○	○
Passenger servicing and management systems *	○	○	○	○	○	○
Dynamic Position System (DP) *	○	○	○	○	○	○
Remote access for maintenance *	○	○	○	○	○	○
Client reporting systems *	○	○	○	○	○	○
Remote access for monitoring *	○	○	○	○	○	○
SafeSeaNet *	○	○	○	○	○	○
Cargo and loading management systems *	○	○	○	○	○	○
Internal reporting systems *	○	○	○	○	○	○

Trust in cyber security competence

Consider your level of trust in the institution or persons competence to perform the cyber security related tasks they are responsible for.

What is your level of trust in the following institutions or persons ability to contribute in the securing of the onboard systems against cyber risks?

	1 No trust at all	2	3	4	5 Very high trust
Your crew *	○	○	○	○	○
Management in your shipping company *	○	○	○	○	○
IT-department in your shipping company *	○	○	○	○	○
Suppliers of onboard systems *	○	○	○	○	○
Government *	○	○	○	○	○
IMO (International Maritime Organization) *	○	○	○	○	○

Trust to act in your best interest

Consider your level of trust in that the institutions or persons don't want to harm you, but are acting in your best interest when performing the cybersecurity tasks they are responsible for.

What is your level of trust in the following institutions or persons that they are acting in your best interest when it comes to securing the onboard systems against cyber risks?

	1 No trust at all	2	3	4	5 Very high trust
Your crew *	○	○	○	○	○
Management in your shipping company *	○	○	○	○	○
IT-department in your shipping company *	○	○	○	○	○
Suppliers of onboard systems *	○	○	○	○	○
Government *	○	○	○	○	○
IMO (International Maritime Organization) *	○	○	○	○	○

Indicate how much you agree or disagree with the statements below

	1 Strongly disagree	2	3	4	5 Strongly agree
The management in my shipping company are focused on cyber security. *	○	○	○	○	○
The IT-department implements necessary cyber security measures on board my vessel. *	○	○	○	○	○
Suppliers are very concerned about the cyber security of the systems they provide. *	○	○	○	○	○
My crew is concerned about cyber security. *	○	○	○	○	○
The employees in my shipping company have sufficient cyber security training. *	○	○	○	○	○
I have sufficient knowledge to handle a cyber incident on board my vessel. *	○	○	○	○	○

ISBN 978-82-326-7694-1 (printed ver.)
ISBN 978-82-326-7693-4 (electronic ver.)
ISSN 1503-8181 (printed ver.)
ISSN 2703-8084 (online ver.)

NTNU

Norwegian University of
Science and Technology