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]:

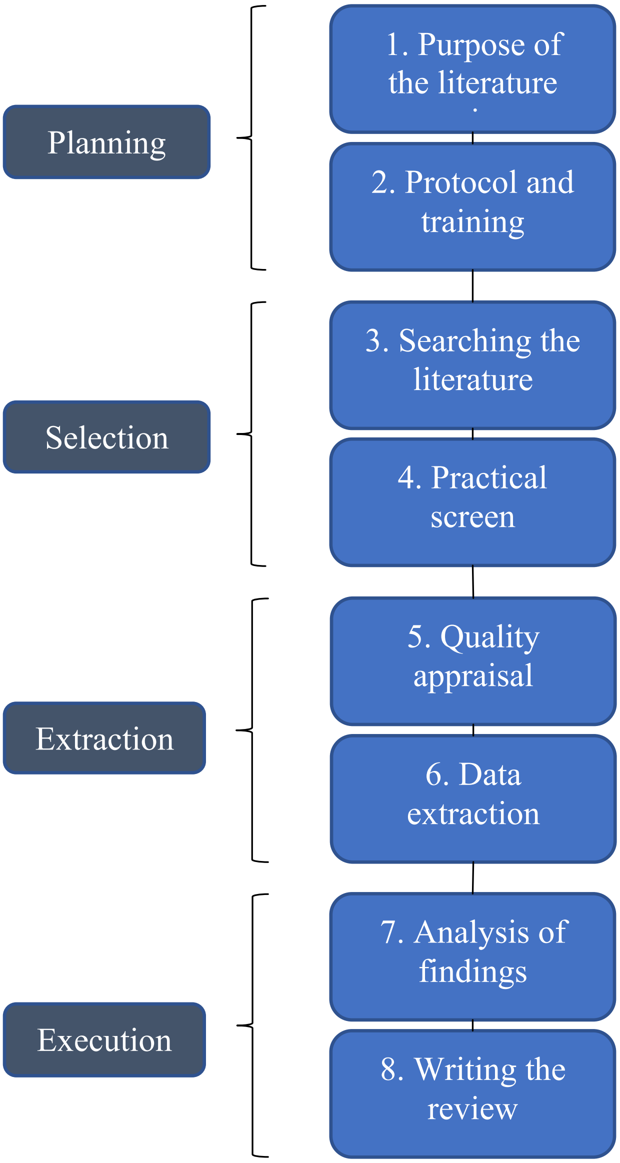

FIGURE 1. A systematic guide to literature review development [52].

- 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].

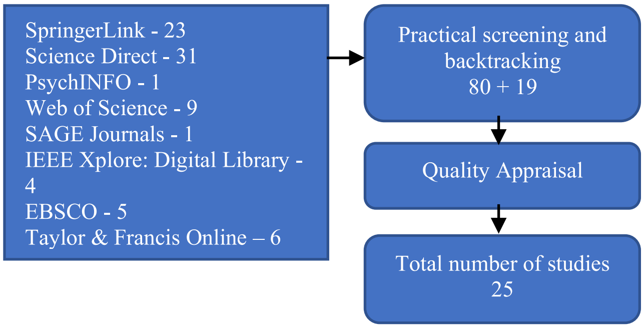
SpringerLink - 23
Science Direct - 31
PsychINFO - 1
Web of Science - 9
SAGE Journals - 1
IEEE Xplore: Digital Library - 4
EBSCO - 5
Taylor & Francis Online – 6
Practical screening and backtracking 80 + 19
Quality Appraisal
Total number of studies 25

FIGURE 2. Selection process of papers.

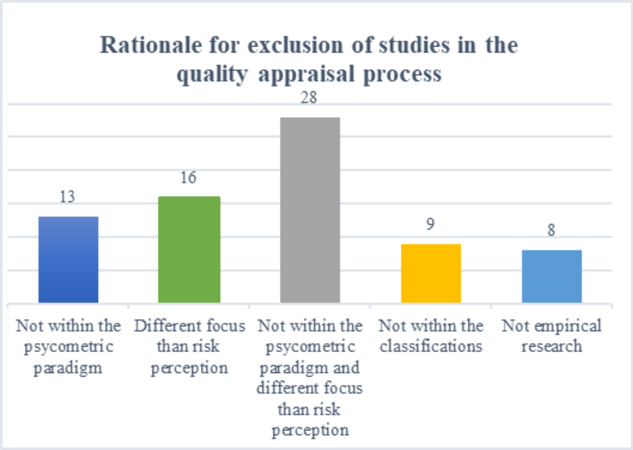

FIGURE 3. Rationale for exclusion of studies in the quality appraisal process.

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

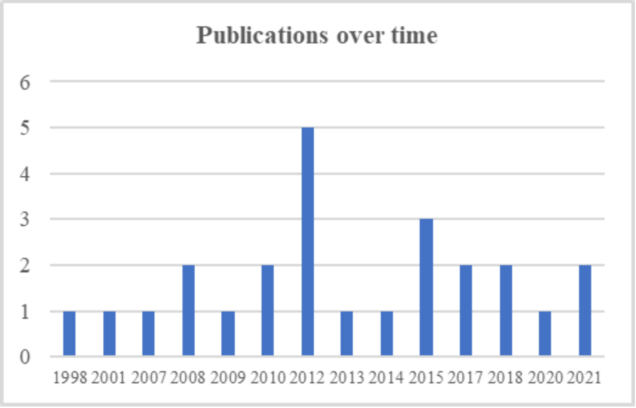

FIGURE 4. Number of papers published over time.

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]

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].

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.