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 Knowledge of maritime cyber security Communication of cyber risks Trust in suppliers	Trust in others for cyberdefence

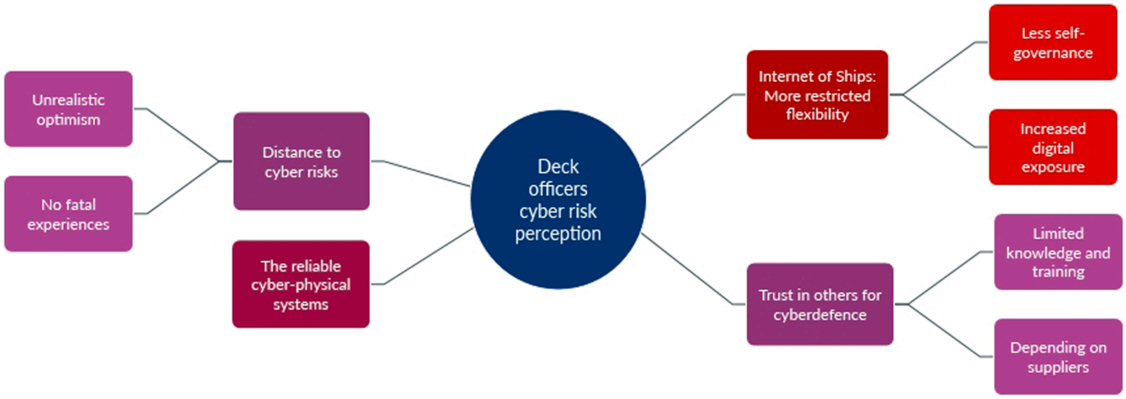
Unrealistic optimism
No fatal experiences
Distance to cyber risks
The reliable cyber-physical systems
Deck officers cyber risk perception
Internet of Ships: More restricted flexibility
Less self-governance
Increased digital exposure
Trust in others for cyberdefence
Limited knowledge and training
Depending on 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 D-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.