Human Factors in Cybersecurity, Vol. 53, 2022, 84–91
https://doi.org/10.54941/ahfe1002205

Navigating Through Cyber Threats, A Maritime Navigator's Experience

Erlend Erstad[1], Mass Soldal Lund[2,3], and Runar Ostnes[1]

[1]Norwegian University of Science and Technology, Ålesund, Norway
[2]Inland Norway University of Applied Sciences, Rena, Norway
[3]Norwegian Defence University College, Lillehammer, Norway

ABSTRACT

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

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

INTRODUCTION

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

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

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

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

FINDINGS

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

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

The Digital Era

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

Table 1. Categories and sub-categories.

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

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

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

What is Actually a Cyber Threat?

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

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

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

Improvised Coping Strategies Towards Cyber Threats

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

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

The Unaddressed Cyber Issue

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

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

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

The Complex Nature of Consequences

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

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

DISCUSSION

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

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

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

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

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

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

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

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

CONCLUSION

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

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

ACKNOWLEDGMENT

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

REFERENCES

Bainbridge, L. 1983. Ironies of automation. *Analysis, design and evaluation of man–machine systems*. Elsevier.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. & Bellekens, X. 2022. Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends. *Information,* 13, 22.

Creswell, J. W. & Poth, C. N. 2018. *Qualitative inquiry & research design : choosing among five approaches,* Thousand Oaks, Calif, Sage.

Erstad, E., Ostnes, R. & Lund, M. S. 2021. An Operational Approach to Maritime Cyber Resilience. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation,* 15, 27–34.

Hareide, O. S., Jøsok, Ø., Lund, M. S., Ostnes, R. & Helkala, K. 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation,* 71, 1025–1039.

IMO, I. M. O. 2012. Operational Use if Electronic Chart Display and Information Systems (ECDIS). *Model Course 1.27 (2012 Edition)*. London.

IMO, I. M. O. 2017a. *International Convention on standards of Training and Watchkeeping for Seafarers (STCW) 1978, consolidated edition 2017*.

IMO, I. M. O. 2017b. Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems.

ISO, I. 2019. 9241-210: 2019 Ergonomics of human-system interaction. *Part 210: Human-Centred Design for Interactive Systems*.

Kessler, G. C. & Shepard, S. D. 2020. *Maritime Cybersecurity: A Guide for Leaders and Managers,* Daytona Beach, Kessler & Shepard.

Lützhöft, M., Grech, M. R. & Porathe, T. 2011. Information Environment, Fatigue, and Culture in the Maritime Domain. *Reviews of Human Factors and Ergonomics,* 7, 280–322.

Malterud, K. 2012. Systematic text condensation: A strategy for qualitative analysis. *Scand J Public Health,* 40, 795–805.

Meland, P., Bernsmed, K., Wille, E., Rødseth, Ø. & Nesheim, D. 2021. A Retrospective Analysis of Maritime Cyber Security Incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*.

Refsdal, A., Solhaug, B. & Stølen, K. 2015. Cyber-risk management. *Cyber-Risk Management*. Springer.

Tam, K. & Jones, K. 2019. Situational awareness: Examining factors that affect cyber-risks in the maritime sector.

Tam, K., Moara-Nkwe, K. & Jones, K. 2021. The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research,* 3.

Wahl, A., Kongsvik, T. & Antonsen, S. 2020. Balancing Safety I and Safety II: Learning to manage performance variability at sea using simulator-based training. *Reliability Engineering & System Safety,* 195, 106698.