2023-03-13

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

Erstad, E

10.1007/s13437-023-00304-7
WMU Journal of Maritime Affairs
Springer

WMU Journal of Maritime Affairs
https://doi.org/10.1007/s13437-023-00304-7

ARTICLE

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

Erlend Erstad[1] · **Rory Hopcraft**[2] · **Avanthika Vineetha Harish**[2] · **Kimberly Tam**[2]

Received: 12 December 2022 / Accepted: 14 February 2023

Abstract

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

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

✉ Erlend Erstad
erlend.erstad@ntnu.no

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

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

Published online: 13 March 2023

1 Introduction

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

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

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

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

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

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

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

2 Maritime learning and cyber training

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

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

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

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

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

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

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

2.1 Related work

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

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

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

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

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

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

3 Human-centred design

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

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

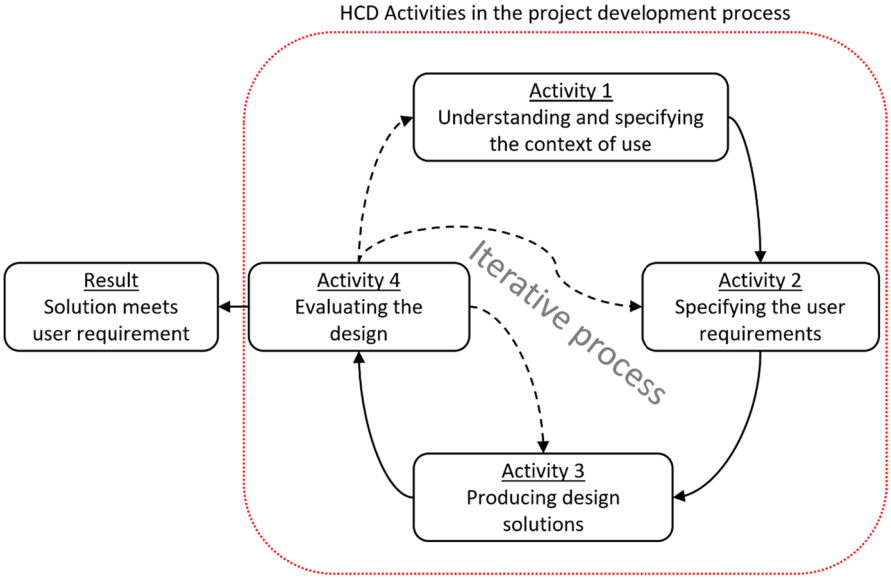

Fig. 1 The human-centred design process, adapted from (ISO 2019)

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

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

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

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

3.1 Understanding and specifying the context of use

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

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

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

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

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

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

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

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

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

3.2 Specifying the user requirements

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

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

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

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

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

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

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

3.3 Producing solutions

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

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

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

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

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

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

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

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

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

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

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

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

3.4 Evaluating the design

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1 Description of scenario

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

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

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

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

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

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

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

4.1.1 Pre-scenario preparation

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

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

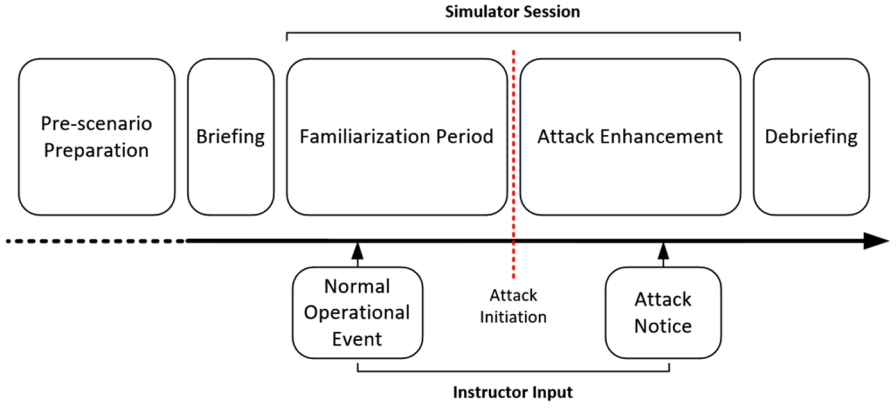

Fig. 2 Timeline of the scenario. Source: Authors

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

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

4.1.2 Briefing

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

4.1.3 Familiarisation

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

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

4.1.4 Normal operation event

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

4.1.5 Attack initiation

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

4.1.6 Attack enhancement

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

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

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

4.1.7 Attack notice

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

4.1.8 Debrief

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

5 Conclusion

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

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

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

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

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

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

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

Declarations

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

References

Abeysiriwardhane A, Lützhöft M, Petersen ES, Enshaei H (2016) Human-centred design knowledge into maritime engineering education; theoretical framework. Australas J Eng Educ 21:49–60. https://doi.org/10.1080/22054952.2017.1287038

Akpan F, Bendiab G, Shiaeles S, Karamperidis S, Michaloliakos M (2022) Cybersecurity challenges in the maritime sector. Network 2:123–138. https://doi.org/10.3390/network2010009

Ashford W (2019) NotPetya offers industry-wide lessons, says Maersk's tech chief [Online]. ComputerWeekly.com: ComputerWeekly.com. Available: https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief. Accessed 23 Nov 2022

Bacasdoon J, Bolmsten J (2022) A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches. TransNav, *The International Journal on Marine Navigation and Safety of Sea Transportation* 16**:**319–334. https://www.transnav.eu/

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

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

Canepa M, Ballini F, Dalaklis D, Vakili S (2021) Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. Proceedings of INTED2021 Conference. 9th. https://doi.org/10.21125/inted.2021.0726

Chowdhury N, Gkioulos V (2021) Cyber security training for critical infrastructure protection: a literature review. Comp Sci Rev 40:100361. https://doi.org/10.1016/j.cosrev.2021.100361

Chowdhury N, Gkioulos V (2021b) Key competencies for critical infrastructure cyber-security: a systematic literature review. Inf Comp Secur. https://doi.org/10.1108/ICS-07-2020-0121

De la Vallée P, Iosifidis G, Rossi A, Dri M, Mees W (2022) Sector-specific training - a federated maritime scenario. Cham: Springer International Publishing, pp 21–35. https://doi.org/10.1007/978-3-031-20215-5_3

Erstad E, Ostnes R, Lund MS (2021) An operational approach to maritime cyber resilience. TransNav, *The International Journal on Marine Navigation and Safety of Sea Transportation* 15**:**27–34. https://www.transnav.eu/

Erstad E, Lund MS, Ostnes R (2022a) Navigating through cyber threats, a maritime navigator's experience. https://doi.org/10.54941/ahfe1002205

Erstad E, Larsen MH, Lund MS, Ostnes R (2022b). Maritime Cyber Simulator Scenario Workshop report. https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/3037765. Accessed 12 Oct 2022

Fayi SYA (2018) What Petya/NotPetya ransomware is and what its remidiations are. Information technology-new generations. Springer. https://doi.org/10.1007/978-3-319-77028-4_15

Goldie JGS (2016) Connectivism: a knowledge learning theory for the digital age? Med Teach 38:1064–1069. https://doi.org/10.3109/0142159x.2016.1173661

Haynes D (2021) Iran's secret cyber files. Sky News [Online]. Available: https://news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871. Accessed 10 Dec 2022

Heering D, Maennel O, Venables A (2021) Shortcomings in cybersecurity education for seafarers. Developments in Maritime Technology and Engineering. CRC Press. https://doi.org/10.1201/9781003216582-06

Hontvedt M, Arnseth HC (2013) On the bridge to learn: analysing the social organization of nautical instruction in a ship simulator. Int J Comput-Support Collab Learn 8:89–112. https://doi.org/10.1007/s11412-013-9166-3

Hopcraft R (2021) Developing maritime digital competencies. IEEE Comm Stand Mag 5:12–18. https://doi.org/10.1109/mcomstd.101.2000073

Hopcraft R, Martin KM (2018) Effective maritime cybersecurity regulation–the case for a cyber code. J Indian Ocean Reg 14:354–366. https://doi.org/10.1080/19480881.2018.1519056

IMO, I. M. O. (2012) Model Course 6.10 Train the simulator trainer and assessor. London: International Martime Organization

IMO, I. M. O. (2015) MSC.1/Circ.1512. Guideline on Software Assurance and Human-Centred Design for e-Navigation

IMO, I. M. O. (2016) International convention on standards of training, certification and watchkeeping for seafarers (STCW). *International Maritime Organisation, London, UK,*

IMO, I. M. O. (2017a) MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management,.

IMO, I. M. O. (2017b) Resolution MSC.428(98) - Maritime cyber risk management in safety management systems.

IMO, I. M. O. (2018) International safety management code: with guidelines for its implementation. London, International Maritime Organization

ISO, I. O. F. S. (2019) 9241–210: 2019 Ergonomics of human-system interaction. Part 210: Human-Centred Design for Interactive Systems. iso.org: International Organization for Standardization

Jo Y, Choi O, You J, Cha Y, Lee DH (2022) Cyberattack models for ship equipment based on the MITRE ATT&CK framework. Sensors 22:1860. https://doi.org/10.3390/s22051860

Kessler GC, Shepard SD (2020) Maritime cybersecurity: a guide for leaders and managers. Daytona Beach, Kessler & Shepard

Larsen MH, Lund MS, Bjørneseth FB (2022) A model of factors influencing deck officers' cyber risk perception in offshore operations. Marit Transp Res 3:100065. https://doi.org/10.1016/j.martra.2022.100065

Lund MS, Hareide OS, Jøsok Ø (2018) An attack on an integrated navigation system. Sjøkrigsskolen.https://doi.org/10.21339/2464-353x.3.2.149

Lund MS (2022) Øving på cybersikkerheit: Ein casestudie av ei cybersikkerheitsøving. Scand J Mil Stud 5(1)**:**244–256. https://doi.org/10.31374/sjms.119

Madsen AN, Aarset MV, Alsos OA (2022) Safe and efficient maneuvering of a maritime autonomous surface ship (MASS) during encounters at sea: a novel approach. Mar Transp Res 3:100077. https://doi.org/10.1016/j.martra.2022.100077

Meland P, Bernsmed K, Wille E, Rødseth Ø, Nesheim D (2021) A retrospective analysis of maritime cyber security incidents. TransNav, *The International Journal on Marine Navigation and Safety of Sea Transportation*. https://www.transnav.eu/

Milinković SA, Lazić LR (2012) Industrial PLC security issues. 2012 20th Telecommunications Forum (TELFOR). IEEE, 1536–1539. https://doi.org/10.1109/TELFOR.2012.6419513

Nazir S, Øvergård KI, Yang Z (2015) Towards effective training for process and maritime industries. Procedia Manufacturing 3:1519–1526. https://doi.org/10.1016/j.promfg.2015.07.409

Norman D (2013) The design of everyday things: revised and, expanded. Basic books

NTSB, N. T. S. B. (2021) Capsizing of roll-on/roll-off vehicle carrier golden ray, marine accident report. In: BOARD, N. T. S. (ed) National Transporation Safety Board National Transporation Safety Board. https://www.ntsb.gov/investigations/Pages/DCA19FM048.aspx. Accessed 10 Dec 2022

Oommen PG (2020) Learning theories – taking a critical look at current learning theories and the ideas proposed by their authors. Asian J Res Educ Soc Sci 27–32%V 2

Porathe T (2016) Human-centred design in the maritime domain. DS 85–1: Proceedings of NordDesign 2016, Volume 1, Trondheim, Norway, 10th-12th August 2016**,** 175–184

Raimondi M, Longo G, Merlo A, Armando A, Russo E (2022) Training the maritime security operations centre teams. 2022 IEEE International Conference on Cyber Security and Resilience (CSR). IEEE, 388–393. https://doi.org/10.1109/csr54599.2022.9850324

Rajaram P, Priyanga R, Goh Voon Wei M, Zhou J (2022) Guidelines for cyber risk management in shipboard operational technology systems. iTrust Centre for Research in Cyber Security: Singapore Univeristy of Techonolgy and Design. https://doi.org/10.1088/1742-6596/2311/1/012002

Refsdal A, Solhaug B, Stølen K (2015) Cyber-risk management. Cyber-Risk Management. Springer. https://doi.org/10.1007/978-3-319-23570-7_5

Scanlan J, Hopcraft R, Cowburn R, Trovåg JM, Lützhöft M (2022) Maritime education for a digital industry. Necesse 7:75

Sellberg C, Wiig AC (2020) Telling stories from the sea: facilitating professional learning in maritime post-simulation debriefings. Vocat Learn 13:527–550. https://doi.org/10.1007/s12186-020-09250-4

Sellberg C, Lindmark O, Rystedt H (2018) Learning to navigate: the centrality of instructions and assessments for developing students' professional competencies in simulator-based training. WMU J Marit Aff 17:249–265. https://doi.org/10.1007/s13437-018-0139-2

Sellberg C, Lindwall O, Rystedt H (2021) The demonstration of reflection-in-action in maritime training. Reflective Pract 22:319–330. https://doi.org/10.1080/14623943.2021.1879771

Siemens G (2004) Connectivism: a learning theory for the digital age. elearnspace

Stoker G, Greer J, Clark U, Chiego C (2022) Considering maritime cybersecurity at a non-maritime education and training institution. Proceedings of the EDSIG Conference ISSN. 4901

Tam K, Jones K (2019) Situational awareness: examining factors that affect cyber-risks in the maritime sector. https://doi.org/10.22619/ijcsa.2019.100125

Tam K, Hopcraft R, Moara-Nkwe K, Misas JP, Andrews W, Harish AV, Giménez P, Crichton T, Jones K (2021a) Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety. https://doi.org/10.4236/jtts.2022.121001

Tam K, Moara-Nkwe K, Jones KD (2021b) The use of cyber ranges in the maritime context: assessing maritime-cyber risks, raising awareness, and providing training. Mar Technol Res 3**:**16–30. https://doi.org/10.33175/mtr.2021.241410

UOB, U. O. B. (2022) Constructivism [Online]. https://www.buffalo.edu/catt/develop/theory/constructivism.html: Univeristy of Buffalo. Available: https://www.buffalo.edu/catt/develop/theory/constructivism.html. Accessed 10 Dec 2022

Vu V, Lützhöft M (2020) Human-centred design application in the maritime industry challenges and opportunities. In: Rina, T. R. I. O. N. A. (ed) Human Factors. London. https://doi.org/10.3940/rina.hf.2020.03

Vykopal J, Vizváry M, Oslejsek R, Celeda P, Tovarnak D (2017) Lessons learned from complex hands-on defence exercises in a cyber range. 2017 IEEE Frontiers in Education Conference (FIE). IEEE, 1–8. https://doi.org/10.1109/fie.2017.8190713

Wahl AM (2020) Expanding the concept of simulator fidelity: the use of technology and collaborative activities in training maritime officers. Cogn Technol Work 22:209–222. https://doi.org/10.1007/s10111-019-00549-4

Wahl A, Kongsvik T, Antonsen S (2020) Balancing Safety I and Safety II: learning to manage performance variability at sea using simulator-based training. Reliab Eng Syst Saf 195. https://doi.org/10.1016/j.ress.2019.106698

Watson J (2001) Social constructivism in the classroom. Support Learn 16:140–147. https://doi.org/10.1111/1467-9604.00206

Windschitl M (1999) The challenges of sustaining a constructivist classroom culture. The Phi Delta Kappan 80:751–755