Maritime Education for a Digital Industry

J. Scanlan¹, R. Hopcraft², R. Cowburn³, J.M. Trovåg¹, M. Lützhöft¹

¹Department of Maritime Studies, Western Norway University of Applied Sciences
²Faculty of Science and Engineering, University of Plymouth
³Safety Management Systems (Sweden) AB

Abstract - The maritime industry is undergoing a digital revolution, and the high pace of change is expected to continue with the adoption of artificial intelligence and increased levels of automation on the horizon. These changes present many opportunities for innovation and improvements to the existing maritime industry, but they also pose a range of challenges. This paper will specifically examine the effects of these changes on seafarers, with regard paid to their education, and ongoing professional development over the length of a career. The evolving working context is resulting in the core skillset of seafarers to grow, particularly in relation to digital literacy. The January 2021 deadline of the IMO’s cyber risk management Resolution MSC.428(98) has drawn attention to the capability and knowledge deficit in relation to cyber security within the industry’s IT and OT infrastructure. As IT system grow in their usage and OT systems become more connected, and are modernized, seafarers need to still be able to use the existing technology, while becoming proficient in the new, creating a complex transition environment, with limited access or time to undertake professional development. This paper describes several new education approaches that are aiming to equip seafarers and other industry members to this changing knowledge landscape.

Keywords

Introduction
The maritime industry is the backbone of global trade, handling 90% of long-range transport. The value of the goods transported is immense, with few other systems having as much impact on economies around the world. As a result, the safety and effectiveness of the entire maritime ecosystem is of interest to governments, regulatory bodies, businesses, and producers all around the world. As the system evolves, improvements can create more opportunities for trade, further fuelling economic growth. Conversely, threats to the maritime ecosystem can have broad impacts, slowing trade, causing massive economic losses. The blockage of the Suez Canal in early 2021, for example, was estimated to cost $9.6 billion US dollars per day of the blockage (Baker, Watkins and Osler, 2021).

Concerns that face the maritime industry, which are of a systematic nature (those that effect the industry as a whole), are of great concern for the possible second and third order effects to the economies of countries around the globe.

The maritime industry, in its efforts to improve, has been becoming increasingly digitised in recent years. IT systems now have a significant role in bridge systems used in navigation, industrial control systems for controlling ship functions, eLogistics interconnections to enable effective transport in and out of ports, business and human resources systems, and personal use by seafarers. With these changes comes impacts that are positive to safety, efficiency, and wellbeing, but have also resulted in negative outcomes in the form of vulnerability to cyber threats, and a shift in the required skillset for personnel to operate vessels. The impact of IT systems is set to increase in the years ahead as connectedness of vessels increases, and as vessel operations adopt more automation.

This paper will explore the current state of affairs in respect to seafarer training in relation to the usage of IT systems, and discuss the current impacts being experienced within the industry. The paper will highlight several education and awareness efforts being undertaken by the authors to motivate change and improve digital literacy and provide cyber risk management skills across the sector. In addition, we examine the need for renewal of the training known as Bridge and Engine (aka Crew) Resource Management (BRM/ERM). BRM/ERM started its existence as a pragmatic approach to aviation incidents and accidents. At present it has a module on automation, but this is the application of BRM/ERM tools to a partially automated environment and it needs complementing or adapting to a more, or even fully, automated work environment.

Background
The maritime industry is rapidly digitising, undergoing a “digital revolution” (Nguyen, 2017). The changes are occurring at multiple levels within the industry, sometimes with differing motivations. IT systems are being used to undertake ship design and construction, seafarer training, ship operations and control, and within the supply chain. Such changes are not a surprise with many industries having undergone sizable change through the adoption of digital systems in the last half of a
For example, in the early 2000s, the IMO mandated that all cargo ships over 300GT and passenger vessels implement the automatic identification system (AIS). The AIS system transmits data that describes the current state of the ship every 3-10s. While primarily a safety measure to assist in collision avoidance, this digital transition resulted in a dramatic increase of data available about ship movements and created multiple opportunities for innovation, particularly in green shipping (Watson et al., 2021), quite removed from its initial goal. However, unfortunately, AIS data has also been misused by pirates to target specific vessels (Wee, 2017). Technology can serve as a great catalyst for change, and the nature of that change is not always predictable – it can impact whether traditional approaches are changed, or indeed how seafarers interact with one another and vessel systems. While adopted for the expected benefits, of which there may be many, there can also be unforeseen challenges which also need to be overcome.

The digital change that is occurring within the sector will create new opportunities for the industry to innovate but could also present challenges to overcome.

Opportunity for Innovation
The digitisation of the maritime industry presents a broad range of opportunities. Sanchez-Gonzalez et al. (2019) argue that the current advances are occurring in eight key areas:

- Autonomous vehicles and robotics,
- Artificial Intelligence (AI),
- Big data and analytics,
- Virtual and augmented reality,
- Internet of Things (IoT),
- Cloud and edge computing,
- 3D printing and additive engineering, and
- Digital security.

Several of these areas, such as autonomous shipping and digital security, have been hot topics within the industry for some time and have also produced new guidance and regulations governing these areas within the industry (IMO, 2017; IMO, 2021). While others, just as commonly discussed, are resulting in shipboard systems evolving from being simple task-based systems, to also being key connected devices to enable digital shipboard and remote monitoring of a vessel, where previously this was not possible. This constant collection of data enables accurate models of performance of a vessel, or a particular system onboard, to be tracked and understood in far greater depth than ever before.

Indeed, across most of these areas, a common factor between many of them is an increased connectedness, and vast amounts of data are being recorded. This data is being used to drive the other areas such as artificial intelligence, to enable more productive use of existing systems. Many of the opportunities that are emerging are built upon leveraging data which were previously not recorded, or were too vast for effective analysis to occur, but thanks to technology advances is now possible.

Currently, AI, fuelled by big data, collected from IoT sensors installed throughout a vessel, can enable the creation of simulations relating to autonomous vessels, giving insight into what the future of shipping may be like. How automated these vessels may be remains to be seen, but, increased assistive technology, designed around AI produced models, that can be applied at the edge (i.e. on device, on board, possibly without external internet activity being required), is likely in the near future (Bergmann, Primor & Chrysostomou, 2021). The amount of data now able to be recorded and utilised, will undoubtedly have a substantial change on how shipboard operations are undertaken. Inmarsat has reported that the data consumption per vessel increased nearly tripled, from 3.4 to 9.8 gigabytes between January 2020 and March 2021 (Thetius & Inmarsat, 2021), illustrating the transformation that is taking place.

A key element which could further accelerate this data driven future, is an external change in internet connectivity which is occurring over the next few years. Starlink, OneWeb, and multiple other companies, are in the process of recreating the satellite internet infrastructure used within the maritime industry. Instead of ships being reliant on low-bandwidth high latency connections, they promise a future of high bandwidth, with low latency (Scanlan, et al., 2019). Such systems will remove the bandwidth constraints which currently can limit the amount of data that is transmitted to and from a vessel while it is at sea. Once adopted, companies can make more use of cloud-based services and live data access to shipboard systems, and indeed can lead to adoption of systems like digital twins fuelled by this increased access to data. This will enable companies to further understand shipboard decision making and to train AI. An increase to the data flow in and out of a vessel will further accelerate the innovation cadence that digitisation has enabled to date.

The opportunities presented are rapidly translating into market value, with the last 18months of the
COVID-19 pandemic resulting in the digital portion of the maritime sector growing 18% more than previously projected (Thetius & Inmarsat, 2021). The global maritime digital technology industry is now forecasted to be worth $345bn by 2030, up from $159bn in 2021. This scale and rate of growth will attract new players to the industry, specifically technology and engineering start-ups, enabling innovation to remain high.

**Challenges to Overcome**

The increased adoption of digital systems is changing the maritime industry, and in particular the role that seafarers undertake. A selection of challenges directly impacting the seafarers include: need for new skillset, over-dependence on automation, security, reliability, and usability of the technology, and legal issues. (Earthy & Lützhöft, 2018). The possible changes are broad and have multiple impacts in how seafarers perform their duties. As such, a key element in the digital transformation is ensuring that, as systems are modified and evolve, designing them for their intended users is central to the process.

The introduction of AI as a truly intelligent colleague will likely be slower than many fear or anticipate but central areas of interest are how to cooperate (designing relationships such as teaming) (ISO, 2020), trust in, and trustworthiness of, the technology and issues regarding liability (Earthy & Lützhöft, 2018). This is a key example of considering human factors which impact how seafarers interact with AI driven systems that may replace or augment existing technologies. The role of trust within safety is a concept with a long history (Reason, 1998), and maritime specific obstacles have been articulated (Gausdal & Makarova, 2017). However, the adoption of AI, and the trust in those systems is a new context for the industry to adapt to. As seen in other sectors, trust and distrust in autonomous systems often leads to poor human decision-making, resulting in stressful and dangerous situations (Tam et al, 2021). Accountability practices will be a key element (Ariga & Sanford, 2021), however an education element for sea farers to understand AI systems capabilities and limitations is also important.

One of the most noticeable challenges being experienced due to the increased reliance of digital technologies, is an increase in cyber-attacks. This also has a trust element, in relation to seafarers being able to trust vessel systems are performing correctly, in the event of a cyber-attack such as a malware infection. This is made particularly challenging as often the source of the attack and its impact on operations is unknown. As shipboard systems become more reliant on sensors and digital systems, an attack could result in systems malfunctioning, or giving strange outputs, which are more subtle, and require critical thinking skills and IT knowledge to comprehend that an incident has occurred. There is also a need to develop trust between the crew and the broader shipping company to develop a just culture. Whereby crew are not blamed for mistakes, yet each member has a clearly defined responsibility in the event of a cyber-attack.

Since the dramatic effects of NotPetya on Maersk in 2017 (Greenberg, 2018), there has been an increase in cyber-attacks, with some estimates ranging as high as 900% across the last three years (Safety4Sea, 2020). The industry had previously enjoyed a relatively low risk of cyber-attack compared to other industries due to the disconnectedness of the systems, and with low digitisation. However, as digitisation adoption has grown, the cyber risk being experienced by vessels and companies has also increased. An argument can be made that cyber attack frequency will continue to grow as digitisation increases (Tuomala, 2021). As new satellite connections come online, enabling more data to flow in and out of vessels, opportunities for malicious actors to impact operations will also increase (Scanlan, 2019). In addition, as illustrated by the Maersk incident, the maritime industry exposure to cyber threats is not limited just to vessels. Shipping companies and ports are also targets of cyber-attack (de la Peña Zarzuelo, 2021). This is an industry wide challenge, which the industry has started to respond to, and will need to continue to in the years to come.

Most of these challenges, whether in relation to cyber security, or the impact of technology changes on seafarers, present a key role for education and awareness raising to mitigate the impact. As changes occur to work processes on vessels, whether it is in collaboration with AI, or whether it is undertaking work in a safe manner to minimise cyber risk, a training element is vital. As such, a recent maritime cyber security white paper found that 52% of respondents considered the human element as their organisations greatest cyber threat (Safety at Sea, 2020). This education element is not only likely a key part of the answer to the challenges previously described but are also a key challenge itself. Maritime is an old industry, with long established ways of operating and training its employees. A report from the World Maritime University (Schröder-Hinrich et al, 2019) states that with new technology, including increased levels of automation, will create new jobs and the requirements and skills needed for existing individual jobs will change. However, the digital revolution that is currently underway is moving quickly and can have direct impacts on to the safety of vessels and crew. Enabling rapid education and re-education of those within the industry is a complex problem, that is going to need a multifaceted solution.
Responding to the Challenges
The challenges that are facing the maritime industry due to the rapid digitisation that has occurred relate primarily to

- Increase in cyber threats
- Changed skill landscape for seafarers, both near term and further into the future
- A need for context and ‘shape’ of learning to fit around operational changes

There has been a sizable response to the cyber threats facing the industry, in part driven by IMO who amended the ISM Code to explicitly include cyber security by adopting Resolution MSC.428(98). The Resolution (IMO, 2017) encouraged ship owners, flag states, and others to ensure that existing safety management systems addressed cyber risks no later than 1 January 2021. This measure requires risk audits of systems to be undertaken, enabling much greater awareness to operators to the risks that are being faced, to facilitate mitigation measures to be implemented.

Furthermore, the Resolution explicitly states that under the objectives of the International Safety Management Code, there should be “…the continuous improvement of safety management skill of personnel ashore and aboard ships”. As such, the ISM Code (IMO, 2018) stipulates that companies should establish and maintain procedures for identifying training which may be required in support of the safety management system. Thus, personnel must have the knowledge and skills to operate digital systems safely and securely during both normal and emergency operations.

In response to IMO’s resolution, many nation states released additional guidance to enable operators to respond effectively to the cyber threat. In addition, a range of non-government organisations have also released guidance, including the following list:

- Baltic and International Maritime Council (BIMCO)
- Comité International Radio-Maritime (CIRM)
- Cruise Line International Association (CLIA)
- Digital Container Shipping Association (DCSA)
- International Chamber of Shipping (ICS)
- International Association of Dry Cargo Shipowners (INTERCARGO)
- International Association of Independent Tanker Owners (INTERTANKO)
- Oil Companies International Marine Forum (OCIMF)
- International Union of Marine Insurance (IUMI).

However, amidst all this guidance to ship owners and operators, it is vital to remember the human element: the seafarers, and their existing skill set. Already in 2018, the Norwegian shipowners’ association encouraged the authorities to develop a strategy for maritime education with particular focus on digitalisation and to ensure financing for maritime and technical education. Several authors have highlighted the need for maritime education to be adapted within the current changing landscape (Sharma, Kim & Nazir, 2021; Heering, Maennel & Venables, 2020). A future where vessel systems operate with a level of autonomy, in a data driven environment, is distinctly different to the current context. Likewise, seafarers need to learn about the impacts of their actions on cyber risk to vessels and their operations. Heering, Maennel & Venables (2020) argue that not only is current education falling short of the need, but industry wide understanding of how the risks can impact vessels is also insufficient, with more research being needed to fully understand the skill requirements of different members of crew to provide adequate protection. Thus, more needs to be done to ensure the specificity of maritime cyber risk is addressed within new training measures.

The need for education across the industry, for ship owners, operators, and seafarers, is key to responding to the challenges. As the industry responds to cyber threats, as it evolves to be more data driven and utilise AI within its systems, there is a need to ensure increased awareness. Conventional education methods, such as Bachelor and Master programs, enable the skills of those entering or retraining to be uplifted. However, those who are not able to commit the time to such programmes require shorter alternatives that can meet their needs to attain the required knowledge and skills. The area of cyber security itself is one that has evolved quite quickly in other industries, and it presents an opportunity to try new education approaches, to increase awareness in an efficient manner, and with repetition as threats evolve.

These education and awareness measures need to be designed and implemented with the ‘student’ at the centre. Whether they are a conventional student, or a worker within industry undertaking an exercise for a few hours to fill a knowledge gap, the measures need to be flexible, engaging, and appropriate. As identified by the Maritime Skills Commission (Maritime UK, 2021) a change in approach to cadet training and skill uplift is needed across the industry, at all levels, so the response needs to meet the need where it is at. This paper explores a few examples of some education approaches currently underway, with a focus on cyber security, however the same initiatives could also be expanded to cover topics in autonomous systems, data analytics or human centred design.
Standard Training

We see a need to implement change at multiple levels within industry. A key component of the existing training is defined in STCW (Standards of Training Certification and Watchkeeping) and is known as Bridge and Engine (aka Crew) Resource Management (BRM/ERM). It was originally based on work undertaken in the aviation industry for flight crew (Flight Deck Resource Management - FDRM) and encompassed an eclectic mix of leadership, decision making, communication and emergency response concepts. As BRM/ERM became established in the shipping world there was little research into their content or learning delivery and the concepts were widely accepted (so much so that the ideas were encapsulated in the STCW (IMO, 2010) updates. The application of an aviation centric training to shipping has been criticized by Helmreich et al (2001), however, a more valid concern now is how suitable is BRM/ERM as it is currently defined, within a maritime industry embracing a digital and connected future.

Principally, non-digital attitudes and skill sets determine the content (and delivery) of BRM/ERM today. Furthermore, we have only apocryphal data supporting the present models; attitude, content and learning approaches. Indeed, regarding maritime training in a wider sense little research has been carried out into learning methods and content included. So today we find ourselves in a fragmented position (Hollnagel, 2021) both regarding content and learning approaches.

To align with other maritime developments, we must establish what role BRM/ERM has to play and what the contents need to be in order to accommodate the coming developments in (maritime) technology and practice. The curriculum needs to equip seafarers with the skills to interact with and understand data from a range of sources, with a strong focus on critical thinking to enable correct application and interpretation of the data. Increased autonomy within shipboard systems, creating a digital colleague, means that seafarers need to be alert and aware of the possible short comings of these systems, with the need for an increased focus on critical thinking within their education. The risks posed by cybersecurity incidents to crew safety, and vessel security, are also vital moving forward, and need to be included within any future version of BRM/ERM. In addition, it is vital to examine new learning methods and technologies, especially regarding learning approaches (a truly andragogical approach) and methods (gamification mentioned here, q.v.) such in the 'learning in the flow of work' (Bersin 2018), guided experiences (Billet 2000), ‘blended approaches’ (Friesen 2012) among others.

The developments in the wider corporate learning environment should be gleaned for those elements that can support an updated renewed content BRM/ERM, as should other domains so we build the best possible learner centric learning experience possible, that is truly responsive to performance needs and fills the space occupied by BRM/ERM. MOOC and game-based learning with simulation will provide motivating learner experience, but other methods need to be deployed as well to provide a lifetime immersive learning experience. Just as BRM/ERM content must evolve so must learning strategies. We need to move learning and content away from abstract knowledge into a learning experience which supports needful performance and is designed to achieve such.

The “shape” of learning needs changes. To provide better learning to the people working in this domain, approaches that consider the peculiarities of maritime work are needed. Increased flexibility, agility and support systems can help. More opportunities for multimodal education – alternate mechanisms to touch on key items, enabling less contact time but better outcomes in retention. However, more research is needed to understand what modes of education is best suited to deliver standardised training (such as that needed by STCW), and to enable workers already within industry to upskill around their work schedule. Such research needs to deliver solutions which scale across the entire industry.

Maritime Education Survey

A novel Bachelor program is underway in Norway which is co-taught across four institutions (University of South-Eastern Norway (USN), Western Norway University of Applied Sciences (HVL), Norwegian University of Science and Technology (NTNU), and the Arctic University of Norway (UiT)). The Bachelor of Maritime Management (BAMM) is taught to students who commonly already work within the industry, and study while at sea or on leave.

A cohort of these students, and several in related Master’s programs, (84 in total) was surveyed to gain an understanding of the barriers they face with their study, and to give insight into the support provided by industry to those who are endeavouring to broaden their skillset.

A primary issue with students studying at sea was the lack of time to undertake study when on board (Figure 1, overpage). Over 50% of students reported only being able to study for 5 or less hours per week while at sea, whereas 85% of students reporting studying more than 5 hours per week when onshore. Granted, this is within a work environment, but there were multiple factors impacting their ability to work...
In late 2021 a range of these solutions were implemented within the delivery of BHAMM. The bulk of the content was available at the start of the semester in written form – although recordings were posted once they occurred. Students were provided with assessment specifications at the start of the semester, with clear guidance as to what content within the course needed to be covered before they could attempt the assessment, effectively giving them submission windows that were weeks long, and could enable planning around shore visits. A time management resource was created, which consisted of a written piece giving advice on how to manage time, along with two different schedules tools, at different time scales, to not only enable them to plan ahead, but to also reflect across shorter time frames, to enable them to understand their studying capacity – with the intention of their becoming more informed of what they were actually capable of while at sea.

The students responded positively to the changes, and the same survey instrument was delivered after the teaching period to this cohort. There was a 25% (76% from 51%) increase in the number of students who stated that they felt supported in their learning, and 20% reduction in the number of students who didn’t feel supported while at sea (from 26% down to 5%). In the ranking of problems that were experienced “I find it hard to allocate time to study while I am at sea” – fell from top ranked problem within the survey to third position. “I find it hard to focus on work and study in the same day” is the new top ranked option. The time management resource positively rated by all students who used the resource.

The students were asked how many weeks of the semester that they were at sea, and the average
response was 4.8 weeks (with a wide variance (std: 3.2) due to some students not being at sea at all, with the most common time away being 8 weeks). The most any student was away during the 13-week run time of the course was 11 weeks. Having students who are not away at all, and others away for 80% of the course highlights the challenges faced within this cohort, and teaching those already embedded within the industry generally.

The survey has enabled greater insights into the challenges that face maritime students, and while it has enabled some improvements within this particular course, there is much more work to be done by industry and education providers to support students studying while they work.

**MariMOOC**

The transformation of the maritime industry into a digital industry is one that is rapid, and affects those who are already within the industry, and may have been for decades already. As such, conventional educational approaches, such as undertaking a degree at a university, is a substantial barrier for them to attain skills or awareness of the kinds of issues most relevant to them during this current transformation.

In response to this a Massively Open Online Course (MOOC) was proposed and then constructed, with it launching in 2020. The MOOC covers a broad range of topics, but is primarily focused on Maritime IT, and in particular cyber security. In order to put IT skills into context, the MOOC also gives an introduction to human factors design principles and a look at technologies of the future such as autonomous shipping. Learners are able to study the content following multiple pathways, with it divided into 4 chapters that can be completed in any order.

The MariMOOC aligns with an xMOOC design, meaning an eXtended Massive Open Online Course. This style of MOOC aims to deliver content which could be delivered within a university setting, but is being offered online with the overarching goal of significantly broaden the number of students who can be exposed to university-level courses. xMOOCs reflect education theories such as instructivism (Jordan, 2014) and cognitive-behaviourism (Admiraal et al., 2015; Bali, 2014) As such, it is focused on instruction on defined topics, through multimedia by an educator. Peer based learning is not central to the approach, enabling students to work to their own timelines. Primary learning outcomes are tied to given tasks with clear instructions – enabling a learner to follow the course without outside assistance. Such a system also enables a competency model of assessment to be applied, which is seen as less arduous than written or exam-based methods. Such a shift is argued to be more accessible to students who have spent a period working in industry or away from educational institutions, while still achieving the same assessment goals. The fully online model of a MOOC provides a great deal of flexibility in relation to the speed at which a student can undertake the course, enabling them to go at their own pace -starting and stopping around other commitments, and not tied to a semester timetable.

To date the MOOC has been trialled with several industry partners and has been undertaken by over 100 learners. The MOOC is being shared with industry partners directly and is able to be imported into existing learning management systems as a standalone course.

**Game-based Learning**

Simulator training within the Maritime industry has been around for decades, with its origins in the 1970s (Homlong et al, 2016). As computer power has increased, the fidelity of the training environments has improved, and as costs have decreased it has also presented additional opportunities to leverage simulation-based training in more contexts (Mallam, Nazir & Renganayagalu, 2019). Examples of this, including using consumer grade AR or VR systems, can be used instead of large room sized custom built environments, leveraging the lower cost to provide educational outcomes in areas not previously focused upon for simulation.

Several of the authors of this paper are currently creating a serious game (i.e a game built for a non-entertainment goal), which can be used in VR or in 2D within a web browser. The intention is to provide a simulation-like environment, at very low cost, available to seafarers wherever they are physically located. Requiring only a laptop, instead of a complex expensive simulator, enabling topics such as cyber security and human factors to be the focus, which is quite different from the traditional simulation environments used for navigation and other vessel operations.

The game environment is being designed and built as flexibly as possible, with multiple scenarios being planned for the future. The current focus is on meteorology and cyber security. The former, for which the VR environment was initially conceived, enables a learner to experience weather conditions as described by the Beaufort Scale (Saucier, 1955). The learner can walk around the environment, and from the bridge of the vessel they can select the current level on the Beaufort scale. The weather within the game environment changes, resulting in the waves buffeting the vessel, effecting in game physics, with other weather effects also being visualised. Within VR it is quite disorientating, due to the immersion effect of the learner’s entire view being the game.
environment – which itself does not watch their real physical surroundings. The intent, once complete, is to illustrate the consequences of weather in combination with navigational choices, and how ship and crew are affected by different weather types.

Building on this same game environment, and in alignment with the pressing needs as described within this paper, a cyber security educational game is also being developed. This is scenario based, and as the learner walks around the vessel, and enters into areas such as the bridge, office or mess, they are presented with pre-scripted scenarios which relate to cyber risk. The learner has multiple options to respond to the scenario, deciding how to act or respond. The learner is informed as to the outcome, but also the repercussions of an incorrect outcome, and how it may affect the vessel. The aim is to explore not only the root causes of cyber incidents, such as how malware may get into a system onboard, but also what are the possible outcomes and the effect on the learner and other crew on board. Understanding the impact, large or small, on the vessel or the quality of life of seafarers, is seen as an important step to motivate behaviour change in relation to activities with a cyber risk.

The game-based learning approach described above is being developed as an additional alternative to more conventional education approaches. It can be embedded within existing curricula or be shared between possible learners within industry in a standalone form. It provides a short, immersive, goal orientated education artefact, aiming to express core fundamentals that are relevant to the human element within cyber risk management on board. The game-based elements aim to increase engagement to promote learning (Hamari, 2016). Many awareness protocols and education activities can be policy driven and can lack explanations as to the impacts if policies are not followed. The game-based environment is aiming to be facilitate cultural change through explaining the impact of cyber risks within the working environment, in a novel manner to attract attention to the challenges that are currently being faced.

**Cyber-SHIP Lab**

The latest version of the industry-published Guidelines on Cyber Security Onboard Ships (BIMCO, 2020) highlights, the broadening risk landscape facing digital bridge systems. However, there are a lack of suitable research and mitigation capabilities available to educate the sector about these risks. This gap led to the development of the Cyber-SHIP (i.e. Software, Hardware, Information, Protection) Lab. The lab hosts a range of real, non-simulated maritime systems, which is capable of configuration to match real-world bridge integrations (Tam et al, 2019).

Through the lab’s ability to run controllable and safe experiments on maritime systems, companies can learn more about their bridge systems integrations, interactions, and risks. These experiments include a range of penetration testing tools, and the running of known, and potentially custom malware. The findings from these experiments will build a detailed picture of the vulnerabilities that specific bridge integrations have.

These findings allow the Cyber-SHIP lab to offer various opportunities for improving maritime education and security education. Firstly, the initial findings from the vulnerability assessments will educate the company of the cyber risks that they face. Thus, allowing them to implement appropriate mitigation measures, including cyber security training. Secondly, these findings can inform the development of simulator-based training exercises. As discussed above, the maritime sector has a long history of benefiting from simulator training with crews (Kobayashi, 2005). When used as part of crew training and awareness programmes, these simulations will allow companies to train personnel, and test their incident response practices. What is more, crews can gain first-hand experience of a “real” cyber-incident, in the safety of a simulator.

**Cyber Ranges**

A cyber range is a simulated environment designed as a representation of an organization’s ICT, operational technology and physical systems, applications and infrastructures (NIST, 2020). These tools allow companies to create specific network topologies and employ a range of tools and attacks without risking the organization’s actual infrastructure (Priyadarshini, 2018). One such tool allowing the development of a simulated environment is the EU’s Cyber-MAR. The platform aims to provide companies with a way to educate themselves about cyber risk (Cyber-MAR, 2019).

To ensure the simulated environment is as realistic as possible, companies must develop a very detailed understanding of their own networks. Once modelled, the tools within the platform allows a company to educate themselves about their network interactions and how these could lead to vulnerabilities. Again, this understanding can then be used to inform the design of maritime education programmes. Thus, ensuring that personnel are provided with the skills and knowledge that is appropriate to the risks they face.

Furthermore, utilising a cyber range as a training tool has other benefits, one of which is federation. Examples of federation includes the support for
running simulations and activities in multiple locations and sharing those activities with others (Tam et al, 2020). Thus, allowing companies to develop and deliver cyber range-based training in different locations. A particularly useful attribute considering the often dispersed geographical location of a company’s maritime assets and personnel.

### Conclusion

The maritime industry is changing, and with that change, as described in this paper, are many positive outcomes, but also several challenges. The education needs of the sector have shifted, and will continue to shift, as the current digital transition continues, and indeed may accelerate. A key area in relation to this is cyber risk management. IMO, and others, have taken steps to lift the capacity of the industry to meet this challenge, but central to this response needs to be equipping seafarers to play their role. A safe and secure shipping industry requires many within the industry to adapt their skillsets to the new landscape. This is a significant educational and awareness challenge. The current skills gap in relation to cyber could be just the beginning of a shifting skills landscape with a future that is more reliant upon data and automation.

Enabling an industry to respond to a new set of risks which it has not had to deal with before requires a substantial effort. There is the need for technological innovation to meet the risks, but also for cultural change to ensure the challenges are given an appropriate level of resources and attention. The educational needs within the sector are shifting, creating skill and awareness gaps. Those working within the sector already have existing workloads and priorities and cannot simply dedicate substantial amounts of time to training courses. The approaches need to be flexible to the time pressures that are present, while still providing meaningful outcomes.

This paper has described several initiatives which aim to meet this challenge. They are focused on raising cyber risk awareness and educating how to manage cyber risk in a maritime context. There is no single solution, and indeed only several possible solutions are presented here. It will require an industry wide effort to ensure the digital systems being used are used in a safe and secure manner. A possible solution is to revisit BRM/ERM and establish what role it can have in providing a firm foundation in skill requirements required for those within the industry. An updated BRM/ERM could define a baseline of skills and awareness in relation to cybersecurity, providing a more defined framework for shipping companies to work within to maintain a highly skilled workforce.

A future where vessels have an increased level of autonomy, will also change the skillsets of seafarers and others within the industry. Many of the education initiatives and methods described here, in relation to cyber security, can be seen as a ‘practice run’ for the further changes which will occur in the years ahead.

### Acknowledgements

We gratefully acknowledge the funding from Kompetanse Norge for the MariMOOC project, and the Directorate for Higher Education and Skills (Diku) for the Student at Sea project (in which the student survey was conducted).

This paper is also partly funded by the research efforts under Cyber-MAR. The Cyber-MAR project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors’ view and European Commission is not responsible for any use that may be made of the information it contains.

### References


Greenberg, A. (2018). The untold story of NotPetya, the most devastating cyberattack in history. Wired, August, 22.


