Developing Maritime Digital Competencies

Rory Hopcraft

Abstract

In recent years, there has been a relentless drive by all industries to digitalize many everyday operations. The maritime industry is no exception, with the increase in digital tools that assist the everyday operations of the seafarer. What is more, much of this technology is now networked together, or to the Internet, which opens the seafarer up to a wave of new cyber risks. Maritime communication systems have often been demonstrated as insecure in the recent past. Thus, without appropriate training, seafarers are ill-prepared to protect themselves, and the systems for which they are responsible, from the impacts of cyber incidents. This article argues that there is a clear link between seafarer training and maritime safety. As such, there is a need to develop standardized digital competencies for all seafarers. The creation of these competencies needs to be considerate of company-specific and operation-specific risk management practices. This article presents one possible solution for the development of maritime digital competencies utilizing the well-established NIST Cybersecurity Framework.

Introduction

In recent years, there has been a rapid increase in the number of digital technologies integrated into ship systems. This technology now forms vast networks, often connecting to the Internet, increasing the reliance on, and vulnerabilities to, maritime communication systems. For example, compromising the satellite communication that underpins both navigation and the Global Maritime Distress Safety System (GMDSS) puts seafarer safety at risk. With an estimated 90 percent of all goods being shipped via the world's oceans [1], providing seafarers with adequate cybersecurity training is vital to ensure the continued safety and security of these vital communication networks.

Ship communication systems have come under increased scrutiny from researchers, proving that some of these systems are vulnerable to cyber attack [2]. While attempting to fool remote-guided weaponry, the Russian government has been demonstrating these vulnerabilities since the early 2000s. More recently in 2019, an escalation of tensions in the Straits of Hormuz led to the accusation that Iran was subtly manipulating GPS to trick ships into entering Iranian territorial waters, allowing their detention [3]. The manipulation of GPS signals leads to a ship's navigational equipment presenting an inaccurate location, raising serious safety concerns for seafarers onboard.

It is worth noting that other cyber risks threaten the safety and security of ship systems. For instance, ships have long lifespans, leading to systems remaining in service long after becoming obsolete. These unsupported systems do not benefit from regular security updates, leaving them increasingly vulnerable until the end of the ship's life cycle. Furthermore, out-of-date systems also pose a threat to modern ships, where, due to limited bandwidth at sea, a ship has to wait until its next port call to download patches and updates. Thus, due to the varied nature of cyber risks, effective risk management should include a combination of different mitigations, including technical, physical, and procedural mitigations.

This article argues that seafarers, as the operators of these systems, play a vital role in ensuring the continued safety and security of their ship. Thus, as part of their cyber risk management, companies should develop digital competencies alongside other mitigations. Equipping seafarers with appropriate digital competencies will ensure that they are not only aware of the risks facing their digital systems, but also better prepared to respond to those risks. Furthermore, these competencies are considerate of the complexities inherent in maritime operations. These complexities include the diverse backgrounds and experiences of seafarers, as well as the challenges in providing training to crews who spend little time in ports.

In 2017, facing growing pressure, the International Maritime Organization (IMO) issued Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems [4] as its first step toward regulating maritime cybersecurity. Using this Resolution and its other instruments, the IMO has placed significant emphasis on the development of seafarers' digital skills as an important risk management strategy. By analyzing the current regulatory requirements, and discussing how these imply the need to develop digital competencies, the first section of this article explores the deep-rooted link between maritime safety, security, and training. The second section presents a framework that allows the development of standardized digital competencies that are considerate of the ship's wider risk management approach. Finally, the article concludes by discussing some of the current and future challenges facing the standardization of digital competencies.

Maritime Safety, Seafarer Competencies, and Training

The IMO, like other regulatory bodies, provides a clear distinction between safety and security.

Digital Object Identifier:
10.1109/MCOMSTD.101.2000073

The author is with the University of Plymouth.

2471-2825/21/$25.00 © 2021 IEEE

Safety means protection from the risk of injury in the context of non-intentional events, like accidents, whereas *security* refers to protection from intentional events [5]. However, the International Atomic Energy Agency (IAEA) argues that managing safety and security often occurs synchronously [6]. Thus, companies will deal with the consequences of an incident similarly regardless of intentionality. For instance, during a power failure onboard, regardless of the cause, the crew will respond the same way by ensuring the event does not compromise the ship's safety or security (i.e., drift into the path of another ship). Therefore, in regard to cyber risk management, crews need to interact with and respond to events involving digital systems appropriately. This ensures that seafarer actions do not cause a safety incident or inadvertently aid a security event. Thus, as the actions of seafarers have a direct impact on the safety and security of a ship's systems, they must be equipped with appropriate digital competencies to make informed decisions about those systems.

The IMO has long since emphasized the link between the human element and the safety and security of the maritime sector. In 1993 the IMO formally acknowledged the relationship between training and ship safety [7]. Developing this further, the IMO argues safety and security are based on many complex interacting variables, which include training, skill, and experience [8]. Thus, as the reliance on digital systems increases, so too should the skill and experience levels of seafarers. A recent survey by the shipping association BIMCO found that 52 percent of respondents felt that their personnel were their organization's biggest cyber vulnerability [9]. The survey also reports that phishing and spear-phishing were the two most common attack vectors, with 68 and 41 percent, respectively, experiencing these types of attacks in 2020. Thus, as seafarers increasingly find themselves and their systems facing cyber risks, they must be equipped with the skills to ensure they do not compromise the safety and security of the ship.

The IMO, STCW Convention, and Digital Competencies

As the United Nations specialized agency charged with the safety and security of international shipping, the IMO has led the way in standardizing maritime skills and practices with the aim to improve the operational safety of the industry. This standardization comes in the form of the International Convention on Standards of Training, Certification and Watchkeeping (STCW) [10]. The STCW Convention argues that the safety and security of a ship are reliant upon seafarers who are qualified and fit for duties. The Convention stipulates the core competencies that all seafarers must demonstrate in order to make a knowledgeable and informed contribution to the safe operation of the ship.

STCW also obligates companies to tailor the development of competencies toward the specific needs of the ship and its operations (e.g., LPG tanker, cruise ship, container ship). Companies are also required to provide a reasonable opportunity for the crew to become familiar with shipboard equipment and operating procedures needed for the proper performance of their duties. Without this familiarization or training, crews will be ill-prepared for operating shipboard systems, increasing the risk they pose to the safety and security of both ship and crew.

Another IMO instrument that provides guidance on seafarer competencies is the International Management Code for the Safe Operations of Ships and for Pollution Prevention (ISM Code). The Code stipulates that "the Company should establish and maintain procedures for identifying any training which may be required in support of the SMS [Safety Management System] and ensure that such training is provided for all personnel concerned" [11]. The SMS should contain instructions and procedures that ensure the safe operation of the ship during normal and emergency operations. Therefore, the company responsible for the operation of the ship and managing its crew must now consider the skills and knowledge required by their seafarers to implement the procedures within the SMS.

Therefore, under the current IMO instruments, there is scope to include digital competencies as part of cyber risk management. With the continued integration of digital systems onto ships, all seafarers now have a duty to ensure they do not compromise the safety or security of these systems. What is more, due to their ability to understand the risks specific to their operations, these regulations place the onus of training on the company. Thus, to fulfill their requirements under STCW, companies should consider the difference in operations, operational environments, vessel types, and the pre-existing digital skills of seafarers when developing digital competencies for their crews.

Safety Risk Management and Training

As mentioned previously, safety and security often have differing focuses, but as companies strive to improve either, they inadvertently advance the other. The IAEA and IMO have both advocated for the synchronous development of both a safety and a security culture that encourages the holistic management of risk [6]. As such, the IMO argues that a safety culture forms an integral part of a company's safety management system (SMS). The IMO also argues that this should also include the development of a just culture [12], where companies accept that accidents do happen, and these offer an opportunity to learn what changes are needed to address failings in the current SMS.

The development of an organizational culture that is considerate of both safety and security, as illustrated in Fig. 1, allows a company to assess the risks they face, and determine the activities required to mitigate that risk. Therefore, with Resolution MSC.428(98) placing cyber risk under the provisions of the ISM Code, companies must now consider it within their SMS and develop their safety cultures to include cyber risk.

In Akshaikh's review of cybersecurity culture initiatives [14], it is evident that human actions and behaviors play a vital role in the development of organizational cultures that consider cyber risk. Thus, the development of a cyber-inclusive safety management system will ensure that an organization understands the cyber risk management skills required by a ship's crew. For example, what skills

As the United Nations specialized agency charged with the safety and security of international shipping, the IMO has led the way in standardizing maritime skills and practices with the aim to improve the operational safety of the industry. This standardization comes in the form of the International Convention on Standards of Training, Certification and Watchkeeping (STCW).

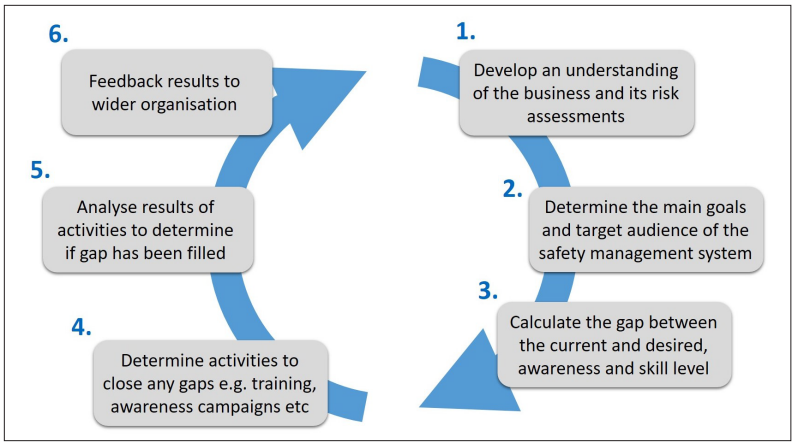

FIGURE 1. Development of a safety and security culture, adapted from [13].

would be required to ensure, and maintain, the safe working practices and working environment of digital systems? (i.e., recognize false sensor data). Second, what skills would the crew require if having to implement emergency procedures due to a cyber incident? (i.e., rebooting a critical system).

What is more, as part of a ship's SMS, companies are obligated to identify equipment and technical systems that the sudden operational failure of which may result in hazardous situations. Therefore, companies should provide seafarers with the appropriate digital skills to ensure that they can manage the risk posed by a compromised system. The loss of these systems may be accidental or deliberate, but by acquiring these digital skills, seafarers will be more able to recognize the change in system circumstances. This reduces the likelihood that a ship enters a hazardous situation, and if it does, they will be better equipped to reduce the impacts of the situation; for example, the ability to safely navigate a ship manually in the event of the loss of digital navigational equipment.

Current Requirements for Digital Competencies

The previous section illustrates that while IMO instruments advocate the development of digital competencies, they contain no explicit guidance as to what this process looks like. However, pursuant to the entry into force of Resolution.428(98), the U.S. Coast Guard has issued a Work Instruction discussing how a ship's cyber risk management will be assessed during a routine inspection [15]. The Instruction argues that if, under questioning, seafarers are unable to demonstrate a general understanding of cyber risk management, it will constitute a failure of the SMS. Failure will lead to the ship being detained, having both financial and reputational repercussions for the operator. It is also conceivable that if a cyber-incident were to occur because of a lack of digital skills, a company can no longer claim ignorance when addressing cyber risk [16]. This reiterates that seafarers must understand the cyber risks they face, and have the appropriate skills required to implement risk management processes.

While the IMO is charged with ensuring the continued safety and security of the maritime sector, it directs its members to other stakeholders for guidance. One such example is the International Organization for Standardization (ISO), who themselves reiterate the importance of developing digital competencies in cyber risk management. First, if a company were to engage in a comprehensive risk management program, they may wish to consider *ISO31000:2009 — Risk Management — Principles and Guidelines* [17]. If used appropriately, ISO31000 could provide a standardized framework to incorporate cyber risk into a ship's risk management practices. The standard reiterates the importance of implementing adequate training sessions and programs to ensure that employees are able to adhere to risk management strategies.

Moreover, endorsed by the IMO's cyber risk management guidelines, companies should be considering *ISO/IEC27001:2013 — Information Technology — Security Techniques* [18] to inform their cyber risk management practices. The standard asserts that all employees shall receive appropriate awareness, education, and training on information security relevant to their job function. Again, this highlights the importance that each seafarer receives the appropriate digital skills allowing them to operate safely.

None of the mentioned documents provide a definitive list of digital competencies required by seafarers. However, they do illustrate the link between cyber risk management and the development of digital competencies. Without clear guidance from the IMO on these competencies, companies have to ensure that they are developing a safety culture that takes into consideration company-specific cyber risks. Developing this culture will ensure that the company is equipping its seafarers with the right skills to implement the SMS.

Developing Standardized Cybersecurity Competencies

As discussed earlier, due to differences in ships and their operations, each system creates a unique network of interactions. This means that companies should be equipping their crews with appropriate knowledge and skills to ensure the continued safety and security specific to that ship. The IMO, through the technical competencies contained within STCW, has demonstrated its ability to create generic standardized training requirements applicable to all ships. It is then the company's responsibility to deliver this training, addressing both the common operational elements (e.g., fire safety) and the ship/operational specific elements (e.g., passenger evacuation), thus, ensuring that all seafarers achieve a minimum standard of competencies which address these operational differences throughout the sector.

Other regulatory bodies, including the U.S. Federal Aviation Administration, have mandated the delivery of standardized information security training [19]. These policies argue that educating and upskilling personnel who interact with digital systems will help to reduce the risk they pose to safety and security. Therefore, the maritime sector should look toward standardizing digital competencies to ensure the continued safety and security of operations, especially as more digitiza-

tion is coming in the form of autonomous ships or Internet of Things devices.

The IMO has started this process through the release of *Circular MSC-FAL.1/Circ.3* [20], which draws a direct link between cyber risk management and crew awareness. The Circular asserts that effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

As with the discussion above, other IMO instruments provide insight into what these different roles and responsibilities are. The levels of assumed responsibility presented by the STCW Convention best illustrate these differences as a hierarchy, where each level has more responsibility for the safety and security of the ship. These are the Management level, Operational level, and Support level. The Management level encompasses the Master, chief engineer, and so on. The Operational level includes the officers, and the Support level is all other seafarers.

Each level of assumed responsibility requires the demonstration of a different set of competencies, which are proportional to the seafarer's overall responsibility onboard. Furthermore, the STCW lays out the competencies with a hierarchical nature. Thus, as a seafarer assumes a higher level of responsibility they must demonstrate all required competencies from the lower tier. One such example of the additional responsibility is the discretion of the Master, as discussed in various IMO instruments. Having this discretion means that no other person shall prevent or restrict the ship from executing any decision that the Master deems necessary for the safety or security of the ship. Thus, illustrating that while all crew must demonstrate broad competencies to ensure a ship's safety and security, the Master must have the appropriate knowledge to fulfill the additional requirements of being in a higher position of responsibility. This includes being able to advise and direct others on the best course of action (Fig. 2).

Determining that the Master requires more cybersecurity training than a deckhand is only part of the puzzle. As discussed above, the IMO has yet to provide clear guidance on the required digital competencies of seafarers. However, inspiration can be drawn from the *NIST Cybersecurity Framework* [21]. The IMO recommends the NIST framework as a guide on the implementation of cyber risk management practices. As such, the framework provides a methodology through which companies can identify critical assets and systems, the threats to those systems, and the required mitigation processes.

As with all socio-technical systems, the human element is just one of the factors that influence a company's cyber risk management approach. Applying the NIST framework ensures that companies consider cyber risk holistically, from both safety and security perspectives. Thus, allowing companies to understand the role of their seafarers within the SMS, and implement other physical, technical, or procedural mitigations, complements this. This process will also highlight where competencies need to be developed to ensure that

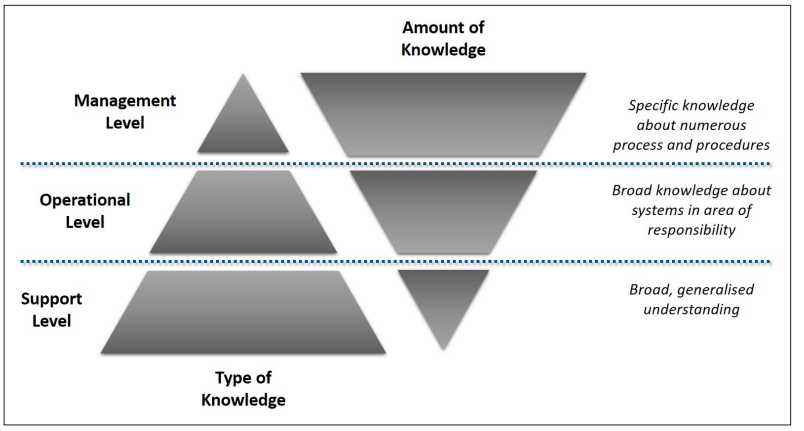

FIGURE 2. Type of knowledge vs. amount and breadth of knowledge.

seafarers are able to not only interact with risk management measures but also recognize when these measures have failed. Through this understanding, companies can provide the right competencies to seafarers, allowing them to implement appropriate responses to safety or security incidents.

The application of the five core functions of NIST (Identify, Protect, Detect, Respond, and Recover) to the hierarchy of responsibility could provide a framework for organizations to understand what competencies are required by crew to fulfill their roles within the core functions (Fig. 3), Illustrating that at each advancing tier, an individual should be able to perform the core functions to a higher degree.

Support Level: At this level, competencies would include a high-level basic awareness style of understanding. Often categorized as cyber hygiene, this awareness would include a basic understanding of their responsibilities. Alongside this, these seafarers would have the skills required to exercise basic cyber risk management practices, including the ability to identify phishing emails, good password practices, and personal device etiquette. As per [15], this is the level of knowledge that all crew members must demonstrate at inspection.

Operational Level: At this level, seafarers should be able to appropriately implement the awareness gained at the Support level. Furthermore, the crew should have a detailed understanding of the systems within their area of responsibility (navigational equipment or engine control, etc.). Training would provide an understanding of system interactions, and the risk posed to these systems, as well as safeguards, recovery measures, and redundancies. Crew competencies should also include the ability to autonomously recognize the occurrence of a cyber incident within their domain of responsibility, and provide recommendations to senior crew on its mitigation.

Management Level: These competencies would provide seafarers with a detailed ship-wide understanding of the ship's systems and their interactions. This knowledge would provide a detailed level of understanding that would allow personnel to identify and prioritize ship-wide risks and safeguards in the event of a cyber incident. This comprehensive understanding places the Master in a unique position onboard. The Master is best

The IMO has been able to produce a set of standardized competencies that ensure the operation-specific risk management requirements are addressed. Thus, at a regulatory level, to ensure that companies are considering digital competencies as part of their cyber risk management practices, a new requirement in the STCW Convention could be included. This requirement would mandate a minimum level of digital competencies for all levels of responsibility.

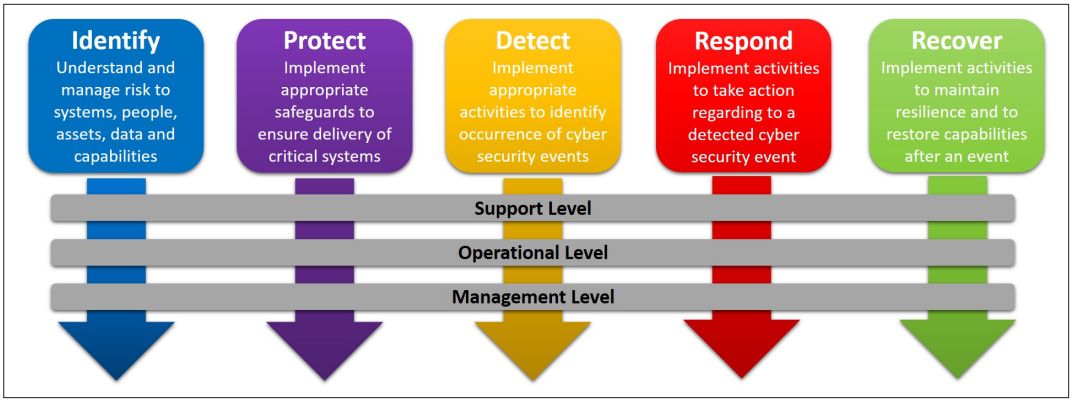

Figure 3. NIST framework with the STCW hierarchy overlaid.

able to disseminate information about the specific risks to the ship's system and its operations to other crew, especially junior personnel. Thus, at the Management level, the seafarer should attain the ability to disseminate, and discuss, cyber risk management practices competently to others, including other crew members, third-party service providers, and other business personnel.

Figure 4 demonstrates the escalating competencies of higher levels of assumed responsibility when aligned with the NIST core functions. Approaching digital competencies through this framework ensures that their development remains complementary to other risk management processes and mitigations rather than being an afterthought. What is more, as each ship, crew, and company is different, this framework allows developing holistic competencies to the individual needs of the ship, its crew, and its operations.

However, this approach is flawed, as the divide between the assumed levels of responsibility is too neat. To align with the development of a safety culture, organizations should be providing opportunities for those seafarers at lower levels of responsibility to engage further with digital competencies. To this end, the STCW Convention actively encourages all seafarers to request any training that they consider appropriate to their job role. Thus, to ensure the development of a resilient safety culture that addresses the constantly changing cyber risk landscape, companies should encourage all crew to actively strive toward a more knowledgeable work environment, allowing seafarers to make better-informed decisions that actively contribute to the continued safe operation of a ship.

Furthermore, while the application of the NIST framework allows companies to recognize the skills their seafarers require, it does little to address the diversity found within the workforce. Due to the nature of the maritime sector, seafarers have a diverse range of social and cultural backgrounds and will often move between ships. Ensuring that this workforce has the appropriate digital skills is challenging, especially considering the following factors:

- The varying levels of digital integration found on ships
- Crews' preconceived notions of cyber risk management
- The diversity in pre-existing technological experience

However, a company implementing a detailed SMS utilizing the NIST framework will ensure a minimum level of digital competency for their seafarers. The SMS would also recognize the need for an appropriate familiarization period as well as the need for other mitigation measures. Altogether, this would reduce the overall impact of workforce diversity.

Future Challenges and Opportunities

As with all industries, there is a constant proverbial game of catchup between technology and digital skills. The rapidly changing cybersecurity landscape means that seafarers are constantly facing new challenges to their everyday operations, and as such require the skills to manage these. This article has argued that cybersecurity and the digital competencies which underpin it are specific to companies, crews, and ship operations.

As discussed above, the IMO has been able to produce a set of standardized competencies which ensure that the operation-specific risk management requirements are addressed. Thus, at a regulatory level, to ensure that companies are considering digital competencies as part of their cyber risk management practices, a new requirement in the STCW Convention could be included. This requirement would mandate a minimum level of digital competencies for all levels of responsibility. This would include being able to:

- Understand basic cybersecurity concepts (*Identify*)
- Follow procedures to use systems in a safe and secure way (*Protect*)
- Recognize a potential cybersecurity incident (*Detect*)
- Know the procedures to follow in response to a cybersecurity incident (*Respond*)
- Take part in cybersecurity emergency and contingency procedures (*Recover*)

Thus, this allows organizations to determine what is appropriate to each level of responsibility within their operations, while ensuring a minimum level of digital competency across the sector.

Aside from the challenge of mandating standardized digital competencies, there are several challenges that the development of digital competencies must overcome.

Training Delivery: Due to the nature of maritime operations, the opportunities to provide

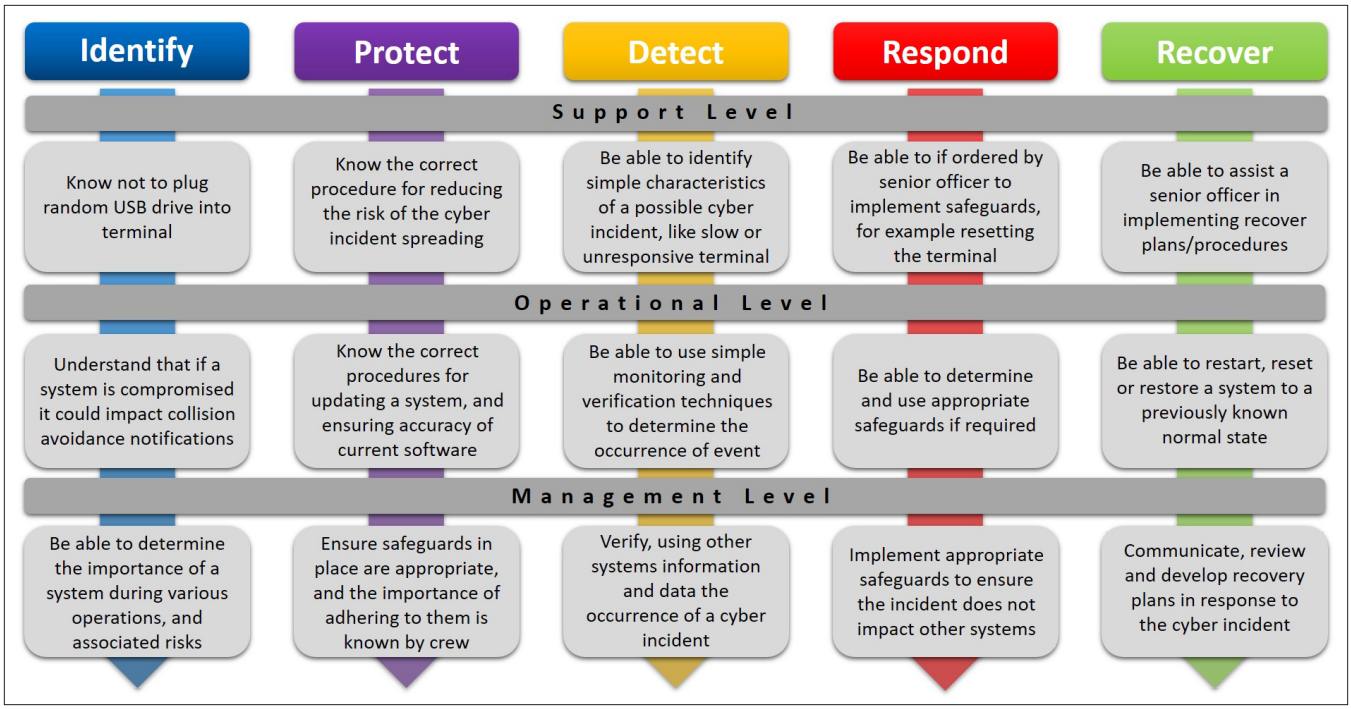

Figure 4. Demonstration of escalating competencies related to the NIST core functions.

training to seafarers are limited. Academy training offers the first opportunity to provide some digital competencies, like many other STCW competencies. However, as discussed, one-off training is not adequate, and companies must offer ongoing tailored training. Providing this type of training also faces challenges; for example, the timeframe for port calls is constantly reduced, giving limited time for seafarers to engage in face-to-face training. Moreover, port calls are an opportunity for seafarers to relax and socialize, so enforcing training during this time could be unpopular. Other challenges include the international nature of operations and the technical limitations of vessels when delivering e-learning.

Transfer of Skills Ashore: With increasing system complexity, it is realistic to imagine that a ship's crew may no longer have the skills required to maintain, service, and repair digital systems. Therefore, ships will become reliant on external engineers to ensure the continuity of their systems. This transfer may also change the duties and responsibilities of the crew onboard (e.g., meaning more monitoring and maintaining of systems), so they will require the skills to do this. Moreover, these engineers, whether accessing remotely or physically, will need appropriate training to understand the unique complexities of a ship's system, and operations to ensure that maintenance is completed safely.

More than Just Seafarers: The maritime sector consists of more than just ships and their crews. The sector includes ports and other service providers, each with their own personnel, completing different daily operations. However, the STCW Convention does not include these individuals, who play a vital role in maritime cybersecurity. As a consequence, the IMO has no ability to enforce the development of digital competencies for these individuals. In 2018, the EU ratified the NIS Directive, which lists ports and other maritime service providers as essential services. As such, these essential services must implement digital skill development to ensure the continued safety of the maritime industry. Therefore, the maritime sector, using other complementary regulatory requirements, needs to develop digital competencies that ensure the continued security and safety of the maritime sector.

Fully Autonomous Ships: As the industry continues to test the viability of autonomous vessels, the competencies of seafarers overseeing their operation also needs consideration. Traditionally, a ship's engineer would oversee the day-to-day maintenance of a ship's system, attempting to limp a ship to the closest port for repair. However, the removal of personnel on an autonomous ship raises important questions. Primarily, what skills do autonomous ship operators need to ensure the safety of operations? Second, what skills do engineers need to maintain these complex systems, and potentially be in a position where they need to manually sail the ship to port?

While the continued integration of technology into the maritime industry raises challenges, it also brings with it opportunities. First, as this article has illustrated, technology offers the opportunity for a safer and more secure working environment, leading to fewer maritime incidents. Furthermore, a company focusing on increasing its crews' digital skills will facilitate the development and enhancement of the company's safety culture. A company with a more mature safety culture will increase the likelihood that crew members are able to make knowledgeable decisions about systems, even in emergencies, which ensure the continued safety of the crew and vessel. There are also other benefits to be had from the integration of technology, including increased efficiency and reduced emissions, both of which contribute to a more sustainable and profitable maritime industry.

Technology also offers greater opportunities

In the near future, due to its requirements as the UN agency charged with ensuring maritime safety, the IMO is expected to include digital competencies within its regulatory instruments. It is therefore vital that these inclusions are created through collaboration with key stakeholders within the sector, thus ensuring that the standardized competencies are considerate of the variations within maritime operations.

to companies when providing training. With the increase of devices onboard and stable internet connections, companies can now develop their training offerings. This could include using emails, multimedia materials, online courses, and simulation to provide training that is engaging and has higher retention. What is more, utilizing the benefits of digital training's interactive elements ensures that training can keep pace with the constant developments and changes in the needs of the crew.

Conclusion

The maritime sector now faces an inevitable surge in digitalization, and the recent amendments to international regulation provide an opportunity to develop seafarers' digital skills. The process of adapting and amending seafarer competencies is by no means a quick and simple task. It will take time to ensure that these competencies match the intricacies of operations, the complexity of systems, and the expectations of operators. This article has outlined one way in which companies can utilize the NIST framework to identify key competencies that their personnel should acquire. As discussed, there could come a point in the future where, if seafarers cannot demonstrate appropriate cyber risk management knowledge, safety compliance certificates are withheld.

The article has also argued that the differences between the different types of maritime operations make it challenging to create a set of standardized digital competencies. In the near future, due to its requirements as the UN agency charged with ensuring maritime safety, the IMO is expected to include digital competencies within its regulatory instruments. It is therefore vital that these inclusions are created through the collaboration with key stakeholders within the sector, thus ensuring that the standardized competencies are considerate of the variations within maritime operations.

Acknowledgments

I would like to thank Dr. Kimberly Tam for her very helpful comments on earlier drafts of this article.

This article has been partially sponsored by the Engineering and Physical Sciences Research Council (EPSRC) as part of the Centre for Doctoral Training in Cyber Security at Royal Holloway, University of London (EP/P009301/1). This article is also partly funded by 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. The content reflects only the author's view, and funders are not responsible for any use that may be made of the information it contains.

References

[1] Organisation for Economic Co-operation and Development, "Ocean Shipping and Shipbuilding," 2021; https://www.oecd.org/ocean/topics/ ocean-shipping/#:~:text=The%20main%20transport%20mode%20for, transport%20arteries%20for%20global%20trade.
[2] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships via False GPS Signals: Demonstration and Detection," *NAVIGATION*, vol. 64, no. 1, 2017, pp. 51–66; https://doi.org/10.1002/navi.183.
[3] U. S. Dept. of Transportation Maritime Administration, "MSCI Advisory 2019-012 — Persian Gulf, Strait of Hormuz, Gulf of Oman, Arabian Sea, Red Sea — Threats to Commercial Vessels by Iran and its Proxies"; https://www.maritime.dot.gov/msci/ 2019-012-persian-gulf-strait-hormuz-gulf-oman-arabian-sea-red-sea-threats-commercial-2019.
[4] IMO, "Resolution MSC.428(98) — Maritime Cyber Risk Management in Safety Management Systems," 2017.
[5] IMO, *Int'l. Convention for the Safety of Life at Sea*, 2020.
[6] IAEA, "Safety Culture Practices for the Regulatory Body," 2020; https://www-pub.iaea.org/MTCD/Publications/PDF/TE-1895web.pdf.
[7] IMO, "Resolution A.772(18) — Fatigue Factors in Manning and Safety," 1993.
[8] IMO, "Resolution A.947(23) — Human Element Vision, Principles and Goals for the Organization," 2003.
[9] BIMCO, "Safety at Sea and BIMCO Cyber Security White Paper," 2020; https: //ihsmarkit.com/Info/1020/safety-at-sea-and-bimco-cyber-security.html.
[10] IMO, *International Convention on Standards of Training, Certification and Watchkeeping*, 2016.
[11] IMO, *International Safety Management Code*, 2014.
[12] IMO, , "MEPC 62/17/2 — Human and Organizational Factors — The Critical Role of 'Just Culture," 2011.
[13] ENISA, "Cyber Security Culture in Organisations," 2017; https://www.enisa.europa.eu/publications/ cyber-security-culture-in-organisations/at_download/fullReport
[14] M. Alshaikh, "Developing Cybersecurity Culture to Influence Employee Behaviour: A Practice Perspective," *Computers & Security*, vol. 98, 2020, pp. 1–10; https://doi.org/10.1016/j.cose.2020.102003.
[15] U. S. Coast Guard, "CVC-WI-027(1) — Vessel Cyber Risk Management Work Instruction," 2020; https://www.dco.uscg.mil/ Portals/9/DCO{\%}20Documents/5p/CG-5PC/CG-CVC/CVC_MMS/ CVC-WI-027(series).pdf.
[16] K. B. Belmont and J. Zola, "Cybersecurity Risk Managment Guidelines for the Maritime Industry," *PRATT'S Privacy and Cybersecurity Law Report*, vol. 4, no. 1, 2018, pp. 22–25.
[17] ISO Std., "ISO31000:2009(E) — Risk Management — Principles and Guidelines," Nov. 2009.
[18] ISO Std., "ISO27001:2013 — Information Technology — Security Techniques," Oct. 2013.
[19] U.S. Federal Aviation Authority, "Order 1370.106 — Information Systems Security Awareness and Training Policy," 2009; https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf, accessed 26 Feb. 2021.
[20] IMO, "MSC-FAL.1/Circ.3 — Guidelines on Maritime Cyber Risk Management," 2017.
[21] NIST, "Framework for Improving Critical Infrastructure Cybersecurity — Version 1.1," 2018; https://nvlpubs. nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdfx.

Biography

Rory Hopcraft (rory.hopcraft@plymouth.ac.uk) is a research fellow at the University of Plymouth. He is currently working on the EU Horizon 2020 CyberMAR Project. Prior to this, he researched his Ph.D. with the Centre of Doctoral Training in Cyber Security at Royal Holloway University. His research primarily focuses on the regulatory aspects of maritime cyber security. He has a keen interest in how the international community uses regulation and governance to increase security.