Enhanced Transparency: Improving Maritime Cyber Governance

1st Rory Hopcraft
Faculty of Science and Engineering
University of Plymouth
Plymouth, UK
https://orcid.org/0000-003-1962-6903

2nd Kimberly Tam
Faculty of Science and Engineering
University of Plymouth
Plymouth, UK
https://orcid.org/0000-0003-2840-5715

3rd Kemedi Moara-Nkwe
Faculty of Science and Engineering
University of Plymouth
Plymouth, UK
https://orcid.org/0000-0003-6449-2249

4th Kevin Jones
Faculty of Science and Engineering
University of Plymouth
Plymouth, UK
https://orcid.org/0000-0002-4960-0978

***Abstract*— Like all sectors, there has been a rise in the integration of technology into everyday operations. This paper will argue that one of the main benefits of this integration is improved transparency of the cyber risk landscape. This transparency acts to enhance the cyber situational awareness of individuals, companies and regulators. This heightened awareness of the cyber risks the maritime sector faces will allow better-informed cyber governance mechanisms to be implemented at all levels of the maritime sector. These mechanisms will include company specific policies that are considerate of operational-specific risks and practices, as well as international level regulatory requirements, which cover high-level risks to the sector more broadly. To do this the paper will firstly explore what situational awareness is and how it is important to decision-making. The paper will then explore the role of technology in enhancing situational awareness. Finally, the paper will discuss how this heightened situational awareness can be utilized to develop cyber governance within the sector.**

Keywords*— Maritime, cyber risk, cyber security, situational awareness, governance

I. Introduction

Every industry has seen a rapid expansion of technology integrated into everyday operations over the last decade. These technologies form vast networks of connected devices including remote monitoring systems, autonomous control systems, and a plethora of IoT devices [3]. With the rising demand for connectivity by seafarers, many of these connected devices are not company assets. Yet, these devices connect to company networks and have the potential to introduce new risks to maritime technologies. A trend that the COVID-19 pandemic has only exacerbated [4].

The integration of connected technologies brings with it both advantages and disadvantages. Many of these new technologies are introduced to improve the efficiency of maritime operations, while also increasing the safety and security of seafarers. However, with much of this technology connected to the internet, the maritime sector now faces a broadening cyber risk landscape. Company-specific factors like operational requirements, crew skill level, physical system integration, and general cyber security preparedness, complicate this risk landscape further.

The complexity of systems and their integration makes understanding the risk landscape challenging. In turn, this complexity makes governing these systems a non-trivial undertaking. In 2017, in an attempt to raise awareness of cyber risk, the International Maritime Organization (IMO) released Resolution MSC.428(98) [5]. This resolution stipulated that by January 2021 a ship's safety management system (SMS) should include cyber risk management. However, this is just the first step in a long journey towards the development of robust and resilient maritime cyber governance [6].

This paper will argue that while the integration of technology into the maritime sector does not come without risks. However, if done correctly it can have a number of benefits. One of these benefits is that a company can enjoy increased transparency around their own cyber risk. Thus, allowing companies to implement cyber risk management practices that are appropriate to their specific risk landscape. Furthermore, through the process of enforcing the assessment and implementation of cyber risk management, the IMO itself will become more informed about sectoral-specific cyber risks. This additional transparency will allow the IMO to discuss, create, and ratify internationally agreed regulations that will enhance the cybersecurity stance of the whole sector.

As [7] points out, an enhancement of situational awareness if often desirable as a way to reduce cyber risk. Therefore, the paper will start by discussing the important role that situational awareness plays in decision-making. The paper will then go onto discuss how, through the engagement with technologies, companies can improve their situational awareness. One example that this paper will use is the EU Horizon 2020 CyberMAR project. The CyberMAR platform aims to provide a digital environment through which companies can engage with and develop their cyber risk management practices [8]. Engagement with technologies that allow companies to enhance their situational awareness ensuring an information-rich decision-making environment. Leading to more effective cyber risk governance, which does not compromise the safety or security of the sector.

Finally, the paper will discuss how IMO Resolution MSC428(98) will improve the situational awareness of the IMO decision-making. The Resolution obligates companies and administrations to document their cyber risk management practices. Thus, by documenting, and sharing these practices where appropriate, the sector as a whole can

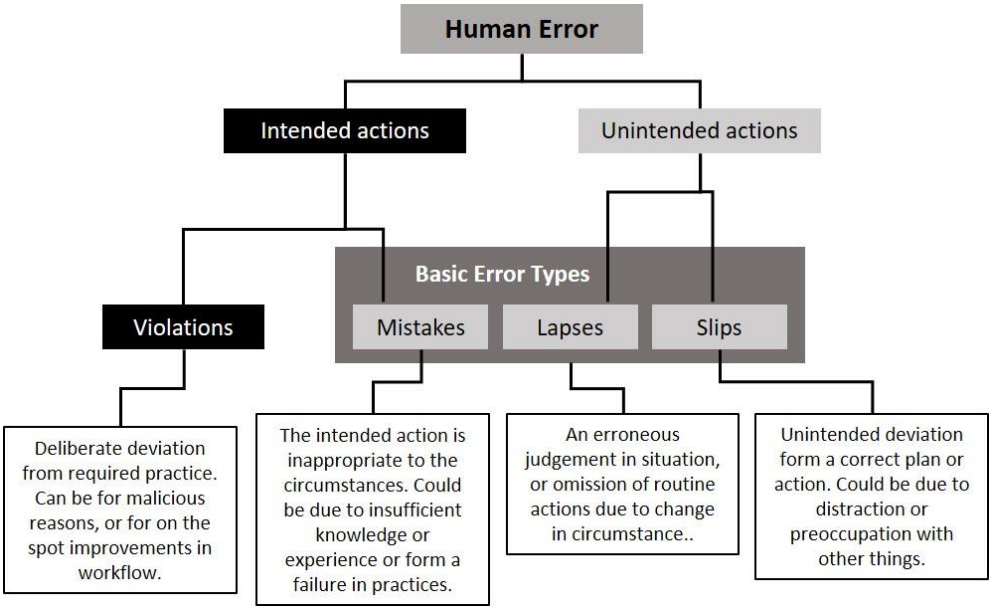

Figure 1: Summarized Sources of Human Error (adapted from [2])

work together to develop a mature understanding of cyber risk. More importantly, feeding this information back into the IMO's governance mechanisms will further enhance the ability of the IMO to create robust and resilient cyber risk governance. What is more, this bottom-up approach to development ensures that any future governance not only considers the broad risks faced by the sector at large, but also the sub-sector-specific risks. For example, a cruise ship and an LNG tanker will share some risks while having some specific to just them.

II. Situational Awareness

The maritime sector has always focused on safety, and the human elements ability to make good decisions. IMO Resolution A.947(23) clearly draws the link between training, experience, skill and safety, with the long-term aim to ensure the human element are best equipped to "do the right thing" [9]. Doing the right thing signifies an action, and in the context of safety, this means taking the right action to ensure the continued safety of the vessel, crew and environment.

As [10] argues, it is often difficult to trace the single cause of maritime incidents back to human error. However, it can be argued that inadequate design, inadequate training or instruction and inadequate attention by the operator are often the major contributors to many incidents [11]. Therefore, cyber risk management and governance should ensure that these factors are considered during the integration, and operation of, digital systems.

However, there are parallels between human error and governance creation. As [2] illustrates (see Fig.1) there are various elements to human error. These errors can translate into governance decision-making, whereby violations are deliberate actions that lead to an undesirable outcome e.g. blocking governance proposals that are seen as too costly. This is something that the members of the IMO have been accused of in the past when discussing pollution prevention [12]. However, on the matter of safety, the safety of life should be considered paramount. Mistakes, lapses and slips are unintentional errors where a lack of judgement or understanding of the proceeding outcomes leads to an error. This is where technology can help improve understanding of governance stakeholders, increasing their cyber situational awareness. In turn this knowledge-rich decision-making environment will reduce the chances of unintentional errors in cyber governance.

The situational awareness decision-making loop, as shown in Fig. 2, further illustrates how situational awareness is a fundamental part of decision-making. At the most basic level in a safety context, situational awareness refers to being aware of what is happening around you in terms of, where you are, where you are supposed to be, and whether anyone of anything around you is a threat to your safety [13]. Therefore, in a sector where safety is paramount, the ability to understand the environment around you and understand how this affects decision-making is vital.

Endsley [14] argues that situational awareness comprises of three stages: perception, comprehension and projection. Whereby, "Situational Awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning and the projection of their status in the near future" [14]. Perception is the most basic of situational awareness, where there is simple recognition of elements pertaining to the operational environment (e.g. objects, people, systems, events). Comprehension comprises of the symphysis of those elements into understanding their impact on goals and

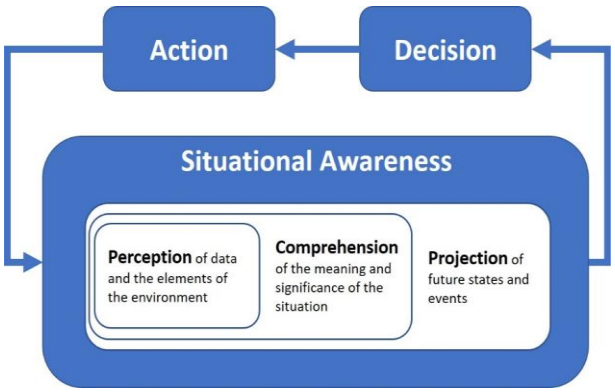

Figure 2: Situational Awareness Loop – Source: [1]

objectives. The third stage is projection, where this knowledge is extrapolated to understand how it will affect future states of the operational environment. Each of these three stages provides some enhancement in situational awareness, but the ability to move from perception to projection will enhance it further.

The maritime sector has always sought to improve safety through developing a better understanding of their operational environment by enhancing situational awareness. For instance, the inclusion of Electronic Chart Display and Information Systems (ECDIS) on board all SOLAS vessels. Utilizing these electronic charts allows the seafarer to enhance their perception of the elements within their operational environment, all overlaid on a chart in relation to their current position. Through the graphical representation of various data sources (e.g. location of other ships, location of sandbars, depths, currents etc.) the seafarer can comprehend how these elements affect their operations in real time. Furthermore, the ability to interrogate this information with the use of other sources of information (e.g. radar) allows the seafarer to make decisions in a timely manner, to proactively avoid unsafe situations.

The same is true for the maritime governance mechanisms. The IMO has encouraged the engagement of experts within their regulatory discussion. This engagement is achieved through the inclusion of non-governmental organizations like BIMCO or the International Chamber of Commerce [15]. As well as through encouraging member states to bring academics and specialist to IMO meetings. As both [16, 17] illustrate, this expertise helps to fill the knowledge gap within the governance discussion, increasing the situational awareness of those discussions.

This additional awareness is important when those governance discussions turn towards cyber risk management. [7] argues that cyber situational awareness is a sub-set of situational awareness. As such, [18] argues that maritime cyber situational awareness comprises of a mix of the traditional physical, static and dynamic elements of situational awareness with cyber elements. To achieve a good level of situational awareness a detailed perception, comprehension and projection of these elements is required. The physical element consists of maritime infrastructure that is present, for example the ship machinery and systems. The static element consists of factors that do not change, these factors include, ship type, age, flag, tonnage etc. [19]. The dynamic element is factors that change, and continue to change throughout operations [20], such as speed, weather, coastline layout etc. [21]. The cyber element consists of understanding the integration of IT and OT devices into everyday operations, and the technical components and interactions of those devices [18].

Therefore, to ensure that good cyber risk governance decisions are made, companies must have a detailed understanding of all these elements, their interactions, and their influence on operations. As such, there is little benefit for a company implementing governance mechanisms that do not consider dynamic elements like operational environment for instance. By way of example, [22] illustrates the adverse effects that weather can have on ship machinery efficiency, and the risks this could pose to safety. Moreover, as discussed above, humans are an "indispensable component" of situational awareness [23]. Thus, operators should be able to interrogate the information from these systems and integrate this into their situational awareness.

This detailed situational awareness is sometimes referred to as a common operational picture (COP), when it is considering as part of the command and control processes. As [24] argues, a core part of the COP is the detailed picture of information about vessel movements, their operations, the coastal environment. [24] goes onto argue that this information needs to be overlaid with as much information about the "enemy", in this case cyber risks. Thus, as much information is needed about these risks goal, intention and capability.

Thus, by enhancing cyber situational awareness it raises the transparency of the cyber risk landscape allowing the maritime sector to make better-informed decisions. This enhancement of situational awareness will have a two-fold impact. Firstly, it will allow operators to make better-informed operational decisions that do not compromise safety or security. Secondly, a raise in situational awareness will ensure that companies are able to create and implement cyber risk governance that is appropriate to the company-specific and operational-specific risks they face. This is vital as every ship has different functionalities, utilizes different systems and operates within different crews in different environments. Companies also have different operational practices, using different systems and are subject to different geographical constraints. As cyber risk management is not only focused on safety, but also security, it is important to consider the influence of malicious system compromise. Again, the motivations behind these attacks will differ depending on the instigators resource level, and the desired outcome.

III. USING TECHNOLOGY TO EHNANCE SITUATIONAL AWARENESS

Arguably, the maritime sector has always utilized various technologies to enhance the seafarers understanding of their operational environments. Rather than rely on the use of many different screens and dials, ECDIS offers a way to consolidate this information into a single, easy to use and universal medium. This simplicity ensure that seafarers have easy access to enough information to develop a detailed situational awareness of their operations. What is more, because ECDIS is a software-based piece of technology it can be adapted as technology changes. This allows companies to collect and present more information collected from sensors around the ship to the seafarer. As the seafarer has the ability to select what information they see this ensures have as much information as they need to make well-informed decisions. However, it is worth noting that there are risks associated with embracing technology within the maritime sector. For instance, [25] notes that automation in the maritime sector can lead to an increase in human stress, consequently leading to more human errors.

As discussed above, good decision-making occurs in an information-rich environment, and technology offers a way to complement and enhance that information gathering. As [7] argues that data from sensors, alongside other sources like news reports can provide additional insight into the situation. Using technology can aid the evaluation analysis and forecasting capabilities [24]. Both through the

engagement of software designed for this purpose, and through data collection for more technological sources feeding this software. This ability to use technology to fuse information together has been the driving force for the German Remote Sensing Data Center [26].

As [23] argues that there are various aspects that complement the process of situational awareness and achieving the goal of cyber risk management. The first of these aspects is the identification of better response plans and actions. Incident response is normally considered separately to situational awareness. However, without good situational awareness a company cannot effectively develop and implement response plans and actions. The second aspect that needs to be developed is the ability to make decisions on the course of action to take. Situational awareness only prepares a decision-maker to understand the situation up to the point a decision is made. Improved cyber risk management needs to ensure decision-makers are able to understand the consequences of their decisions and make decisions as a result of their initial actions.

There are various ways through which cyber situational awareness can be gained e.g. intrusion detection, trend analysis and digital forensics. However, these methods are limited in their approach [23], as they require humans to complete the synthesis of this data at the comprehension and projection phases of situational awareness. However, there are technologies that can be utilized to help the human element synthesis the data available and make informed decisions. These include the use of platforms like the Cyber-MAR, or engagement with research facilities like the CyberSHIP lab.

As briefly mentioned earlier, the Cyber-MAR project aims to develop an innovative cyber security simulation environment [27]. A simulated environment is a representation of an organization's ICT, OT and physical systems, application and infrastructures [28]. This simulated environment allows users and companies to create company-specific network topologies. It is against these simulated environments that companies can then employ a range of tools, attacks and procedures without risk to the organization's actual infrastructure [29].

The process of creating these topologies accurately requires companies to have a detailed understanding of their networks and its interactions. Therefore, just the initial planning phases of utilizing a cyber range can lead to an improvement in a company's cyber situational awareness. The testing functionality of the platform allows companies to understand what risks their systems face, and how the integration affects these risks. This ability to test risks allows companies to develop internal cyber risk governance strategies e.g. password policies or access control policies, which are considerate of their operations and risks. This testing also allows companies to develop response plans for various eventualities. Furthermore, as [30] argues, cyber ranges offer an opportunity for companies to develop personnel situational awareness. This development occurs through the exposing of personnel to the information from multiple sources within the simulated environment. Thus, allowing personnel to gain experience in synthesizing this amount of data and making decisions in a safe and control environment.

However, in a recent training session delivered by Cyber-MAR, of 50+ participants roughly 51% had only heard of cyber-ranges a little, 33% had never heard of a cyber-range (CR), and roughly, 16% knew of this technology fairly well. As discussed above cyber ranges offer a useful tool for companies to understand and test their cyber risk management practices. Thus, more should be done to raise awareness about these platforms as a way to improve cyber situational awareness. Training participants were most interested in using CRs for risk assessment, followed by vulnerability identification, and then analysis of the exercise. Of the participants, the vast majority were interested in both Information and Operational Technology (IT/OT), with only one person interested in IT only and another interested in OT only.

Another way to meet needs for IT/OT risk assessment and vulnerability identification is with real equipment, not simulated or emulated, for higher fidelity. There are various testbeds for Industrial Control Systems (ICS), but just as a cyber-range based scenarios and training differ between the maritime sector and others, testbeds will also require a different set of capabilities when designed to best serve this sector. One growing research capability that meets this is the Cyber-SHIP (i.e. Software, Hardware, Information, Protection) Lab [31] which applies realistic, controllable, safe, and repeatable experiments to marine systems to improve understanding of maritime cyber security. In particular, this improves risk assessment of single systems, and the interconnected system-of-systems from the hardware, to the software, to the human-in-the-loop. Again, the use of this technology enhances a company's cyber situational awareness, and act appropriately to mitigate them.

IV. Improving Cyber Risk Management and Governance

As argued above, the development of situational awareness and transparency is a two-fold process. Firstly, by operators engaging with more technology they can themselves develop their situational awareness. In turn, this gain in situational awareness will lead them to improve their cyber risk management decision-making. The section above has discussed how, through these technologies, companies can enhance their situational awareness and develop their own cyber governance.

This section will focus on the second phase of this process. Due to the reporting and documentation requirements of the IMO, the improved situational awareness at the lowest governance level (company level) will be fed into the middle level governance (national authority). In turn, this will be then fed into the highest level (international level). This improved transparency will ensure that any future international regulations and requirements are considerate of the specific factors at all levels of the sector (e.g. operational, environmental, cultural and national specific requirements).

[24] provides a simplistic, but effective, framework for understanding situational awareness and could be used to understand how maritime cyber governance could be improved. The authors devise three inputs needed for understanding the operational environment. Firstly, there are the threat indicators. These indicators are situations that would lead up to an undesirable situation occurring. In

other words, situations where the normal process and activity patterns are no longer followed. The next element are observables. These observables describe the current situation of the operational environment e.g. vessel speed, size etc. The third and most important element is intelligence. Intelligence is what provides context about the observables and how these may change.

As such, through the engagement of these three elements better fusion and analysis can occur, which in turn can develop governance. For Instance, the IMO has currently only released Resolution MSC.428(98), in dealing with maritime cyber risk. It has been argued that the primary reasoning behind the placement of cyber risk in a ships SMS was to ensure companies were assessing their risks and eventually this would filter back to the IMO [6]. This Resolution, because of the IMO's documentation requirements enforces transparency at all level throughout the sector in principle. Arguably, the IMO has a good understanding of the normal process and activity patterns within the maritime sector. Whereby, as companies have to have their SMS's approved by their national authorities, who in turn engage directly with the IMO governance processes. Thus, the standard operational patterns and activities are already heavily regulated and understood, due to the IMO's long history of maritime governance. Thus, the IMO already understand the undesirable situations and obviously wish to avoid those from occurring. The engagement of a bottom-up approach by companies completing cyber risk management processes ensures the IMO can start to gather both observables and intelligence.

The IMO itself does not sensor data directly, rather relying on national authorities for that information. However, the IMO does collect and collate a wealth of information from national authorities and makes this available through the Global Integrated Shipping Information System (GISIS) [32]. Thus, as companies produce their cyber risk management strategies, and national authorities approve these, the IMO will gain more information about the sectors cyber threat landscape. This intelligence gathered through the national authorities will allow the IMO to provide context to the understood activity patterns and determine how this potentially affects the safety of operations.

One way in which this information could be feedback into the governance process within the IMO is through the amendment of its various instruments. For instance, the requirements of the International Safety Management (ISM) Code could be amended to explicitly include cyber risk management practices e.g. the inclusion of cyber training drills. Another possibility is the amendment of the International Ship and port Facility Security (ISPS) Code, which looks at the security processes of ships and ports. Again, amendments to this instrument could be the inclusion of specific risk management practices like the installation of redundancies for all critical systems.

The final, and probably one of the most important instruments that could be amended is the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW). As this paper has argued, the human element plays a vital role in cyber risk management. The paper has also argued that to ensure humans can make good decisions they must be equipped with the appropriate knowledge and skills to gain and process that knowledge (i.e. situational awareness). Through the IMO improving its own situational awareness, through the engagement with the cyber risk assessments carried out by operators, they can in turn improve the competencies required by maritime personnel. As such, these competencies would include the ability to gather and process data to better understand the implications of their decisions.

V. Conclusions

This paper has briefly explored the importance of situational awareness in decision-making, and how the engagement with technology can help enhance this. The raising of cyber situational awareness throughout the maritime sector will have a dramatic positive impact on the resilience of the maritime sector. Firstly, through the improvement of an operator's situational awareness, they are better prepared to make decisions that do not compromise the safety and security of operations. Secondly, as companies improve their cyber situational awareness they will increase the transparency and understanding of their cyber risk landscape. This in turn will ensure they are able to implement appropriate governance mechanisms to mitigate those risks. Thirdly, and most importantly, the bottom-up approach to cyber risk management adopted by the IMO will ensure the enhancement of their situational awareness within governance discussion. Allowing the IMO to discuss, create and ratify cyber risk governance frameworks that are considerate of both the sector-side risks as well as the subsector-specific risks.

Acknowledgment

This paper is a partly funded by the research efforts under Cyber-MAR. 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

1. Stan Institute, *Situational Awareness*, 2015, Available from: https://stan-institute.com/en/news/situational-awareness/.

2. Barnett, M.L., *Searching for the Root Causes of mariitme Casualties.* WMU Journal of Maritime Affairs, 2005. **4**(2): p. 131-145.

3. Verchot, M. *Shipping Industry Bets Big on IoT in Bid to Save Billions*. 2019; Available from: https://spectrum.ieee.org/tech-talk/telecom/internet/shipping-industry-bets-big-on-iot-in-bid-to-save-billions.

4. UNCTAD, *COVID-19 and Maritime Transport: Impact and Responses*, 2020, Available from: https://unctad.org/system/files/official-document/dtltlbinf2020d1_en.pdf.

5. International Maritime Organization, *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*. 2017, International Maritime Organization: London.

6. Hopcraft, R. and K.M. Martin, *Effective maritime cybersecurity regulation – the case for a cyber code.* Journal of the Indian Ocean Region, 2018. **14**(3): p. 354-366.

7. Franke, U. and J. Brynielsson, *Cyber situational awareness - A systematic review of the literature.* Comput. Secur., 2014. **46**: p. 18-31.

8. Cyber-MAR, *Cyber-MAR - The Project at a Glance*, 2019, Available from: https://www.cyber-mar.eu/about/.

9. International Maritime Organization, *Resolution A.947(23) - Human Element Vision, Principles and Golas for the Organization*. 2003, International Maritime Organization: London.

10. Hetherington, C., R. Flin, and K. Mearns, *Safety in Shipping: The Human Element.* Journal of Safety Research, 2006. **37**: p. 401-411.

11. Singleton, W.T., *Theoretical Approaches to Human Error*. Ergonomics, 1973. **16**(6): p. 727-737.

12. Influence Map, *Corporate Capture of the IMO*, 2017, Available from: https://influencemap.org/report/Corporate-capture-of-the-IMO-902bf81c05a0591c551f965020623fda.

13. Health and Safety Executive, *Knowing what is going on around you (situational awareness)*, 2012, Available from: https://www.hse.gov.uk/construction/lwit/assets/downloads/situational-awareness.pdf.

14. Endsley, M.R., *Toward a Theory of Situation Awareness in Dynamic Systems.* Human Factors, 1995. **37**(1): p. 32-64.

15. International Maritime Organization, *Rules and Guidelines for Consultative Status of Non-Governmental International Organizations with the International Maritime Organization*, 2019, Available from: http://www.imo.org/en/About/Membership/Documents/RULES%20AND%20GUIDELINES%20FOR%20CONSULTATIVE%20STATUS%20-%20December%202019.pdf.

16. Haas, P.M., *Policy Knowledge: Epistemic Communities*, in *International Encyclopedia of the Social & Behavioral Sciences*, N.J. Smelser and P.B. Baltes, Editors. 2001, Pergamon: Oxford. p. 11578-11586.

17. Radaelli, C.M., *The public policy of the European Union: whither politics of expertise?* Journal of European Public Policy, 1999. **6**(5): p. 757-774.

18. Tam, K. and K.D. Jones, *Situational Awareness: Examining Factors that Affect Cyber-Risks in the Maritime Sector.* Int. J. Cyber Situational Aware., 2019. **4**(1): p. 40-68.

19. Balmat, J.-F., F. Lafont, R. Maifret, and N. Pessel, *MAritime RISk Assessment (MARISA), a fuzzy approach to define an individual ship risk factor.* Ocean Engineering, 2009. **36**(15): p. 1278-1286.

20. Dinis, D., A.P. Teixeira, and C. Guedes Soares, *Probabilistic approach for characterising the static risk of ships using Bayesian networks.* Reliability Engineering & System Safety, 2020. **203**: p. 107073.

21. Koldenhof, Y., C. Van der Tak, and C. Glansdorp. *Risk Awareness; a model to calculate the risk of a ship dynamically*. in *International Scientific and Technical Conference on Maritime Traffic Engineering*. 2009.

22. Vanem, E. and A. Brandsaeter, *Regression models for the effect of environmental conditions on the efficienct of ships machinery systems*, in *Risk, Reliability and Safety: Innovating Theory and Practice*, L. Walls, M. Revie, and T. Bedford, Editors. 2017, Tayloe & Francis Group: London. p. 362-374.

23. Barford, P., et al., *Cyber SA: Situational Awareness for Cyber Defense*, in *Cyber Situational Awareness: Issues and Research*, S. Jajodia, et al., Editors. 2010, Springer US: Boston, MA. p. 3-13.

24. Broek, A.C.v.d., R.M. Neef, P. Hanckmann, S.P.v. Gosliga, and D.v. Halsema. *Improving maritime situational awareness by fusing sensor information and intelligence*. in *14th International Conference on Information Fusion*. 2011.

25. Tam, K., R. Hopcraft, T. Crichton, and K. Jones, *The potential mental health effects of remote control in an autonomous maritime world.* Journal of International Maritime Safety, Environmental Affairs, and Shipping, 2021. **5**(2): p. 51-66.

26. Schwarz, E., D. Krause, M. Berg, H. Daedelow, and H. Maass, *Near Real Time Applications for Maritime Situational Awareness.* ISPRS - International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, 2015. **XL7**: p. 999.

27. Cyber-MAR, *Cyber-MAR Fact Sheet*, 2019, Available from: https://www.cyber-mar.eu/wp-content/uploads/2019/12/Cyber-MAR_Fact-sheet_v.4.pdf.

28. NIST, *The Cyber Range: A Guide*, 2020, Available from: https://www.nist.gov/system/files/documents/2020/06/25/The%20Cyber%20Range%20-%20A%20Guide%20%28NIST-NICE%29%20%28Draft%29%20-%20062420_1315.pdf.

29. Priyadarshini, I., *Features and Architecture of The Modern Cyber Range: A Qualitative Analysis and Survey*. 2018.

30. Debatty, T. and W. Mees. *Building a Cyber Range for training CyberDefense Situation Awareness*. in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*. 2019.

31. University of Plymouth. *Cyber-SHIP Lab*. 2021; Available from: https://www.plymouth.ac.uk/research/cyber-ship-lab.

32. International Maritime Organization. *Global Integrated Shipping Information System*. 2021; Available from: https://gisis.imo.org/Public/Default.aspx.