TRANSNAV
http://www.transnav.eu
the International Journal
on Marine Navigation
and Safety of Sea Transportation
Volume 15
Number 1
March 2021

DOI: 10.12716/1001.15.01.01

An Operational Approach to Maritime Cyber Resilience

E. Erstad[1], R. Ostnes[1] & M.S. Lund[2]
[1]*Norwegian University of Science and Technology, Ålesund, Norway*
[2]*Norwegian Defence University College, Lillehammer, Norway*

ABSTRACT: As a result of the last decades development of technology and increased connectivity of maritime vessels, the need for maritime cyber security is undoubtedly present. In 2017, IMO officially recognized "… the urgent need to raise awareness on cyber threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks". Thus, Maritime Cyber Resilience is seen as key by IMO in the improvement of the maritime cyber security. It is assumed that human error is the cause of more than half successful cyber-attacks. If technology somehow fails, in example because of a cyber threat, the human is expected to handle the problem and provide a solution. It is therefore necessary to focus on the human aspect when considering maritime cyber threats. This paper aims to provide a working definition of "Maritime Cyber Resilience". Further, the paper argues why the human should be a focus of study, as the human is at the sharp edge in a potential maritime cyber emergency.

1 INTRODUCTION

There is no longer a question of "if" an organization is harmed by a cyber incident, but "when" [41]. There is therefore a need for cyber resiliency in maritime operations. International Maritime Organization (IMO) recognizes in the resolution "Maritime Cyber Risk Management in the Safety Management Systems" [31] that shipping needs to be operationally resilient towards cyber risks. Thus, the concept of "Maritime Cyber Resilience" can be seen as of importance in the improvement of maritime cyber security.

IMO, as the global standard-setting authority for the safety and security in shipping, further provides the "Guidelines on Cyber Risk Management" [29], as a result of the resolution [31]. The guidelines provide high-level recommendations for maritime cyber risk management and includes functional elements to mitigate cyber risks. IMO urges ship owners to implement a cyber risk management approach, which is meant to be resilient towards cyber risks. This raises the question regarding what maritime cyber resilience is and how it can be defined. Resilience and risk, as well as robustness, are connected terms, yet not the same thing [38]. "Cyber risk management" is properly addressed in the Guidelines and means "… the process of identifying, analyzing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders." [29]. Even though maritime cyber resilience is also addressed by IMO, it is not as properly defined in the way that cyber risk management is. As maritime cyber resilience is stated of importance for IMO, it should be useful to produce a working definition of the term for future research.

A literature review was conducted in March 2021, aiming to find a definition of "Maritime Cyber

Resilience". The search phrase "Maritime Cyber Resilience" was searched for in the "International Journal on Marine Navigation and Safety of Sea Transportation" (TransNav) [55], Sage Journals [49], as well as Springer Link [51], which provided zero results and no definition. In addition, a search on Oria [46], the Norwegian University of Science and Technology (NTNU) library search engine covering the most of what NTNU University Library has to offer, only four different articles [13, 34, 36, 44] were provided as results, whereas none of the articles provided a definition of what maritime cyber resilience is. This article aims to provide a working definition of "maritime cyber resilience" which can be used in future research. This will be achieved through breaking up the term and analyze what is important to consider in each momentum of the term. In addition, the operational aspect of maritime cyber resilience will be explored, by investigating the human aspect in maritime cyber resilience.

Traditionally, there are two ways to address a maritime risk: by technological measures or by human factors [17]. Commercial cyber security protection measures provided by companies aiming to make ship systems cyber secure are mostly technical protection mechanisms. Fitton, Prince, Germond and Lacy [16] describe the maritime environment as divided into three elements: information, technology, and people. However, more attention is given to the technical aspect of cyber security [4, 8, 27], than the human aspect. Furthermore, several guidelines emphasize the importance of technical maritime cyber security and resilience [5, 15, 26]. The solutions provide less considerations to operational aspect of maritime cyber security and resilience, and what the human, e.g. the navigator, are supposed to do if e.g. the navigational systems fail to function. Humans are often considered the weak link in a sociotechnical system, however, also the agent of a system which can bring order to an emergency situation [11]. There is a connection between unexpected events and lack of control [58], and when technology fails the human is expected to "take the wheel" [3]. It is important to note that the implementation of more technology in a maritime system does not necessarily cohere with the reduction of human error [48]. Maritime organizations are different [29], and every maritime vessel may be considered a prototype [7]. This may argue why the human aspect is important for the concept of maritime cyber resilience, especially in a nautical operation.

Section 1 has provided background and introduction to the paper, as well as a literature review of "Maritime Cyber Resilience". Section 2 will explore what a maritime operation is, emphasizing the nautical part of a maritime operation, as well as the problems connected with navigation. Section 3 explores the concept maritime cyber security, what is threatening the operation of navigation and how the cyber threats have been tackled traditionally. Further, section 4 investigates the concept of cyber resilience, deriving from the concept cyber security being merged with the concept of resilience. The three previous sections will be synthesized in section 5, explaining how maritime cyber resilience can be defined. Section 6 will describe how a cyber threat situation is different from a more known emergency, and further emphasize why the human is important in this setting. Section 7 provides summary and conclusion.

2 MARITIME OPERATION

This section will explore the nautical part of a "maritime operation", as well as highlighting what is important for such operations. All over the world there are maritime operations going on, such as offshore operations, fishing, military operations, and passenger/cargo operations. A maritime operation can even be the remote operation of a vessel from land, or the coordination of a search- and rescue operation from a rescue coordination centre. The maritime operation will be dependent on the context of the operation. The words by themselves have a board meaning, as "maritime" can be defined as "connected with human activities at sea" or "near the sea or coast" [9], and "operation" can be defined as "an activity that is planned to achieve something" [10]. Thus, maritime operations can be many things, but at least it must be related to human activities to achieve something at sea, or in relation to the sea. One very important aspect of most maritime operations is the need to know one's position and direction, which makes the concept of navigation of importance to the maritime operations.

A ship's bridge can be considered as a socio-technical system [11] on which the navigator is the responsible actor expected to ensure the vessel's safety and security. The navigator interacts with the navigational instruments, as well as with other crew members of the bridge team and others in the maritime traffic system. The navigator has three main duties: navigation, collision avoidance and ship management [7], and part of this is the navigator's responsibility to find and fix the vessel's position. Traditionally this was carried out manually, while navigators today work more like system operators, monitoring the vessel's automatic presented position on the ECDIS (Electronic Chart Display and Information System) [7], usually with the input of a GNSS (Global Navigation Satellite System) sensor [20]. This gives the navigator the opportunity to perform also other tasks, as the vessel's position is automatically projected on the ECDIS.

Navigation is a technology driven practice [29], ranging from celestial navigation with relatively unprecise precision, to electronical navigation with high precision [7], close to centimeter positioning of the vessel. From earlier days, a ship's position was determined by the stars and the sun, and as the technology developed, more advanced instruments have been introduced to the ship bridge. Several types of navigation are available, for example dead reckoning, piloting, celestial navigation, radio navigation, RADAR (RAdio Detection And Ranging) navigation and satellite navigation [7, 12]. Whatever methods a navigator chooses to use, there are usually three challenges to be solved considering navigation. These are the determination of position, direction and distance [12], which will provide the navigator with the vessel's previous-, present-, and predicted future position. The International Convention for the Safety of Life at Sea (SOLAS), chapter V/15 provides

regulations regarding bridge design as well as SOLAS V/18 provides performance standards of type approved navigational systems. Also, Integrated Navigation Systems (INS) are recommended by IMO [30] to be installed on ships built after 2011.

Today, the vessels are operated by both IT (Information Technology) and OT (Operational Technology) systems [5]. IT-systems are used for storing and processing data information, such as information on persons onboard the vessel and their next of kin, the different policies and procedures relevant for the vessel, the vessel's certificates and compliance documents, amongst other information. OT-systems are used for controlling the vessel and its movement, as well as controlling the industrial systems onboard, such as thruster direction and force, rudder angle, cargo handling, ballast water handling, power distribution and navigational aiding system [5]. As the navigational systems are becoming more digitalized and increasingly being networked, the ships are getting more dependent on cyber systems for safe and efficient navigation [20].

To summarize this section, the nautical operation can be claimed to be of great importance for maritime operations where ships are involved. The navigator needs to know where the vessel is to carry out safe operations. In next section, maritime cyber security will be explored.

3 MARITIME CYBER SECURITY

There is a lot of problems connected with the concept of maritime cyber security and the research area is not well studied [14]. "Cyber security" derives from "information security", and are similar terms, but not the same [50]. What distinguish these terms are what they are protecting. Information in itself can both be in knowledge, material or electronic form [36], however, in this paper only the electronic form will be addressed. Information security concerns the protection of data information, such as administration of business plans and procedures, as well as the technological structures and protection measures around the information. In its most general sense, cyber security concerns the protection of cyber-systems against cyber threats [47]. Cyber security comprehends a broader meaning than information security, including everything from the protection of people using the cyber systems to the protection of national infrastructure depending on cyber-systems [50]. Traditionally, the confidentiality, integrity and availability has been seen as the characteristics in need of protection [5], when considering information security and cyber security [32, 33]. For IT-systems, this considers the protection of the information within the system and the technology storing, processing, and protecting that information. For maritime OT-systems this also considers the projection of the right information at the right time for the navigator, i.e. using the INS for safe navigation. The navigator is then dependent on the correct input of position, as well as the vessel's speed, to be able to determine situations of collision avoidance. This implies further that what is most important for the maritime cyber security aspect of nautical operations is the integrity and availability of the information presented and the system functionality, with less attention paid to the confidentiality aspect [5]. Still, as the level of complexity in information systems are increasing, these characteristics are important to protect, but no longer adequate [50, 57]. New protection measures and models which exceeds these characteristics must be implemented, and [57] urges the need to implement accuracy, authenticity, utility, and possession. These measures will most probably aid the security process, yet these protection measures are only technological measures, paying less attention to the operational aspect. This may serve as an argument to emphasize the navigator as an important asset. As the cyber security vendors often only consider the technological parts of the maritime environment, it is vital to remember that a single part of the system cannot be seen in isolation, but rather must be seen in relation to other parts. In contrast to a technical computer system, a human cannot be as easily patched, corrected, or rewritten. The human can be trained to avoid danger, yet there is always a possibility of error, manipulation, coercion, or sedition in every human–machine interaction [16].

A vessel's IT and OT systems have previously been protected from cyber threats, as the vessels have been "air gaped", meaning the ships have been isolated at sea, unconnected to the internet. In addition, the onboard IT and OT systems have been segregated. However, today the demand for remote monitoring and control, as well as increased connectivity and interconnections due to more complex vessels are threatening this natural protection. One of today's emerging challenges is the cyber threat towards safe navigation, which is also a reason why IMO has addressed the issue. Today there is an overweight of electronically navigated vessels, which makes the vessels vulnerable to cyber-attacks. IMO urges the need for safe and secure shipping, and IMO places "Maritime Cyber Risk" [29, 31] under banner of "Maritime Security" [28]. The idea of maritime cyber security is to protect the given system from cyber risk. "Maritime Cyber Security" can be defined as "… a part of maritime security concerned with the protection from cyber threats of all aspects of maritime cyber systems…" and "… maritime cyber security is concerned with the reduction of the consequences of cyber-attacks on maritime operations" [20]. A cyber risk can be defined as a risk caused by a cyber threat, and cyber threat is a "threat that exploits cyberspace" [47]. Thus, a "maritime cyber threat" is here understood as a cyber threat affecting the maritime domain, in this paper related to the cyber threats which affect navigational systems on board ships, as well as the navigator operating the navigation system. Cyber risks, as financially risks, affects a company's bottom line, by driving up costs and can bring harm to the revenue [4]. This can be a factor with regards to the secrecy of cyber incidents in the maritime industry [37, 43], where for example the fear of losing a charter contract may succeed the cost of paying ransom to a hacker. What are reported in the media are only the huge cyber accidents, and there is reason to believe there are huge dark numbers, as 47% of seafarers report that they have been the target of a cyber-attack [37]. A cyber security consultancy company reported recently that as much as up to 75% of the vessels the company had been studying, had

interconnected IT and OT systems, even though the network diagrams showed the systems to be segregated and the vessels superintendents told them the networks were segregated [45]. As ships are becoming highly technological and complex systems, the potential surface for cyber-attacks is also increasing, yet there is apparently only a small amount of seafarers which have received any form of cyber training [37]. Recent research [2, 20, 39, 52–54] shows that cyber-attacks can interfere with either one or several of the tasks of navigation.

In this paper, the authors emphasize Hareide's [20] definition of "maritime cyber security", which will be understood as the protection from cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. In the next section, the paper will explore the concept of "cyber resilience", as cyber resilience can be viewed as part of cyber security [6], and further investigate how cyber resilience can be applied to nautical operations.

4 CYBER RESILIENCE

Resilience can be ecological, financial, psychological, technical, and organizational [42], amongst many others forms. Literature reviews indicates there are over 300 different definitions of the term "resilience" [58]. Resilience can be many things, depending on the context of the matter [18]. The aim of this paper is not to untangle the definition of resilience itself, but it is important to understand that also resilience is dependent on the context.

The goal of risk management is to be in a state "free from danger or threat", while resilience management focus on system recovery [38]. A way to say this is that resilience management processes acknowledge that "free from danger or threat" is an impossible system state. This view matches with Hollnagel's approach to resilience [21]. For enhancing risk assessment process and risk management process, Johnsen [35] emphasizes the need to implement resilience principles, which further strengthen the resilience to be a part of something, and not necessarily a standalone concept or ability. Resilience should be considered during the risk assessment and management processes, as any other risk mitigation action [35].

The navigational equipment of a vessel is its critical infrastructure because that makes the ship move safely from A to B, which is controlled by the navigator. Resilience is a highly desirable property for critical infrastructure [35], and Hollnagel [22] argues that a system cannot be resilient but can have resilient abilities. A key feature of a resilient organization is that it does not lose control and is able to continue and recover [35]. Hollnagel [21] argues that the concept of resilience is changing from considering materials or structures and shifting towards the functioning or performance of a system, and as previously highlighted, a ship bridge can be considered a sociotechnical system. Resilience focuses on enhancing a system's response to crisis rather than on the crisis itself and its causes [1]. Resilience also needs to consider emerging and unknown threats [38], which further supports the resilience assumption that a system cannot be free from danger or threat. The goal of increased resilience is overall improved system functionality, and what is particularly interesting for this paper is the concept of cyber resilience.

As stated earlier, IMO urges the maritime industry to incorporate resilience principles in the maritime cyber risk management. IMO applies National Institute of Standards and Technology's (NIST) "Framework for Improving Critical Infrastructure Cybersecurity" [4] principles to the risk management approach, where the following steps are emphasized; Identify, Protect, Detect, Respond and Recover. The purpose of the framework is quite clear, to provide organizations with tools to improve the cyber security and resilience of the organization, regardless of the size or degree of cyber security risk and cyber security sophistication. However, when considering resilience, the framework almost stops after the process of "Recover". Cyber resilience should be treated as an iterative and simultaneously process [40]. The framework also implies that "recovery plan is executed during or after a cybersecurity incident". This raises the question if it even is possible to plan for what one does not have knowledge of, and do not see the consequences of, until it is too late. As demonstrated by Lund [39] this can potentially be the case with cyber incident.

Bodeau and Graubart [6] urges that people engaging in enhancing cyber resilience, must understand the context of where they aim to improve cyber resilience. This means there is a need for a framework to apply, as well as identify technologies and practices which could be integrated into the relevant systems and operations. The MITRE "Cyber Resilience Engineering Framework" [6] defines cyber resiliency as: "The ability of a nation, organization, or mission or business process to anticipate, withstand, recover from, and evolve to improve capabilities in the face of, adverse conditions, stresses, or attacks on the supporting cyber resources it needs to function." This concept is not so different from the NIST frameworks principles, yet includes the momentum of evolving, which is seen as an important ability of the concept of resilience. The NIST framework emphasized by IMO can be claimed to lack the momentum of learning and evolving, still, the NIST framework are more directed to the cyber security aspect of the cyber risk mitigation. Hollnagel [24] also addresses this issue when addressing resilience engineering, by emphasizing the momentum of "Learning" as an important aspect of resilience. The MITRE framework highlights that the momentum of evolving corresponds with Hollnagel's momentum of learning [6].

As resilience can be seen as an emergent property, cyber resilience must be engineered [6]. The MITRE framework has a strong fundament in Madni's conceptual framework for Resilience Engineering [40], which again is founded partly on Hollnagel's principles of resilience engineering [23]. The MITRE resilience goals are Anticipate, Withstand, Recover and Evolve, which will further be treated as the resilience abilities under study in this paper. A vital

difference between a computer and a human, is that the computer only needs to learn things once, however, a computer cannot do things it has not learned, as the human can. A maritime vessel can be seen independently as a "working machine", but also conforms a society of different types of seafarers, such as navigators, engineers, and sailors. Hence, it might be need for a combination of the mentioned perspective of cyber resilience and take both organizational and engineering/infrastructural cyber resilience into account [38]. In this section, cyber resilience abilities have been explored on a holistic level and the next section will synthesize the findings from the previous sections.

5 MARITIME CYBER RESILIENCE

The previous chapters have explored the terminology of "maritime operations", "maritime cyber security" and "cyber resilience". This section aims to synthesize the findings of the previous chapters, presenting a working definition for "maritime cyber resilience".

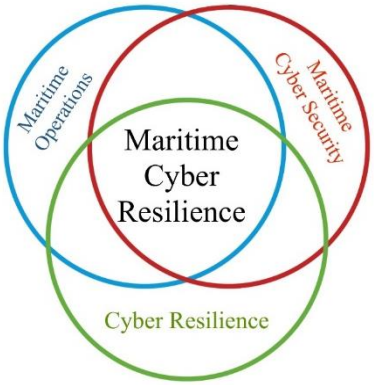

Figure 1. Origins of Maritime Cyber Resilience

We have seen that a maritime operation in its most general sense must be understood as human activities to achieve something at sea and that a resilient organization is one that does not lose control and is able to continue, recover and learn. A resilient maritime operation must then be an activity at sea conducted by an organization that does not lose control of the activity and is able to continue and recover the activity in the face of challenges. As we have seen and will illustrate further later in the paper, navigation is an important part of these activities, so the resilient organization must in this case be able to continue and recover its ability to navigate. What can be threatening the maritime domain today are the potential cyber threats, which put both the vessel and the crew on board at risk. The usual way to address this issue is by highlighting maritime cyber security, which is here understood as the protection from cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. We have also seen that cyber resilience should be a part of the risk mitigation process, as the traditional models for risk mitigation might not cover the emerging cyber threats in the maritime domain. The bridge on board a ship is a complex maritime sociotechnical system, which needs to consider both human and technical aspects, as one cannot exist without the other (for now). Furthermore, "maritime cyber resilience" will be defined as a nautical system's ability to learn how to maintain and evolve a normal operation, as well as anticipate, withstand, recover and evolve from a cyber threat, in the minimum amount of time possible.

By investigating the concept of maritime cyber resilience, it seems that term is meaningless without consideration of the human aspect, which in this paper refers to the navigator. This will be further considered in the next section, which will argue why the human is important in maritime cyber resilience.

6 THE IMPORTANCE OF THE NAVIGATOR

In this section, we will describe how a cyber threat situation is different from a commonly known emergency, and further emphasize why the human is important in the handling of an emergency.

The complexity of sociotechnical systems can make the procedures of operational situations underspecified, and the designers of such systems cannot anticipate everything in advance. Johnsen [35] argues that functions cannot be seen as a bimodal (functioning or not functioning), as seen in [20] where the ECDIS was gradually compromised, giving no alarms even when the system was hacked. A cyber-attack does not need to be immediate and visible; it can be lurking in the background without any warning of its occurrence. The navigator needs to be prepared to be surprised [35], which means that unexpected situations should be assumed to occur at any given time. According to Johnsen [35] a key resilience principle is "Reduction in Complexity", which contradicts with the concept of INS [30] and the increasing complexity of navigational technology [48], which increase the risk of losing control. The purpose of an INS is to make every navigational tool readily available when the navigator needs it. This may affect the concept of maritime cyber resilience, especially if the navigator is not alert.

There is an unthinkable number of different crisis scenarios which can occur on a vessel; however, an easily approachable and very plausible example is fire detected on board in the engine room department of the vessel. IMO provides regulations in SOLAS, stating how onboard equipment should be made fire-safe and preventing fire from occurring and spreading. This makes the ship and its system more robust, as the fire should not easily emerge if every component is designed to be fire safe. It is a common fact that wear and tear happen to equipment, as well as an engine room is a place where work is conducted with tools, fuel and lubricating oils and rags in narrow and high-temperature compartments. This can increase the risk of fire, even if the components are designed to be fire safe in the first place. Aiding to mitigate the risk of fire, every modern ship is fitted with fire detecting and firefighting equipment, as regulated by IMO in SOLAS. This increase the navigator's resilience ability of anticipating, as the firefighting system provides early detection of known characteristics of fire, such as temperature, smoke, or gas. This aids the navigator responsible for the

firefighting- and detection equipment on board to investigate an alarm more closely. The firefighting itself is related to the capacity of withstanding, as the operation must continue, and the navigator must fight the (potential) fire on board. The navigator is at the sharp end of the operation and needs to handle crisis as they emerge.

However, if the risk has become a reality and the normal situation have turned into a crisis, it is up to the planning, handling and response of the crew to get control over the fire which have occurred, using the predefined emergency procedures for fire, as well as improvisational "know-how" from the vessel's crew. We are now in the recovery part of resilience, where the navigator must determine damages and restore the vessel's capabilities. The goal is of course getting the vessel back to normal operation, as soon as possible. Time is, without doubt, a crucial factor in such a crisis, which means this is an important factor of the resilience abilities combined [23]. If the fire is put out, the crew enters the evolving state, debriefing the situation and learning from the incident and how to avoid the situation from emerging again. This also urges re-architecture of either technical barriers, policies, and procedures.

Resilience can relate to the ability to put things together after they have fallen apart [56]. Most crisis which can occur on board a vessel is expected to be described in the Emergency Manual, and the crew is expected to be regularly drilled and tested in these crisis scenarios, where everyone has a dedicated role. The role of the navigator is often a decision maker, as i.e. the captain is responsible for deciding if, and when, the fixed firefighting system in the engine room is to be released, as this system (depending on the onboard solution) also may have the capacity to kill a person being in the engine room at the time of the release of the gas. The Chief Mate is normally responsible for leading the deck crew in firefighting, making quick and effective plans, having control of persons on board, as well as who is not accounted for, and send the crew who are designated as smoke divers and firefighters to find any missing persons. The crisis of fire on board a vessel, as well as all the other "well-known" crisis a vessel can find itself in, are usually tangible and to one extent comprehendible to the decision makers on board. Cyber-attacks, in contrast to a fire, may not be as tangible and visible, and are not yet addressed in standardized training of the seafarers [25], such as the emergency of a on board fire is.

Considering the resilience abilities of anticipate, withstand, and recover, it could be difficult for a navigator to maintain these abilities, who never have encountered, or even heard of, a cyber threat. This is what makes the factor of evolving and learning important, as the threat is being recognized in the maritime industry. That again urges the re-architecting of systems and procedures and transforming of processes and behavior. Depending on the operation that is undertaken, the implementation will of course vary. The consequences of not having a high-precision position are different for a crude-oil tanker in the middle of the Pacific Ocean sailing with low to medium speed, compared to a high-speed passenger vessel sailing along the shores of Norway. Still, both vessels must undertake the process of changing in the face of the prominent threats of today, in order to be able to maintain safe operation and navigation.

Hollnagel describes an organization going through "states" in an event of an emergency, and that it is vital for the organization to know what the current state (i.e. normal operation) is and know when that state is changing. This may be hard with a cyber threat, as what can seem to be a normal situation actually is a disturbed operation state, depending on the cyber threat. A system can be claimed to have three states; stopped, idle and running. If a system finds itself in a matter of emergency, the system needs first to go to an "idle" state, to be able to return to "normal state" [23]. This can also be applied to a vessel. In an example where the navigator loses the control of steering from the autopilot, the navigator needs to take an active choice to steer the vessel manually, to maintain normal operation. This taken into consideration, the navigator needs to know he is in an emergency state. Lund [39] exemplifies that a cyber emergency onboard a vessel might not be as imminent and visible as one might think. This urges the navigator to be the most important cross check sensor on-board [19].

Recovery is often a result of a function of the scale of damage and frequency of the type of the crisis [56]. This can be one of the reasons the emergency response plans are standardized, addressing previously known problems which can occur on a vessel. Fire on board is addressed because of earlier ship emergencies and have thus received attention in the regulations for safe and secure shipping. As discussed above, being resilient is about evolving and adapting to the challenges at hand. The shipowners today need to be resilient in their approach to cyber threats, and not have a passive attitude, hoping to avoid being struck by a cyber-attack.

This section has now discussed an "normal" and very well-known emergency which can occur on board a vessel. A fire onboard is a very visible, tangible and "easy-to-visualize" kind of crisis. A cyber crisis can be described as the exact opposite of that. A cyber crisis may not be tangible, not easy to comprehend and not easy to visualize, especially if the persons who are responsible for handling the crisis have not encountered a cyber incident before. This is also why evolving of the human is important when considering maritime cyber resilience, as the human is capable of adjusting to the situation, whereas emphasizing the good qualities of a "normal operation" and applying resilience principles to the everyday work.

6. CONCLUSION

In this article, the authors have argued for the lack of a definition of the term "Maritime Cyber Resilience" and aimed at providing a working definition for future research.

What is an emerging problem today is the cyber threats and risks towards nautical operations. Maritime cyber security concerns the protection from

cyber threats of all aspects of maritime cyber systems and the reduction of the consequences of cyber-attacks on maritime operations. In order to apply resilient attributes to the nautical operations, the people undertaking such operations must be able to protect the ongoing operations from a potential cyber threats and risks, as well as constantly expect the unexpected, evolving and learning from own operations.

"Maritime Cyber Resilience" has been defined as a nautical system's ability to learn how to maintain and evolve a normal operation, as well as anticipate, withstand, recover and evolve from a cyber threat in the minimum amount of time possible. The authors have also argued for why the navigator should be the focus of study when considering maritime cyber resilience, as the navigator is at the sharp edge of the operation, maybe being the only agent able of detecting an unwanted variation to a situation. Furthermore, the navigator is expected to take the wheel when the technology fails. One assumption when considering maritime cyber resilience is that the navigator needs to accept that the safety of the situation can, and eventually will be, compromised.

This article has discussed that robust systems can fail, and even technical resilient systems can fail. In this case, the navigator, who is a major decision maker onboard needs to take command to take control over the situation. The article mentions that there are many types of cyber-attacks and many of them are not yet known. A cyber-attack can be lurking in the system, not to cause any trouble, before a given time or position. This means that the navigator and the human aspect is key, when considering Maritime Cyber Resilience.

ACKNOWLEDGEMENT

This paper is part of the research project MarCy (Maritime Cyber Resilience). The MarCy project has received funding from the Research Council of Norway, with project number 295077. Contents reflects only the authors' views, and the Research Council of Norway, nor the project partners, are not responsible for any use may be made of the information it contains.

REFERENCES

1. Anholt, R., Boersma, F.K.: From security to resilience: New vistas for international responses to protracted crises. In: Linkov, I., Florin, M.-V., and Trump, B.D. (eds.) Resilience (Volume 2, 2018). pp. 25–32 International Risk Governance Center (2018). https://doi.org/10.5075/epfl-irgc-262527.
2. Awan, M.S., Al Ghamdi, M.A.: Understanding the Vulnerabilities in Digital Components of an Integrated Bridge System (IBS). Journal of Marine Science and Engineering. 7, 10, (2019). https://doi.org/10.3390/jmse7100350.
3. Bainbridge, L.: Ironies of automation. Automatica. 19, 6, 775–779 (1983). https://doi.org/10.1016/0005-1098(83)90046-8.
4. Barrett, M.: Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, https://doi.org/10.6028/NIST.CSWP.04162018, (2018).
5. Bimco, Clia, ICS, Intercargo, Intermanager, Intertanko, IUMI, OCIMF and World Shipping Council: The Guidelines on Cyber Security onboard Ships. BIMCO (ed.) Version 4.0 (2020).
6. Bodeau, D.J., Graubart, R.D., Picciotto, J., McQuaid, R.: Cyber Resiliency Engineering Framework. The MITRE Corporation (2011).
7. Bowditch, N.: The American practical navigator : an epitome of navigation. National Imagery and Mapping Agency (2002).
8. Boyes, H., Isbell, R.: Code of Practice: Cyber Security for Ships. Institution of Engineering and Technology, London, United Kingdom (2017).
9. Cambridge Online Dictionary: Maritime. Cambridge Univeristy Press (2021).
10. Cambridge Online Dictionary: Operation. Cambridge Univeristy Press (2021).
11. da Conceição, V.P., Dahlman, J., Navarro, A.: What is maritime navigation? Unfolding the complexity of a Sociotechnical System. Proceedings of the Human Factors and Ergonomics Society Annual Meeting. 61, 1, 267–271 (2017). https://doi.org/10.1177/1541931213601549.
12. Cutler, T.J.: Dutton's Nautical Navigation. Naval Institute Press; (2004).
13. Daum, O.: Cyber Security in the Maritime Sector. J. Mar. L. & Com. 50, 1–19 (2019).
14. DiRenzo, J., Goward, D.A., Roberts, F.S.: The little-known challenge of maritime cyber security. In: 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA). pp. 1–5 (2015). https://doi.org/10.1109/IISA.2015.7388071.
15. DNV: Cyber security resilience management for ships and mobile offshore units in operation, https://www.dnv.com/maritime/dnvgl-rp-0496-recommended-practice-cyber-security-download.html, last accessed 2021/04/15.
16. Fitton, O., Prince, D., Germond, B., Lacy, M.: The future of maritime cyber security. Lancaster University (2015).
17. Giacomello, G., Pescaroli, G.: Managing Human Factors. In: Kott, A. and Linkov, I. (eds.) Cyber Resilience of Systems and Networks. pp. 247–263 Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-77492-3_11.
18. Haimes, Y.Y.: On the Definition of Resilience in Systems. Risk Analysis. 29, 4, 498–501 (2009). https://doi.org/10.1111/j.1539-6924.2009.01216.x.
19. Hareide, O.S.: Podkast: Teknologi og mennesket som "sensor," https://www.kystverket.no/Nyheter/2021/januar/ny-podkast-teknologi-og-mennesket-som-sensor/, last accessed 2021/04/16.
20. Hareide, O.S., Jøsok, Ø., Lund, M.S., Ostnes, R., Helkala, K.: Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. Journal of Navigation. 71, 5, 1025–1039 (2018). https://doi.org/10.1017/S0373463318000164.
21. Hollnagel, E.: Resilience engineering and the built environment. null. 42, 2, 221–228 (2014). https://doi.org/10.1080/09613218.2014.862607.
22. Hollnagel, E., Pariès, J., Woods, D., Wreathall, J.: Epilogue: RAG – The Resilience Analysis Grid. In: Resilience Engineering in Practice. pp. 275–296 CRC Press, London, United Kingdom (2011). https://doi.org/10.1201/9781317065265-19.
23. Hollnagel, E., Woods, D.D., Leveson, N.: Resilience Engineering: Concepts and Precepts. CRC Press (2006).
24. Hollnagel, Erik: How resilient is your organisation? In: An Introduction to the Resilience Analysis Grid (RAG). , Toronto, Canada (2010).
25. Hopcraft, R., Martin, K.M.: Effective maritime cybersecurity regulation – the case for a cyber code. null. 14, 3, 354–366 (2018). https://doi.org/10.1080/19480881.2018.1519056.
26. IACS: Rec 166 - Recommendation on Cyber Resilience, http://www.iacs.org.uk/publications/recommendations/161-180/, last accessed 2021/04/15.

27. Inmarsat: Best Practice Information and Communications Technology (ICT) Recommendations, https://www.inmarsat.com/en/insights/maritime/2019/best-practice-ict-guide.html, last accessed 2021/04/15.
28. International Maritime Organization: Maritime cyber risk, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, last accessed 2021/04/15.
29. International Maritime Organization: MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, last accessed 2021/04/15.
30. International Maritime Organization: Resolution MSC.252(83): Adoption of the Revised Performance Standard for Integrated Navigation Systems (INS).
31. International Maritime Organization: Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems, https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx, last accessed 2021/04/15.
32. ISO: ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls, https://www.iso.org/standard/54533.html, last accessed 2021/04/15.
33. ITU: ITU-Tx. 1205. Interfaces. 10, 20–X, 49 (2008).
34. Jensen, L.: Challenges in Maritime Cyber-Resilience. Technology Innovation Management Review. 5, 4, 35–39 (2015). https://doi.org/10.22215/timreview/889.
35. Johnsen, S.: Resilience in Risk Analysis and Risk Assessment. In: Moore, T. and Shenoi, S. (eds.) Critical Infrastructure Protection IV. pp. 215–227 Springer Berlin Heidelberg, Berlin, Heidelberg (2010).
36. Karahalios, H.: Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. Journal of Transportation Security. 13, 3, 179–201 (2020). https://doi.org/10.1007/s12198-020-00223-1.
37. KVH Intelsat: Crew Connectivity 2018 Survey Report, http://www.crewconnectivity.com/?product=2018-crew-connectivity-survey-report, last accessed 2021/04/15.
38. Linkov, I., Kott, A.: Fundamental Concepts of Cyber Resilience: Introduction and Overview. In: Kott, A. and Linkov, I. (eds.) Cyber Resilience of Systems and Networks. pp. 1–25 Springer International Publishing, Cham (2019). https://doi.org/10.1007/978-3-319-77492-3_1.
39. Lund, M.S., Hareide, O.S., Jøsok, Ø.: An Attack on an Integrated Navigation System. Necesse. 3, 2, 149–163 (2018). https://doi.org/10.21339/2464-353x.3.2.149.
40. Madni, A.M., Jackson, S.: Towards a conceptual framework for resilience engineering. IEEE Engineering Management Review. 39, 4, 85–102 (2011). https://doi.org/10.1109/EMR.2011.6093891.
41. Markit, I.: Safety at Sea and BIMCO cyber security white paper, https://ihsmarkit.com/Info/0819/cyber-security-survey.html, last accessed 2021/04/15.
42. Martin-Breen, P., Anderies, J.M.: Resilience: A literature review, https://opendocs.ids.ac.uk/opendocs/handle/20.500.12413/3692, last accessed 2021/04/15.
43. McGillivary, P.: Why Maritime Cybersecurity Is an Ocean Policy Priority and How It Can Be Addressed. Marine Technology Society Journal. 52, 5, 44–57 (2018). https://doi.org/doi:10.4031/MTSJ.52.5.11.
44. Mileski, J., Clott, C., Galvao, C.B.: Cyberattacks on ships: a wicked problem approach. Maritime Business Review. 3, 4, 414–430 (2018). https://doi.org/10.1108/MABR-08-2018-0026.
45. Ng, D.: Safety first: maritime cyber security, IMO guidelines and the maritime supply chian. Riviera Maritime Media (2021).
46. NTNU: Literature review of "Maritime Cyber Resilience," https://bibsys-almaprimo.hosted.exlibrisgroup.com/primo-explore/search?query=any,contains,%22maritime%20cyber%20resilience%22&tab=default_tab&search_scope=default_scope&vid=NTNU_UB&offset=0, last accessed 2021/04/15.
47. Refsdal, A., Solhaug, B., Stolen, K.: Cyber-Risk Management. Springer International Publishing (2015). https://doi.org/10.1007/978-3-319-23570-7.
48. Relling, T., Lützhöft, M., Ostnes, R., Hildre, H.P.: A Human Perspective on Maritime Autonomy. In: Schmorrow, D.D. and Fidopiastis, C.M. (eds.) Augmented Cognition: Users and Contexts. pp. 350–362 Springer International Publishing, Cham (2018).
49. SAGE Journals: Literature review of "Martime Cyber Resilience," https://journals.sagepub.com/action/doSearch?filterOption=allJournal&AllField=%22maritime+cyber+resilience%22, last accessed 2021/04/15.
50. von Solms, R., van Niekerk, J.: From information security to cyber security. Computers & Security. 38, 97–102 (2013). https://doi.org/10.1016/j.cose.2013.04.004.
51. Springer: Literature review of "Maritime Cyber Resilience, https://link.springer.com/search?query=%22maritime+cyber+resilience%22, last accessed 2021/04/15.
52. Svilicic, B., Brčic, D., Žuškin, S., Kalebic, D.: Raising Awareness on Cyber Security of ECDIS. TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation. 13, 1, 231–236 (2019). https://doi.org/10.12716/1001.13.01.24.
53. Svilicic, B., Kamahara, J., Rooks, M., Yano, Y.: Maritime Cyber Risk Management: An Experimental Ship Assessment. Journal of Navigation. 72, 5, 1108–1120 (2019). https://doi.org/10.1017/S0373463318001157.
54. Svilicic, B., Rudan, I., Jugović, A., Zec, D.: A Study on Cyber Security Threats in a Shipboard Integrated Navigational System. Journal of Marine Science and Engineering. 7, 10, (2019). https://doi.org/10.3390/jmse7100364.
55. TransNav.eu: Literature review of "Maritime Cyber Resilience," https://www.transnav.eu/Search_maritime%20cyber%20resilience.html, last accessed 2021/04/15.
56. Westrum, R.: A Typology of Resilience Situations. In: Hollnagel, E., Woods, D.D., and Leveson, N. (eds.) Resilience Engineering: Concepts and Precepts. pp. 55–65 CRC Press, London, United Kingdom (2006). https://doi.org/10.1201/9781315605685-8.
57. Whitman, M.E., Mattord, H.J.: Principles of Information Security. Cengage Learning (2017).
58. Woltjer, R.: Deliverable D1.1 Consolidation of resilience concepts and practices for crisis management, https://h2020darwin.eu/project-deliverables/, last accessed 2021/04/15.