University of Plymouth

PEARL **https://pearl.plymouth.ac.uk**

Faculty of Science and Engineering School of Engineering, Computing and Mathematics

2023-06-01

CERP: A Maritime Cyber Risk Decision Making Tool

Erstad, E

https://pearl.plymouth.ac.uk/handle/10026.1/20775

10.12716/1001.17.02.02
TransNav: International Journal on Marine Navigation and Safety of Sea Transportation
Gdynia Maritime University

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

CERP: A Maritime Cyber Risk Decision Making Tool

Erlend Erstad

Norwegian University of Science and Technology

Rory Hopcraft

University of Plymouth

Juan Dorje Palbar

University of Plymouth

Kimberly Tam

University of Plymouth

Abstract

An increase in the complexity of systems onboard ships in the last decade has seen a rise in the number of reported maritime cyber-attacks. To tackle this rising risk the International Maritime Organization published high-level requirements for cyber risk management in 2017. These requirements obligate organisations to establish procedures, like incident response plans, to manage cyber-incidents. However, there is currently no standardised framework for this implementation. This paper proposes a Cyber Emergency Response Procedure (CERP), that provides a framework for organisations to better facilitate their crew's response to a cyber-incident that is considerate of their operational environment. Based on an operations flowchart, the CERP provides a step-by-step procedure that guides a crew's decision-making process in the face of a cyber-incident. This high-level framework provides a blueprint for organisations to develop their own cyber-incident response procedures that are considerate of operational constraints, existing incident procedures and the complexity of modern maritime systems.

1. Introduction

Considering the global maritime cyber risk landscape, the likelihood of maritime digital systems becoming the target of a cyber-incident has increased in recent years [1]. Research indicates that critical onboard systems are susceptible to compromise by both accidental actions and deliberate interference [2]. There are currently several approaches to manage these threats. Firstly, the UN Specialised Agency the International Maritime Organization (IMO) has provided high-level requirements and recommendations for cyber security on board ships [3, 4]. Secondly, one of the largest global shipping associations BIMCO, has provided a maritime cyber risk management specific framework for preparing against the cyber threat on an organisational level [5]. Thirdly, the International Association of Classification Societies (IACS), has recently published two new Unified Requirements (UR) considering cyber resilience for ships, namely "E26 Cyber resilience of ships" and "E27 Cyber resilience of on-board systems and equipment". As IACS consist of the largest class societies in the world, covering a majority of the world's fleet, these URs will have a worldwide impact [6]. However, with these requirements only being implemented on new builds from 1st January 2024, the realisation of these impacts will be a long time coming.

All the above documentation is designed to aid shipowner companies in the management of the risks they face due to connected technology. However, on board ships, the cyber risks are still being handled pragmatically and by improvisation, as seafarers currently have little to no formalized education of the cyber risks they face [7]. Thus, there is need for operational tools which can be used by crew in response to cyber incidents that are considerate of the organisational management processes. It is therefore vital for management to provide procedures that allow the crew to be able to recognise, respond and recover effectively to a cyber incident, whether the incident is deliberate or accidental.

Developed through engagement with a large offshore operator and a national coastal administration, this paper proposes a maritime cyber risk decision making tool, the Cyber Emergency Response Procedure (CERP). Based on an operational flowchart, the CERP intends to serve three purposes. Firstly, it provides a blueprint that allows organisations to include cyber incident response within their standard incident response procedures. Allowing the development of policy and procedures that are considerate of processes and practices already in place. Secondly, it provides a high-level of decision-making tool that guides crew through the response to a cyber incident. This tool guides the crew through the initial identification of a cyber incident, and managing its symptoms and outcomes using standard documentation found on board. Thirdly, the CERP sets out to demonstrate the need for, and procedure for attaining, external support in the face of a cyber-incident the crew cannot handle independently.

The rest of the paper is as follows. Section 2 will explore the current approach to current maritime incident response and cyber incident response, justifying the use of a flowchart like the one presented in this paper. Section 3 will present the CERP and demonstrate its implementation through the use of examples. Section 4 will explore the future work that would be required to effectively implement the CERP into maritime operations. Section 5 will conclude by arguing that the CERP is a vital first step on a longer road to the effective emergency response to maritime cyber incidents.

2. Maritime and cyber incident response

The response to maritime incidents is heavily driven by regulatory bodies and international requirements. As such, this section will start by introducing the current maritime incident response and some of the tools, like checklists, that have been standardised in an attempt to aid that response. The section will also investigate several of the key cybersecurity standards that provide some insight into the development of an appropriate cyber incident response. Finally, the section will explore how

the sector is currently coping with maritime cyber risk and lay the foundations of how the work of this paper can enhance that response.

2.1 Maritime incident response

The current response to a maritime risk event is illustrated in Figure 1, whereby in the event of an incident the primary objective is to ensure the safety of the vessel and crew through the use of incident procedures. If completed correctly this should lead to the safe conclusion of the incident, whereby operations will continue as normal, or in a reduced mode. For simplicity, this paper will adopt the following definitions. Returning to normal operations means that the incident has not limited the operation of the vessel and no further action would be required. Reduced mode covers all other outcomes including the need to gain outside assistance in order to return to normal operations.

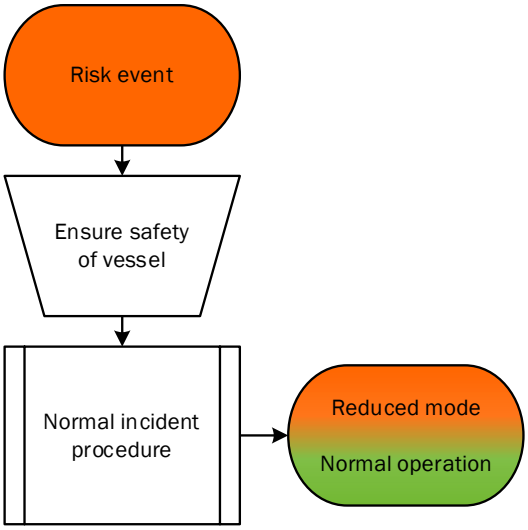

Figure 1 Traditional incident management

As the UN regulator charged with governing the maritime sector, the IMO has developed a variety of regulatory frameworks to improve the safety and security of the sector [8]. The framework most relevant to this article is the International Safety Management (ISM) Code [9], which is mandated under Chapter IX of the International Convention for the Safety of Life at Sea (SOLAS) [10]. The primary aim of the ISM Code is to guarantee, preserve and embed maritime safety and pollution prevention into everyday maritime operations [11]. One particular requirement of the ISM Code obligates companies, and their vessels, to implement, and maintain, a Safety Management System (SMS). Failure to implement an SMS will result in the vessel being unable to obtain its Safety Management Certificate (SMC) and subsequent Document of Compliance (DoC), hindering its ability to operate.

A compliant SMS provides crew with measures to respond at any time to accidents, hazards, and emergency situations, such as fire, grounding, and collision. Through the use of risk assessments these measures are adapted by each company to be considerate of operational constraints and organisational structure. As part of this process companies should identify response procedures to emergency situations, and established drills and exercises to practice them [9]. For the offshore operator the authors engaged with, these drills were on a trimonthly basis and were complimentary to other incident drills like fire or evacuation.

Part of the response procedures and plans include the use of checklists that detail the process through which the expected, and essential, actions should be taken to manage the incident [12]. For example,

see Figure 2 that details the contents of the checklist action plan that is to be used in response to a suspected ransomware attack.

Cyber Security - IT Action Plan

Title Cyber Security - Ransomware

Description A ransomware attack is easy to recognize, as it holds important files or data hostage. This means that your files will become inaccessible. For example, if you try to open a word document, it will ask for an encryption key, but you must pay the ransom in order to get it. In most cases there is a a pop-up window, advising you about the infection and how to pay the ransom

Immediate action plan			
Action	**Complete**		**Comments**
Turn off equipment to minimize the spread of the infection through the network	Yes		
	No		
	N/A		
Immediately power off an disconnect affected systems from the onboard network until further investigation	Yes		
	No		
	N/A		
Contact ICT Department for further investigation, coordination and support	Yes		
	No		
	N/A		

Figure 2 Example maritime checklist

As the example illustrates, each checklist is designed for a specific incident, in this case that is ransomware, but others include sensor failures or fire. The checklist provides a brief description of the risk to outline the parameters that this checklist is appropriate for. The final, and most important element is the action plan, which provides clear steps that the crew should take in response to the incident. These actions should be developed in collaboration with both crew and onshore management to ensure the response is both appropriate to the operations and considerate of the existing organisation policies and procedures.

2.2 Cyber incident response

Cyber security and information security have gone hand-in-hand for many years. To this end there are a number of key documents, both regulations and standards that have been published to provide an insight into improving the cyber security of digital systems. The ISO 27000 series, consisting of multiple standards, are one of the most iconic within the domain. The introductory ISO 27000 provides the high-level terms of reference for the security management of any system that collects, processes, stores and transmits information [13]. ISO 27001 provides the requirements for establishing, implementing, maintaining, and improving such information security management systems. These requirements include the establishment and practice of procedures that allow for a quick, effective, and orderly response to information security incidents [14]. In section 5.24, ISO 27002 provides more details on the development of incident plans. The standard argues that organisations should establish plans that are considerate of the organisation's specific risks, capability for detection and response, as well as ensuring appropriate training is identified, and delivered to those expected to respond [15].

Arguably the ISO 27000 series focuses on Information Technology (IT) systems and not the Operational Technology (OT) systems commonly found onboard ships. However, many of these OT systems are underpinned by IT systems, and require accurate and reliable data (i.e., information) to operate

effectively. Therefore, the high-level security requirements, like response plans, are easily transferable between the IT and OT space. Whilst standards are useful for providing guidance for incident response practices, they are only voluntary requirements.

In 2016, the European Commission published the NIS Directive, which lays down requirements that certain organisations within the European Union must adhere to in order to raise the level of security of network and information systems [16]. At the start of 2023, the EU Commission published NIS2 which will replace the original NIS Directive when it enters into force in 2024 [17]. Within NIS2, there are clear requirements for organisations defined as either 'essential' or 'important' to have cyber incident response plans. These plans themselves must include reporting mechanisms of incidents to the national authorities. Again, highlighting how cyber response procedure do not only require the involvement of the operator but often include the involvement of external stakeholders.

The above documents, whilst reiterating the importance of having cyber incident response plans do not provide clear details on what these plans should include aside from the potential need to report. The National Institute for Standards and Technology (NIST) Cybersecurity Framework [18], whilst again having an IT focus, does provide some details on what these plans should contain with the "Respond" function. There are several activities that are particularly relevant to the context of this paper. Firstly, personnel should know their role and the order of operations in response to an incident. Therefore, the availability of checklists detailing procedures are a useful tool. There should also be coordination between stakeholders, both internally and externally, to ensure an effective response.

2.2 Maritime cyber incident response

The maritime industry has for a long time been vulnerable to cyber security risks, and over the last few years regulations and requirements have been implemented to reduce these risks. Whilst this resolution marks the formal need for organisations to consider cyber risk, arguably others had been pushing this approach for many years prior. For example, in 2011 the European Union Agency for Cybersecurity (ENISA) published one of the earliest reports highlighting the sector's cyber security risks, and the need for plans to be developed [19]. In 2016 the maritime cyber security discussion intensified with a plethora of documents calling for more action were published. Firstly, classification society DNV published their Recommended Practice "Cyber security resilience management for ships and mobile offshore units in operation" [20]. Secondly, IACS published "IACS-166 Recommendation on Cyber Resilience" [21]. Thirdly, BIMCO published the first version of the "Guidelines on Cyber Security Onboard Ships" [22]. Such were the popularity of these documents they have all since been updated, with the BIMCO guidelines now on their fourth edition [5].

Following increasing pressure for action from its membership the IMO published "MSC-FAL.1/Circ.3 – Guidelines on maritime cyber risk management" [3], which provides high level recommendations on maritime cyber risk management. The following year, after intense discussion the IMO ratified MSC.428(98), making cyber risk management a mandatory element within a ship's SMS [4]. This requirement meant that from 1st January 2021 in order to obtain their DoC, shipowners were required to consider their cyber risks within their SMS and subsequently develop plans and procedures to manage those risks.

Both these IMO documents argues that the sector should consider "industry best practice" when addressing cyber risk. Thus, the IMO recommend operators to consider the NIST Cybersecurity Framework, the ISO 27000 series and the BIMCO guidelines as a way to inform their practices. In light of the entry into force of Resolution MSC428(98) the ISO have released ISO 23806:2022, which focuses on cyber safety for ships and marine technology [23]. Again, like the other documents there are little details in the specifics of cyber incident response. However, the standard does present a high-level

cyber safety risk assessment that allows the company to determine the specific risks that they face and mitigate against those.

Some states, like the USA have produced documentation outlining their expectations for ships that are compliant to Resolution MSC.428(98). Produced by the US Coast Guard (USCG), a Work Instruction (WI) entitled "Vessel Cyber Risk Management" (CVC-WI027) stipulates the expectation that all companies should maintain a Vessel Security Plan alongside the SMS, both of which should include cyber risk [24]. These plans should include a training element to ensure crew are able to respond effectively to a cyber incident. The WI also provides some details on what that response should look like, including the need to request assistance from Coast Guard Cyber Protection Team and Port State Control Officer when appropriate.

The previously listed documents focus on developing cyber incident response plans for ships that are currently operating. As mentioned in Section 1, IACS have been proactively developing new cyber risk management requirements for new builds post-2024. Both UR E26 (cyber resilience of ships) and UR E27 (cyber resilience of ships equipment) stipulate that all new builds classified by an IACS member should have an incident response plan [25, 26]. These plans should "…contain documentation of predetermined set of instructions to detect, respond to, and limit consequences of incidents…" [25, page 18]. As per UR E27 these plans should be developed considering the vessels operational requirements as well as key information available from the manufacturer.

Therefore, whilst maritime cyber incident response forms part of the mandated requirements for ships, there is still little information available to what these plans should include. What is clear, is that failure to comply with the development of cyber response instructions, and drills to test them, could lead to non-compliance which would have a negative impact on the operation of the vessel. To ensure compatibility with current practices these new plans should resemble the existing documentation for incident response. Thus, these plans and instructions should take the form of checklists and flowcharts which support the decision-making process of crew during incidents.

3. A cyber incident decision support tool

The previous sections have discussed there is little work currently being done in applying the response to cyber incidents to maritime operations. Therefore, the core aim of this paper is to introduce a maritime cyber incident response framework that can aid organisations in the development of their own response plans that are considerate of the company specific nuances of their operations, systems, and crews.

In keeping with the traditional methods as these represent both best practice, and the most effective methods of responding to maritime incidents, the authors considered the development of a checklist that would provide details on the handling of a cyber incident. However, following discussions with a variety of stakeholders, including a large offshore operator and coastal administration, it was decided that in isolation these checklists would be of limited benefit. What was clear from these discussions was that crews and organisations, while capable of creating and completing checklists, do not fully understand the correct procedure for dealing with cyber incidents at large. Thus, the authors decided to develop a cyber risk decision support tool that fulfils the three purposes listed in Section 1:

1) Act as a blueprint for organisations to include cyber incident response within their existing response procedures;
2) Provide high-level decision support to crews responding to a cyber incident;
3) Demonstrate the role that external support will play within cyber incident response.

The decided format for this support tool, mimicking the norm within the sector, is a flowchart identified as the CERP (Cyber Emergency Response Procedure). As argued by [27], flowcharts provide a visual representation of the procedures allowing crew to address risks rationally and systematically.

3.1 Cyber Emergency Response Procedure (CERP) flowchart

By introducing the maritime cyber risk decision support framework in this way, the authors emphasize that the handling of cyber risk shall not be prioritized before safety critical incident processes. Aligned with the requirements of Resolution MSC.428(98) [4] cyber risks should simply be included in the existing incident handling procedures, as any other risk, such as fire or flooding. Safety of the vessel, crew, and the environment are, as always, the priority.

Remembering **Error! Reference source not found.** that presented a simplified emergency response procedure on board. Figure 3 takes this one step further and illustrates how the crew should initiate the CERP, if there is a "cyber" element to the incident. In some situations, particularly time critical incidents, it may not be possible to initiate the CERP immediately. Therefore, crews first step should be to ensure the safety of the ship, crew, and environment before attempting to initiate the CERP. For example, consider the following ransomware scenario.

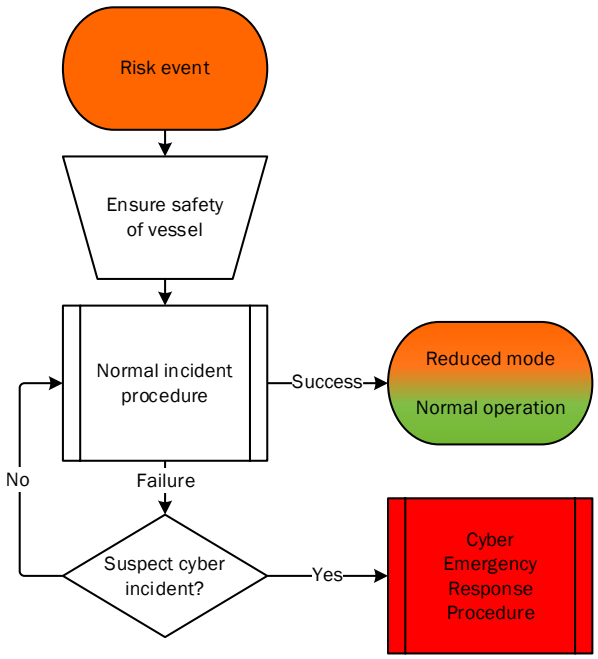

Figure 3 Traditional incident response expansion to include cyber incident response.

A vessel is currently underway and suddenly all the bridge equipment screens display an image saying all their systems are encrypted until a ransom has been paid. The crew realise that this means that they have now effectively lost control of the steering and propulsion systems of the vessel. The crews' response to this scenario, whilst clearly a cyber incident, has two different potential routes depending on the current operational environment. If this scenario were to occur whilst the vessel was transiting open seas then, as long as there is no immediate risk to the crew, ship or environment, the crew could initiate the CERP. However, in the same scenario but the vessel is now transiting a busy Traffic Separation Scheme (TSS) then the crew would need to ensure the safety of their ship and crew as well as others before initiating the CERP. In this case it would be to manually take control of the vessel and remove themselves from danger, and eventually alert vessels in the vicinity following their standard incident procedures. For example, by the use of lights, horn, Automated Identification System, Global

Maritime Distress and Safety System (GMDSS) and a PAN-PAN broadcast via VHF (i.e., initiating PAN PAN procedure by voice via VHF). Once the ship and crew are safe then the CERP can be initiated.

The flowchart itself is developed giving consideration to ISO 5807-1985 [28], which provides standardised symbols and definitions for flowcharts. Whilst the standard does not fit the authors purpose directly, the paper has adopted the approach under the description of a "Program Flowchart", whereby it details the procedural sequence of operations within a program. Whilst this type of flowchart is best suited for a computer program, in a simplified format it can appropriately be used to visualise the procedure a human operator can follow within their own system of working.

Figure 4 illustrates the CERP developed by the authors and verified with experts within the maritime sector. The CERP has 4 distinct phases, which also relates to specific divisions on board and on shore. The first labelled *Operational Team* is the initial phase of the CERP. The operational crew, bridge, or engine room have already determined that there is a potential cyber incident occurring and that the safety of the vessel is currently not at risk. Within this initial phase crew would be expected to identify the risk (M1), this might be as simple as identifying the potential system(s) at fault, or potential causes for the consequences presented within the incident. Once the system(s) at risk have been identified then the crew need to determine whether they can mitigate the risks, by either using a manual/alternative measure (M2) or isolating the system (M3). It is not essential that both are achieved, but it could help reduce the risk of the incident spreading to other systems. Companies would need to provide procedures for how to achieve manual operation and isolation of systems, with acceptable alternatives listed.

The second phase labelled as the *Onboard Technical Response*, is the onboard crews initial attempts to manage and mitigate the cyber incident. Once the crew have identified the systems at fault, they should be following preprepared checklists and procedures in troubleshooting the affected devices (Doc1). In some cases, this will work, and the ship can return to normal operations (T2). However, if the crew consider there is a possibility that the problem as propagated to other systems, they should restart the CERP for that particular system. This should continue until crew have exhausted all possible solutions.

Once this exhaustion has occurred onboard, the crew should determine that contacting the *Shoreside Support Team* for technical support is the next option (D4). These teams will contain a greater expertise in cyber incident handling or have access to this expertise (contact with manufacturer support). In some cases, this shore side team may be able to solve the incident remotely (T3), or by providing instructions to the crew, who will either succeed (T2) or fail. On failure, it may be determined that the only possible solution would be to initiate the companies repair and replacement procedures (P2). In these situations, the Master must consider the integrity of the DoC. For example, if the ship only navigates using an Electronic Chart Display and Information System (ECDIS) and does not have updated paper charts, then the vessel could be deemed un-seaworthy and must, in the worst case, seek emergency harbour to rectify deficiencies in the DoC.

There are two important points of note that crew should be aware of during the implementation of the CERP. Firstly, if the situation of either the ships operational environment or incident changes, then the crew should reassess the safety of the ship and determine whether preventative measures need to be taken immediately before proceeding with the CERP. Secondly, the three termination points (T2, T3 and T4) are labelled as reduced mode/normal operations. This is because there will be situations whereby the risk has been mitigated enough to an acceptable level that operations can continue, just at a reduced level.

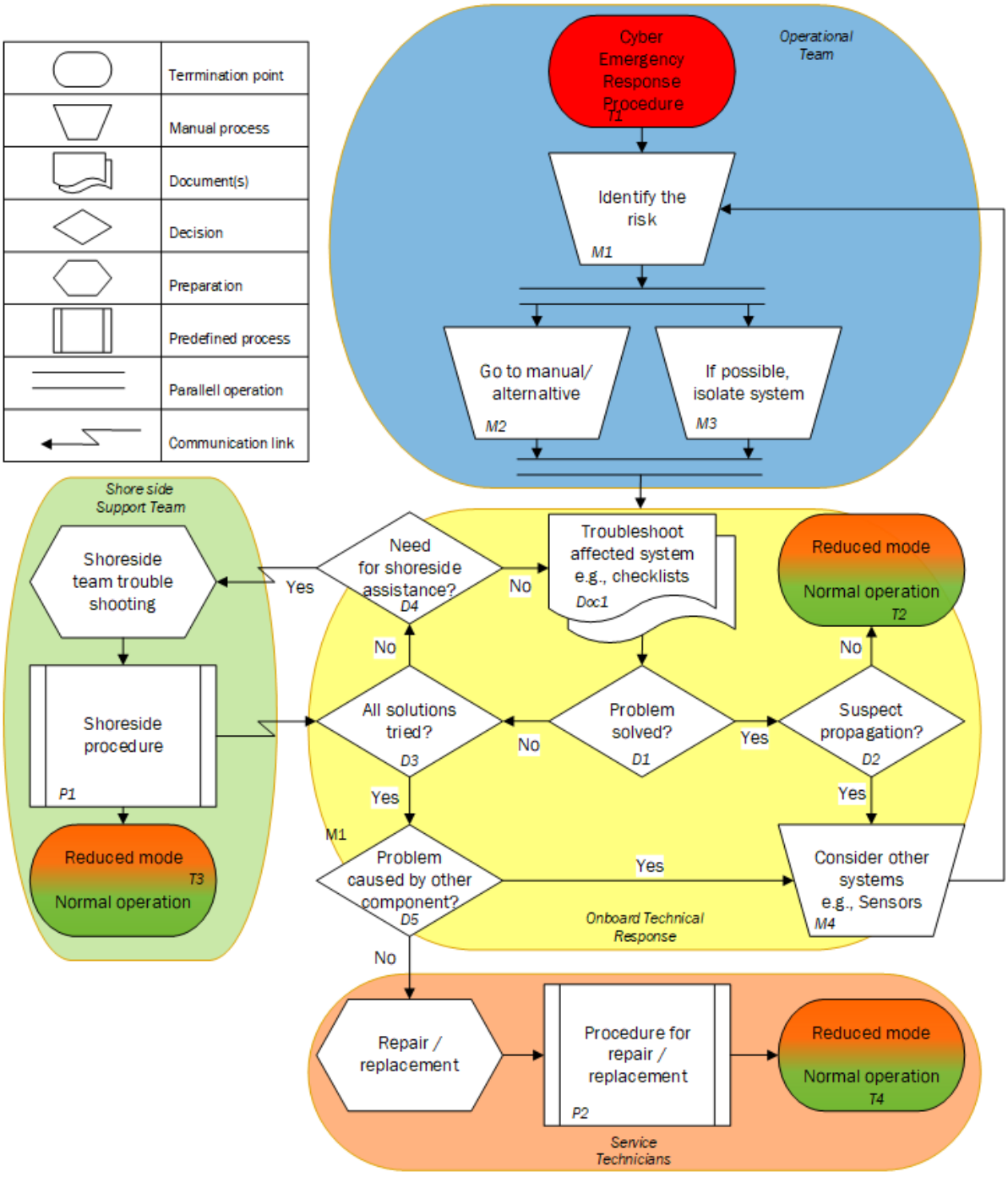

Figure 4 Flowchart for the Cyber Emergency Response Procedure (CERP)

3.2 The CERP in practice

This section will present three scenarios that demonstrate how the CERP can be utilised by companies and crews to respond to cyber emergencies. The scenarios are written to be generic in order for the reader to adjust each scenario to their own experiences and operations. For instance, the bridge scenario could target the Multi-Function Displays (MFD) or the Dynamic Positioning (DP) systems. Each scenario will illustrate the route through the CERP that crew will take (with manual actions notated by M#) to reach each of the termination points (T2, T3 and T4).

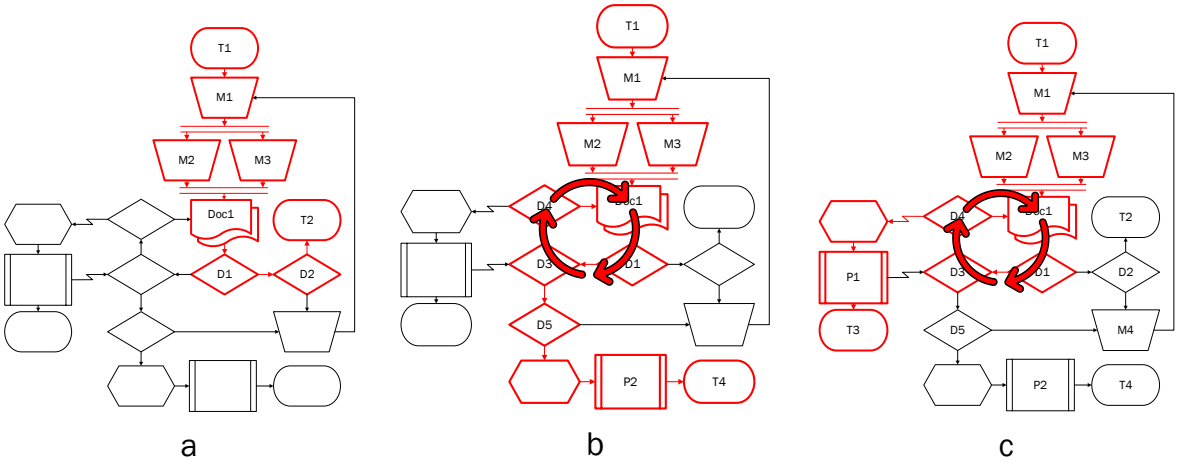

Figure 5 Implementation of CERP (a: Section 3.2.1, b: Section 3.2.2, c: Section 3.2.3)

3.2.1 Compromised non-essential device

During normal operations, a computer suddenly displays a ransomware message, and the crew member is unable to access any files on the device. The crew member immediately notifies the Master of the problem. Using the CERP, the Master determines there is no direct impact on safety and instructs the crewmember to remove the network (ethernet) cable to isolate the device (M3). As per the documentation (Doc1), the Master notifies the engineer on board responsible for IT systems of the problem who then takes responsibility for troubleshooting and reporting back to the Master. Having already isolated the device, the engineer reboots the device from a backup and the computer is no longer infected (D1). The Master confirms with the rest of the crew that no other devices seem to be impacted, so assumes the ransomware has not propagated (D2). Allowing the vessel to continue normal operations (T2).

3.2.2 Faulty GNSS Sensor

During normal operations, the crew are actively using the ECDIS for navigation and determines that the observed position is not corresponding to the other position fixing methods (i.e., visual and radar). The officer of the watch notifies the Master of his concerns. The Master determines that whilst there is no risk to the safety of the ship, ECDIS is a critical system so corrective action is required. As it is not possible to isolate the ECDIS, the Master instructs crew to use other position fixing methods and posts an extra lookout as an alternative to the device whilst it is being troubleshooted (M2). The crew then follow the troubleshooting checklists for ECDIS (Doc1). After several unsuccessful attempts, the crew cannot solve the problem (D3) and determine another device might be at fault (D5). Crew determine that it is a Global Navigation Satellite System (GNSS) sensor causing the issue (M4), so begin the CERP for that device. After unsuccessful attempts to troubleshoot the GNSS sensor (Doc1) the Master instructs the crew to use the backup sensor and with support from shore initiates the decommission and replacement procedures for the faulty GNSS sensor (P2), allowing the ship to continue operations at in a reduced mode (T2).

3.2.3 Engine control room (ECR) systems

When entering the Engine Control Room (ECR) the Chief engineer notices an E-cigarette plugged into a USB port of the control panel. Unsure if the device has transferred malware onto the control systems, the Chief Engineer immediately notifies the Master of the situation. The Master determines that all systems are fully operational so deems it not appropriate to take alternative measures, or isolate a system (M2, M3). The engineer considers the appropriate checklists (Doc1) which involves the notification of the shoreside team (D4). The shoreside team, implement their own procedures for

remotely accessing the ECR systems and running their own security checks (P1). They determine that the systems have not been compromised, so instruct the vessel to continue operations as normal (T3).

3.3 Roles and responsibilities

As per the requirements of a ships SMS, all crew should be aware of their responsibilities when responding to an incident [9]. Furthermore, as this paper has argued the response to a cyber-incident might require the involvement of shoreside personnel. Therefore, all personnel, both on board and ashore need to be aware of their responsibilities to ensure the most effective response to an incident whilst maintaining the highest level of safety.

3.3.1 Service technicians

The management level onboard a ship, primarily the Master and Chief Engineer, hold the highest level of responsibility for responding to incidents. While both must work seamlessly in response to a cyber incident, both have slightly different roles to play. The Master's primary role is to ensure the continued safety of the vessel and its crew with an operational focus. It is the Master who completes the mental risk assessment to determine if the ship is in a safe enough position and/or state to initiate the CERP, or if other action is required prior to initiation. The Chief Engineer, on the other hand, whilst still having a responsibility for ensuring safety, will primarily be focused on providing the technical support during an incident and complete mental risks assessments regarding the criticality of systems.

In both instances the management level on board will primarily fulfil a coordination role, pulling on their substantive experiences and training to direct other crew members in their response. They would also be the ones responsible for contacting shoreside assistance, as required. These personnel would also be expected to synthesis the information from all sources across the ship and ashore and disseminate that back to others in the form of instructions or information.

3.3.2 Technical team on board

The technical team would be those personnel who have clearly defined areas of responsibility which play a critical role in the safe operation of a vessel. These personnel include navigation officers and members of the engine department. These personnel hold several critical roles in the response to cyber incidents. Firstly, as they are the operators of the technical equipment (hands-on), they are likely to be the first to detect a problem. The second responsibility they have is to ensure they communicate this problem to the management level, along with any other operational information that could influence the response. The third and final role that these personnel will fulfil is the implementation of the response. Take the example in Section 3.2.2, the technical operator would be expected to implement the troubleshooting documents when instructed by the management level, and report back on its success.

3.3.3 Shoreside assistance

With the complexity of many maritime systems, and the plethora of attack vectors, it would be surprising if the crew on board the vessel was able to respond to all cyber incidents independently. Therefore, shoreside assistance should be available when needed.

3.3.3.1 Company support team

Operators should recognise that whilst capable of responding to many incidents, the crew are operational experts, not technical experts. Whilst many operators have a team, commonly termed "IT Support", they may lack the operational knowledge and skills like communication, required to respond to incidents on a moving vessel [29]. Therefore, operators should ensure a shoreside team that has the correct operational and technological knowledge and skills is able to provide support to the crew when needed. This team will have their own set of procedures for responding to a cyber incident. These

procedures may include the remote access and maintenance of a system, or the communication of more detailed, and technical, instructions back to the vessel for the crew to implement.

3.3.3.2 Service technicians

The second part of the shoreside assistance includes service technicians, either from 3rd party service providers employed by the operator to maintain the vessel systems, or members of the technical support teams from the original equipment manufacturers. Again, operators should recognise that their technical staff may require the assistance of those more intimately aware of the systems to enable an effective response. Operators have the responsibility to ensure that, when involving external support, information is passed to these teams so that they can provide a response which is considerate of the current operational requirements of the vessel. The external technicians have a responsibility to comprehend this information and utilise the knowledge within their own organisations to facilitate an effective response to an incident.

3.3.3.3 Other shoreside assistance

Whilst outside of the scope of this paper, it is also important to highlight that there might be other stakeholders who would be involved in the response to a cyber incident onboard. This could include entities like the coastguard, military (or equivalency), or other operators involved in the rescue and recovery of the vessel. All these entities have different roles to play, and operators should be aware of which situations would require the involvement of them and have procedures in place to initiate that involvement.

4. Implementation of CERP into maritime operations

The previous section illustrated the CERP and demonstrated how the CERP can function in a practical, shipboard environment, affected by a cyber incident. However, to include the CERP fully and safely into maritime operations, several aspects must be accounted for. The CERP must be tested and verified in order to prove the integrity of the flowchart, as well as supporting documentation and discussion of Cyber Emergency Response Teams (CERT) training must be considered.

4.1 Testing and verification

There are two perspectives that need to be considered for the testing and verification of the CERP. Firstly, there is the verification of the CERP itself. Secondly is the verification of the organisation's implementation of the CERP.

In terms of validating the overarching CERP framework, the authors presented the framework to experienced operators who provided feedback and comments. All of which have been implemented into the final design, ensuring it is accurate at an operational level. To further validate and test the framework more work must be done by putting the CERP into practice either via workshops or simulation exercises with experienced crews. The use of these simulated exercises will determine whether the CERP is a useful decision support tool for crew to understand their response. However, through the use of the three scenarios in Section 3.2, the authors can demonstrate how the CERP works in application providing a soft verification of results. Once further validation has occurred it will allow the CERP to fully fulfil its core purposes.

For an organisation using the CERP as a blueprint for their own cyber incident response it should be tested at all levels of maritime personnel (support, operational and management). To ensure effective preparation and response, both shoreside and ship side personnel should participate in joint training drills allowing technical and operational knowledge to be shared. These drills will also illustrate how decision-making processes may differ across the response team. Thus, informing the development of organisational policy. What is more, through these drills and practices the implemented CERP can be

amended and adapted as required by the organisation. Coupling these results with a detailed cyber risk assessment methodology like the NIST Cybersecurity Framework, will allow organisations to understand crucial systems, assets, their threats and other possible mitigation measures.

Consequently, the utilization of this tool will guide the user through the collection of key information about the cyber incident, affected systems, and operational status. The application will be similar to the NIST Cybersecurity Framework [18], which is recommended by the IMO, as it provides companies with a methodology that they can identify as crucial systems and assets, assess systems threats, and provide needed mitigations procedures. This information can then be used to inform the decision-making process of the crew in response to an incident, to restore normal operation as soon as possible, eventually a safe-enough, temporarily reduced mode.

4.2 Development of checklists

As seen in Section 2.1 it is important for operators to follow industry guidelines as well as comply regulatory requirements addressing cyber security [5]. One such requirement is the development of response plans. Whilst the CERP represents a part of that plan, this paper has also identified checklists as an essential cognitive aid that has many benefits to incident response. In safety-critical industries, checklists have been described as a 'fourth crew member' [30]. Thus, when designed correctly checklists help users recall critical steps, reduce the stress experienced during an incident, as well as maintain effective teamwork [31].

The BIMCO Cyber Workbook provides several examples of checklists which include guidance on the initial response, notification, and investigation of cyber incidents on board [32]. However, these are generic and should be used for reference by organisations as they develop their own which are considerate of their operation specific risks, including the different IT and OT systems. This also includes engaging with other key stakeholders like system operators or manufacturers.

It is also important to note that whilst checklists are useful, they do have limitations such as they set out explicitly the expected actions the crew should take. However, from discussions with industry authors noted that in response to real-world incidents crew often act independently. This deviation, whilst not exactly desirable, might in certain circumstances be the most appropriate response.

Therefore, to help ensure these checklists are appropriate they should be implemented during drills and practices. This has two benefits, like the CERP, firstly it allows the organisation to determine if changes are required, and secondly it allows crews to become familiar with their contents [33]. What is more, by practicing these checklists it allows practice to be reflected upon. As philosopher John Dewey argues, "We do not learn from experience… we learn from reflecting on experience" [34].

4.3 Development of cyber response teams

The roles and responsibilities of people engaging in cyber incident handling are of importance, as emphasised in Section 3.3. The paper has argued that to ensure effective incident response dedicated cyber response teams both onshore and onboard should be developed.

On the shore side, the maritime industry is increasingly using Security Operation Centres (SOC) [35] which can benefit from implementing non-maritime cyber security specialists [36]. As mentioned in the USCG WI, the USCG have already implemented Cyber Protection Teams, which also support the maritime sector, not just land-based companies [24]. BIMCO have put the NIST framework in a maritime context and specify that cyber emergency response team (CERT) should be available to provide timely support to the Designated Person Ashore (DPA) [5, page 53]. In IACS UR E26, cyber emergency response team is not specifically mentioned. However, the document does require that

companies implement procedures for managing cyber security incidents, and designate personnel with the appropriate training and experience to respond to such incidents [25].

Regarding ships, it is not unreasonable to argue that the lines of communication to shoreside support may be unavailable/compromised. Furthermore, with seafarers fulfilling the role of operator they are expected to bring order to an unnormal situation [37]. Therefore, the authors argue that there should be a dedicated CERT on board similar to the dedicated firefighter on board. This crew member should be provided with specific incident response training, which goes beyond cyber awareness. However, as a 2022 study found there is a limited amount of formalized training considering cyber risk in the industry [7]. Thus, operators should develop training that provides key knowledge and skills regarding cyber response, that is considerate of the organisation's operations.

4.4 Training

As argued throughout this paper, certain skills are required to implement the CERP. As the CERP (Figure 4) illustrtaes there are four teams required for effective response. Each of these teams fulfill different roles within incident response therefore need different skills in order to handle cyber emergeny situtations. Thus, different training modules will need to be developed. As per roles and responsobilities, at management-level the general responsibility relies on the Master's and Chief Engineer's operational experience and team management skills. Therefore, training must provide a detailed understanding of cyber risks, and mitigation measure to allow them to identify potential incidents and direct the appropriate resources in response. At an operational level, the onboard technical response team will need specific details regarding systems, their dependencies and troubleshooting methods. For the shoreside teams this training should include the skills required to remotely implement measures, or communicate those mitigations to the crew in language they understand.

As argued drills and practices form a vital role of verfying and testing procedures, they also offer the opportunity for personnel to gain familiarization of the skill they need to deal with abnormal situations. Thus, these drill can provide a dual purpose in training, allowing personnel to not only implement response plans but also develop experiences which can help inform their decisions at a later date.

5. Conclusions

This paper has investigated traditional maritime incident handling, traditional cyber incident handling and maritime cyber security handling. Many of the approaches discussed argue for the need for cyber incident response plans but fail to provide clear details of what these should contain. In response, by analysing incident handling and taking a pragmatic approach in collaboration with maritime industry actors, the authors purpose a maritime Cyber Emergency Response Procedure. As crew on board a ship is traditionally known to take a pragmatic approach to problem solving, the flowchart provides the crew with more a visual representation to a cyber problem-solving approach, than a text-based approach.

This flowchart serves three purposes. Firstly, the CERP acts as a blueprint for organisations to include cyber incident response within their existing response procedures. The proposed CERP is also considerate of the traditional incident response and builds upon and adapts best practices to include elements relevant to cyber incidents. Secondly, the CERP in its current format provides a high-level decision support tool for crews, providing enough details of what steps they should be taking to safely manage a cyber incident. These steps, again considerate of normal incident response procedures, include the involvement of shoreside support and the requirement to consider whether the incident has propagated to other systems. Thirdly, the CERP illustrates where external support from the

shoreside might be needed in order to respond appropriately. This support can come from the technical support teams, equipment manufacturers, or as in the USCG example, the state.

In conclusion, the maritime sector lacks a standardised approach to cyber incident response. By adapting current best practices, the CERP is a vital first step to addressing this issue. However, it is important to note that this is just the first step on a longer road to the effective emergency response to maritime cyber incidents. Further work will be needed to understand the CERP's implementation at an organisational level, as well as the training required to fulfil the roles and responsibilities it highlights. However, the CERP does represent a visual tool that will hopefully start much needed discussions regarding maritime cyber emergency response.

References

[1] NORMA Cyber, "NORMA Cyber Annual Threat Assessment 2022," Norwegian Maritime Cyber Resilience Centre, normacyber.no, 2022. [Online]. Available: https://www.normacyber.no/news/norma-annual-threat-assessment-2022

[2] K. Tam *et al.*, "Case Study of a Cyber-Physical Attack Affecting Port and Ship Operational Safety," 2021, doi: https://doi.org/10.4236/jtts.2022.121001.

[3] International Maritime Organization, *MSC-FAL.1/Circ.3. Guidelines on maritime cyber risk management*, 2017. [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx.

[4] International Maritime Organization, *Resolution MSC.428(98) - Maritime Cyber Risk Management in Safety Management Systems*, 2017. [Online]. Available: http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx. Accessed on: 22.02.2023.

[5] *The Guidelines on Cyber Security onboard Ships Version 4.0*, BIMCO, 2020. [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[6] IACS. "IACS adopts new requirements on cyber safety." IACS. https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/ (accessed 20 February, 2023).

[7] E. Erstad, M. S. Lund, and R. Ostnes, "Navigating Through Cyber Threats, A Maritime Navigator's Experience," 2022, doi: https://doi.org/10.54941/ahfe1002205.

[8] International Maritime Organization. "Maritime Safety." IMO. https://www.imo.org/en/OurWork/Safety/Pages/default.aspx (accessed 20 February, 2023).

[9] International Maritime Organization, *International safety management code: with guidelines for its implementation*, 2018 edition.; Fifth edition. ed. (ISM-Code). London: International Maritime Organization, 2018.

[10] International Maritime Organization, *SOLAS, Consolidated Edition, 2020* (SOLAS). London: International Maritime Organization, 2020.

[11] International Maritime Organization. "The International Safety Management (ISM) Code." IMO. https://www.imo.org/en/ourwork/humanelement/pages/ISMCode.aspx (accessed 23 February, 2023).

[12] International Chamber of Shipping, *Bridge Procedures Guide*. Marisec, 2022.

[13] *ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary*, ISO, iso.org, 2020. [Online]. Available: https://www.iso.org/standard/73906.html

[14] *ISO/IEC 27001:2017 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*, ISO, iso.org, 2017. [Online]. Available: https://www.iso.org/standard/82875.html

[15] *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*, ISO, iso.org, 2022. [Online]. Available: https://www.iso.org/standard/75652.html

[16] *Directive (EU) 2016/1148* European Union Parliament, Official Jounral of the European Union, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[17] *DIRECTIVE (EU) 2022/2555*, European Union Parliament, Official Jounral of the European Union, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1677163438395&from=en

[18] *Framework for improving critical infrastructure cybersecurity*, N. I. o. S. a. T. NIST, 2018. [Online]. Available: https://www.nist.gov/cyberframework/framework

[19] ENISA, "ANALYSIS OF CYBER SECURITY ASPECTS IN THE MARITIME SECTOR," https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1, 2011. [Online]. Available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1

[20] *Cyber security resilience management for ships and mobile offshore units in operation*, DNV, standards.dnv.com, 2016. [Online]. Available: https://standards.dnv.com/explorer/document/0ED73B3209DA42CDA6392BC3946585C9/4

[21] *Rec 166 - Recommendation on Cyber Resilience*, IACS, 2020. [Online]. Available: http://www.iacs.org.uk/publications/recommendations/161-180/

[22] *The Guidelines on Cyber Security onboard Ships Version 1.0*, BIMCO, 2016. [Online]. Available: https://www.bimco.org/about-us-and-our-members/publications/the-guidelines-on-cyber-security-onboard-ships

[23] *ISO 23806:2022 Ships and marine technology — Cyber safety*, ISO, iso.org, 2022. [Online]. Available: https://www.iso.org/standard/77027.html

[24] *Vessel Cyber Risk Management Work Instruction*, United States Coast Guard, https://www.dco.uscg.mil/, 2020. [Online]. Available: https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Inspections-Compliance-CG-5PC-/Commercial-Vessel-Compliance/CVCmms/

[25] *IACS UR E26 Cyber resilience of ships*, IACS, https://iacs.org.uk/, 2022. [Online]. Available: https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

[26] *IACS UR E27 Cyber resilience of ships equipment*, IACS, https://iacs.org.uk/, 2022. [Online]. Available: https://iacs.org.uk/news/iacs-adopts-new-requirements-on-cyber-safety/

[27] T.-r. Qin, W.-j. Chen, and X.-k. Zeng, "Risk management modeling and its application in maritime safety," *Journal of Marine Science and Application,* vol. 7, no. 4, pp. 286-291, 2008.

[28] *ISO 5807:1985 Information processing — Documentation symbols and conventions for data, program and system flowcharts, program network charts and system resources charts*, ISO, iso.org, 1985. [Online]. Available: https://www.iso.org/standard/11955.html

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

[30] P. Greig, A. Maloney, and H. Higham, "Emergencies in general practice: could checklists support teams in stressful situations?," (in eng), *Br J Gen Pract,* vol. 70, no. 695, pp. 304-305, Jun 2020, doi: 10.3399/bjgp20X709373.

[31] D. L. Hepner *et al.*, "Operating room crisis checklists and emergency manuals," *Anesthesiology,* vol. 127, no. 2, pp. 384-392, 2017.

[32] BIMCO, International Chamber of Shipping, and Witherby Publishing Group, *Cyber Security Workbook for On Board Ship Use - 4th Edition, 2023*. Livingston: Witherby Publishing Group, 2023.

[33] F. S. Foundation. "FSF ALAR Briefing Note 1.5, Normal Checklists." SKYbrary Aviation Safety. https://skybrary.aero/bookshelf/fsf-alar-briefing-note-15-normal-checklists (accessed 21 February, 2023).

[34] G. Di Stefano, F. Gino, G. Pisano, and B. R. Staats, "Learning by Thinking: How Reflection Can Spur Progress Along the Learning Curve," *Management Science, Harvard Business School NOM Unit Working Paper No. 14-093,* 2014, doi: https://dx.doi.org/10.2139/ssrn.2414478.

[35] A. Nganga, M. Lützhöft, J. Scanlan, and S. Mallam, "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment," 2022.

[36] G. Stoker, J. Greer, U. Clark, and C. Chiego, "Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution," in *Proceedings of the EDSIG Conference ISSN*, 2022, vol. 2473, p. 4901.

[37] E. Erstad, R. Ostnes, and M. S. Lund, "An Operational Approach to Maritime Cyber Resilience," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation,* vol. 15, no. 1, pp. 27-34, 2021, doi: https://doi.org/10.12716/1001.15.01.01.