Maritime Cyber Resilience project

Maritime Cyber Simulator Scenario Workshop report

Erlend Erstad
Marie Haugli Larsen
Mass Soldal Lund
Runar Ostnes

NTNU in Ålesund, 11.02.22

Norwegian University of Science and Technology
Faculty of Engineering
Department of Ocean Operations and Civil Engineering

Document history:
11.02.22 Revision 1 First issue of document

NTNU

Summary

The 7th of December 2021, the Maritime Cyber Resilience (MarCy) project held a Cyber Simulator Scenario workshop aiming to create a fundament for training to enhance operational maritime cyber resilience.

MarCy is a research project collaboration, between the academic partners Norwegian University for Science and Technology (NTNU), Norwegian Defence University College (NDUC), and the industry partners DNV, Norwegian Hull Club (NHC) and Kongsberg Defence & Aerospace (KDA).

The scope of the workshop was to invite maritime stakeholders and people in the maritime industry to discuss how and if simulator training should be part of cyber awareness training, and what simulator scenarios can be beneficial to implement in such training. The aim was to develop both operational level scenarios for the crew handling ships, and management level scenarios for the shipowners and maritime stakeholders. In addition to this, the workshop led to fruitful discussion how the maritime industry is dealing and coping with cyber threats, and what could be considered as beneficial for cyber training. Real life incidents and experiences was also shared among the participants.

The MarCy project partners and the authors of the report want to express their greatest gratitude for all the participants attending the workshop. The workshop could not have been completed without you. Due to the protection of the privacy for the attendants, no individual level information is given. See more in Section 2.

List of the organizations attending the workshop:

DNV
Island Offshore
Kongsberg Aerospace & Defence
Norwegian Defence University College
Norwegian Hull Club
NTNU – COAST project
NTNU in Ålesund
NTNU in Gjøvik
NTNU – SFI-Move project
Royal Norwegian Naval Academy
The Norwegian Armed Forces Cyber Defence
The Norwegian Armed Forces
The Norwegian Coast Guard
The Norwegian Coastal Administration
The Norwegian Society for Sea Rescue

1 Introduction

The maritime industry is being digitalized and is constantly changing with new technology. This introduces new types of cyber threats towards navigational equipment which is essential for safe navigation. If a cyber threat occurs on board, the navigators and deck officers are expected to handle the situation, yet there is no standardized training on the topic. Cyber security is not even mentioned in the STCW-convention (International Convention on Standards of Training, Certification and Watchkeeping for Seafarers) which is the international baseline curriculum for maritime navigators.

The MarCy[1] project is a "Knowledge building Project for Industry" (KPI), funded by the Research Council of Norway, project number 295077. The MarCy project target cyber security challenges that are specific for maritime digital control systems and maritime operations. The primary objective of the MarCy project is to develop validated means for improving cyber resilience of maritime digital control systems and maritime operations. A part of this is to investigate and develop education and training programs to increase maritime navigators' and operators' awareness of, and resilience against, cyber risks. A vital part of nautical education is simulator training. The scope of this workshop was two-folded. The primary objective was to invite maritime stakeholders to take part in a discussion to map out potential cyber threat simulator scenarios to be implemented in maritime training and education, as well as discuss nearby topics, as relevance, plausibility, realism, and handling of the scenarios. The second purpose of the workshop was to collect data for a PhD project which is part of the MarCy project.

Section 1 introduces scope of the workshop as well as how the workshop was performed. Section 2 presents the identified cyber simulator scenarios. Section 3 presents a summary of the discussions of the workshop sessions. Section 4 concludes the workshop report and provides recommendation for future work.

1.1 Workshop information

In addition to facilitate for discussion, this workshop also intended to give the participants an insight into the equipment used in nautical education at NTNU in Ålesund. NTNU in Ålesund have modern, high-end, full mission bridge simulators, delivered by Kongsberg Digital, type K-SIM[2]. The participants were briefed in the simulators before they were exposed to two cyber threat test-scenarios. The test-scenarios were intended for inspirational purpose only. The idea was to stimulate for creativity and engagement of the participants, making them more willing to share ideas and thoughts later in the workshop discussion sessions. Below is a short description of the introduction scenarios.

[1] Read more on the Research Council of Norway website:
https://prosjektbanken.forskningsradet.no/project/FORISS/295077?Kilde=FORISS&distribution=Ar&chart=bar&calcType=funding&Sprak=no&sortBy=date&sortOrder=desc&resultCount=30&offset=0&Fritekst=marcy

[2] Read more on Kongsberg Website:
https://www.kongsberg.com/no/digital/products/maritime-simulation/k-sim-navigation/

Introduction to the simulators: All participants were given a tour of the simulator-park at NTNU Ålesund. This included the K-SIM Nautical Educational Simulators, K-SIM Research Simulator, and Offshore Simulator Centre (OSC) Research Simulators. All participants were then put in a Nautical Education and Training Simulator for briefing, prior to the introduction scenarios. The briefing was simple, the different components on the simulator bridge were demonstrated to the participants and the simulation were located in the port of Ålesund. This helped the participants to easily explore the capabilities and limitations of the simulators.

First scenario: The first scenario took place onboard a High-Speed Craft bound from Ålesund to Hareid, which is a real-life voyage for freight of passengers. The participants entered the bridge when it was about 10 minutes remaining of the voyage bound to Hareid. When entering port of Hareid very dense fog occurred, and it should be hard to navigate visually past the narrow molos in the entry point of the port. The vessels radar and ECIDS should not indicate any alarms but were set up with a 160-metre antenna offset, providing a false picture of position for the participants. This means, if the participants would have sailed solely using radar and/or ECDIS, they would have crashed into the molo, if they did not proceed with very low speed.

Second scenario: The second scenario also took place onboard a high-speed craft bound from Ålesund to Hareid. This scenario took place in Breisundet, just west of Ålesund. In Breisundet, a military convoy was coming from west, heading into the Hessafjord, all with active AIS and good radar reflectivity, even though they were hard to see due to dense fog. When sailing south towards Hareid, the participants needed to give way for the convoy, forcing them on a collision course with a frigate with no AIS and no visible radar target. The intended thought was that the radar has been intentionally jammed, making the participant unable to view some targets. This could result in a severe collision or near collision with the frigate.

1.2 Privacy of attendants

This workshop was partly audio recorded. Due to the protection of the privacy for the attendants there will not be mentioned any names or personal information which can be traced back to the individual in this report. The participating organizations will therefore be mentioned and appreciated. The participants in the workshop had given written consent to participate, and the workshop was approved by NSD[3], Notification Form 422483. Further information regarding the tape recording of the discussions will be presented in section 3.

For more information, please contact Erlend Erstad, +47 995 00 777 / erlend.erstad@ntnu.no.

[3] More information: www.NSD.no

2 Cyber simulator scenarios

This section documents scenarios identified during the workshop. The intention was to define cyber threat scenarios for operational level and management level operators in the maritime industry, which can be trained for in a safe simulator environment. However, the scenario findings are not divided into operational level and management level scenarios, as the scenarios were found to fit both operational and management level, depending on the context of the to-be-developed scenarios. For example, a plausible ransomware scenario will affect both the crew on board and the shipowner, but it will initiate more action on one part, depending on the setting of the scenario. This section is meant to give inspiration to development of cyber threat simulator scenarios, and not to be considered as a product ready to be deployed in a simulator scenario. By operational level scenarios are meant scenarios which are relevant for crew on board a ship bridge. Management level scenarios are more relevant for other maritime stakeholders, such as shipowners, insurance companies and class societies. Below is a list and explanation of the scenario findings:

- Unintentional cyber threat-scenario
    - Remote access is being mentioned as an emerging issue. Uncontrolled remote handling of the maritime digital control systems from shore can cause severe problems for ships. Service providers can potentially connect to the wrong equipment or even wrong ship, when performing intended maintenance. The participants talked about situations where remote maintenance failed and created a possible dangerous situation. Workshop participants discussed experiences with remote operators shutting down generators and other critical ship equipment on an unaware ship in operation. The intention was to perform service on the equipment on an other ship, but the remote operator connected to the wrong vessel-system.
- Intentional adverse actor cyber threat-scenario
    - Adverse actors can have interest in controlling the maritime digital control systems, using it as leverage for ransom. Possible attack surfaces could be malicious USB-flash drives, unsafe mobile phone charging in the affected equipment, or unsafe internet connection. More and more vessels are somehow connected to the internet, and the internet link may not always be safe. These kinds of scenarios can relate directly to a traditional ransomware scenario but targeted against ship critical infrastructure. Possible scenarios and affected equipment can be:
        - Ballast water treatment system – A cruise ship which gets 15 degrees list to either side will have troubles deploying their lifeboats. This potential attack can be a Remote Access Trojan-attack (RAT).
        - Forced blackout of generators – Adverse actor actively shutting down the generators or machine control systems of a ship in a dangerous situation, for example close to rig or in narrow waters. This potential attack can be a Denial-of-Service attack (DoS).
        - Steering gear equipment – Altering the steering gear in a dangerous situation, for example in port or a dense traffic area. “Ever Given”-

incident is indicated to be a potential cyber threat scenario. This can be both RAT and DoS.
        - Dynamic Positioning (DP) System – Same as the two previous mentioned but affecting the DP system. Could be very critical in close to rig operations. Can be both RAT and DoS.
        - Electronic Chart Display and Information System (ECDIS) and RADAR attack – Alterations, manipulations, and/or DoS of the ECDIS or radar could lead to dangerous situation for the vessel. Can be both RAT and DoS.
        - "Kidnapped cargo"-situation – If a hacker can control maritime digital control systems, a potential situation is the hacker taking control of the vessel cargo. Some ships are carrying freezer containers, which is dependent on constant low temperature, or else the value of the cargo will be damaged. The container systems on board ships are also highly electronical systems today, which means the wrong cargo can go to the wrong destination, if the malicious actor finds a way to do it. This scenario can also relate to tank operations, where a potential adverse actor takes control of the digital control system operating valves and pumps for tankers.
- Manipulating critical onboard sensors and equipment
    - Global Navigation Satellite Systems (GNSS) are today important for the safe navigation of vessels, and high precision of positioning of vessels. GNSS provides signals which can automate most of the navigational tasks a navigator needs to do today. Alterations of such signals could have impact on the control systems used by navigators on a ships bridge.
        - Jammed GNSS signal – The equipment used for navigation is deprived from receiving input from GNSS, and the navigators must utilize more manual modes of navigation. This is reported to be part of real-life incidents, collision of vessels in a situation with lost GNSS signals. GNSS jammers can also be installed in cars or trucks for blocking the authorities' surveillance of the vehicles, which again can affect ferries. Roads and ship fairways are often in the same areas.
        - Spoofed GNSS signal – An adverse actor maliciously manipulating the GNSS signals to send a ship on a course the navigator did not intend to sail, while displaying erroneous position information. This can also have impact on other systems, such as integrated navigation systems, as technologies and equipment on board ships are increasingly interconnected. If the steering gear control system is controlled by Track Pilot mode (i.e., the ship follows a pre-determined route), and the altering of course is controlled by the ECDIS, which again receives GNSS-input, the consequences can be fatal, in for example narrow waters.
    - Automatic Identification System (AIS) are used to identify vessels, displaying information of position, course of vessel, speed, size, etc. Maliciously altering

the AIS information can have impact on the safety of ships traffic, as it is common to rely on the information provided by AIS.

- Nation state attacks could alter the position of vessels, falsely displaying a ships position in hostile waters, while the ship is not actually there. This kind of attack relate closely to spoofing attacks, where the adverse actor alters the position input to the AIS.
- AIS also shows information of what kind of cargo is carried. Some nation states could alter the cargo information to "Nuclear", which is prohibited to carry in some territorial waters. This will initiate an investigation and ship can be subject to unjustified and unwanted ransacking.

- Port stay vulnerabilities
  - This is not directly a scenario but can provide the fundament for a scenario setting or context to a scenario. Port stay is associated with more risk than sailing on the ocean. This is because there is often an uncontrolled flow of service technicians, port authorities, crew for mobilizing the vessel, salesmen, etc. Both physical and digital access to the ship is more accessible than on open waters, and even though there are strict port regulations, malicious actors can use port stays as entry points and attack vectors. Port stays are often also a time with increased internet activity and connectivity, which can cause a potential attack surface for attackers.

3 Workshop discussions

This chapter presents a summary of what was discussed in the different workshop sessions. The participants were divided into three groups for the discussion sessions. Two groups talked in Norwegian and one in English. Each session was moderated by one of the authors of this document, and tape recorded with consent from the participants. After the workshop the tape recordings were transcribed for analysis purposes. The tape recordings were stored on a local tape-recording device, and the transcriptions stored locally.

The aim of the discussions was two folded. The participants were primarily asked to identify possible scenarios for cyber threat situations, but the intention was also to discuss around the handling of these potential situation, their origin, and the potential outcomes. It was also found that the groups discussed more around the topics than first anticipated. The scenarios mentioned in the previous section will not be repeated in this section.

3.1 The discussions

The participants agreed that there should be a difference when facilitating for simulator scenarios to nautical students, compared to experienced navigators. For training scenarios in the nautical education, the observant students will most probably detect errors at once because the scenarios are concentrated and the students actively surveillance the systems, due to the simulator situation they are used to find themselves in. The students will always expect something to happen. For example, GPS-failures will be easily detected, as the students are paying utmost attention to the position and utilizing visual/radar navigation,

as they know they are being observed and evaluated. Simulator training for the nautical students may also be hard to generalize to the common navigator around the world. The NTNU nautical training centre is a very high-end simulator centre, which may not be the case for simulator centres in other parts of the world. The educational system around the world is very diverse, so are the different vessels sailing the oceans.

The participants discussed that small disturbances are the hardest ones to detect. If your vessel jumps from the North Sea to the shores of Canada within a second, you can easily assume something is wrong, for example erroneous position input. The level of alertness will vary during the voyage for navigators. Navigators will most probably be more alert sailing near the coast, than open waters. The participants discussed that humans are only able to hold a sufficient level of alert for 30 minutes in a task, i.e., humans cannot focus on one task for more than 30 minutes, before the level of alertness disintegrates. A question raised in the discussion was if the common navigator is as attentive as the students in a simulator situation. Simulator scenarios are compressed and synthesized situations of what can occur in the real world, however, when sailing a vessel, it can be hours, days, or weeks of sailing before the ship encounters a situation, considering for example overseas voyages. It is seen as unreasonable to expect the navigators to always be agents monitoring the navigation systems sufficiently, especially considering 6- and 12-hour shifts. The instruments navigators are using are working well most of the time. The participants believe it will be hard to detect anomalies in systems that are showing correct information/status 99-100% of the time. The participants do not think the seafarers are expecting something to happen to a more or less stable system, when the ship is not in a critical situation.

A navigator cannot learn all aspects of cyber threats. Therefore, the participants believe the focus of training should be towards situational awareness of cyber-attacks. Making the navigators take a step back and reflect if a cyber-attack is the potential fault in a system is seen as a key factor for success. By exposing navigators to possible cyber threats in simulators, the navigators' troubleshooting-mindset could be altered to also consider possible cyber-attacks/threats. When troubleshooting problems on board ships, cyber threats are not the first thing which comes to mind. In short, the navigators are supposed to look for a ghost they never have seen before. Regarding cyber awareness, both simple scenarios and "James Bond"-like-scenarios are needed, as the participants do believe it is only a matter of time before "James Bond"-scenarios could be realistic.

For seafarers, it can be hard to convert cyber security theory into practice, as the seafarers' interest for cyber security are on a generally low level. The participants believe that for a cyber incident to be relevant for crisis management on board, the cyber incidents need to result in larger and more destructive accidents, such as grounding or collision. Therefore, a cyber crisis will also be treated as a "traditional" crisis. If trained for in a simulator environment, this type of accidents can stimulate to cyber security awareness, as the consequences of a fault will be visualized.

The participants highlight that asking the right questions is important in traditional preparedness scenarios. What is the situation and what to the shipowner do? Do they have the resources, the right persons, the right procedures? The key is to create awareness and

understanding of the situation. Regarding maritime cyber resilience, the seafarers should be trained in the most common cyber-attacks to build experience and a mental library of possible situations. Going from a novice to an expert takes time and experience. The participants also highlight that an expert in navigation can be a novice in cyber security, and vice versa.

A triangular approach to threats is suggested, where technical equipment, competence, and culture are considered. These factors need to correlate, and one should not exceed the other. Simulator scenarios need to be classified to pinpoint the purpose of the scenarios. The scenarios can range from tabletop scenarios to full scale preparedness onboard or onshore scenarios. When designing simulator scenarios, it could be beneficial to have a different approach when considering highly experienced seafarers and novice seafarers. Highly experienced seafarers might not take a "James Bond"-scenario seriously, as the consequences is too farfetched and unrealistic for their understanding of reality. They will not consider such scenarios to be likely for their ship and operation. Scenarios designed for highly experienced seafarers should have a solid foundation in reality, to get the seafarers interest and attention. The scenarios should also be relevant for the ship, as the experienced seafarers have in-depth ship knowledge. In contrast, the students may be more open for "James Bond"-scenarios, as they have not yet developed the same kind of in-depth knowledge. They will tend to trust the simulator instructor more than their own experience, which will often be opposite for the experienced seafarers. The training could also benefit from being gradually incorporated. Some examples are drawn to the companies who send "friendly" malicious emails to their employees and gives a warning if the employee have clicked on a potential malicious link.

The participants who have previously participated in cyber crisis preparedness exercises urges the importance of debriefing with cyber security experts after such an exercise. In one mentioned cyber preparedness exercise where the ballast water management system of a vessel was compromised and hijacked by hackers, the dedicated cyber crisis response company had a walkthrough with the navigators after the exercise. The intention of this was to explain how the attack was even possible. This was seen as an eye-opener and clearly beneficial to the participants in the cyber preparedness exercise. The most vital part of the simulators scenarios is the people in the scenario. This adds an important dimension which is needed to get a fruitful test of the preparedness of the company.

Participants from the naval defence sector highlights that they do not treat "cyber" as a separate focus area, but rather as an addition to traditional problem solving. Cyber is balanced across the whole industry, similar as safety and security is implemented in an organisations procedures and operation. Today, leaders must have a better understanding of the system the organisation is using. It is no longer acceptable for a leader to mean that cyber security is someone else's problem. A leader in the armed forces need to take more responsibility towards cyber security. If they cannot adapt to these kinds of requirements, the leaders will be asked to reconsider their role. This issue can be challenging for many leaders, as leaders in any organisation will normally be expected to consider operations and matters on a management level, not a detailed, operational level. This is now changing for cyber threats and may also be a momentum for civilian organisations to consider.

4 Conclusion

This workshop report has summarized the findings of a cyber security simulator workshop. Cyber security cases undertaken in simulator scenarios were in unison seen as beneficial for the maritime industry. Mariners are familiar with simulator training, and if done right, one could get the attention of both novices and expert mariners. Design of scenarios should be tailored to the intended people undertaking the scenario. The participants were eager to share what they found important and realistic to consider when designing scenarios. Organisations could benefit of implementing cyber security in the organisation as a whole, and this could also be the case for education. Cyber security should be an integral plan of business strategies and educational plans, to create foundation for inherent cyber resilience in the maritime industry.

Future work will be to implement the findings from this workshop report in the development of maritime cyber resilience training. This implementation will aim at developing both shipowner and ship crew specific training, as well as simulator training in the M.Sc. course “Maritim Digital Sikkerhet” within the M.Sc. degree program “Management of Demanding Marine Operations” at NTNU in Ålesund.