2022

Multi-Purpose Cyber Environment for Maritime Sector

Visky, G

10.34190/iccws.17.1.26
International Conference on Cyber Warfare and Security
Academic Conferences International Ltd

Multi-Purpose Cyber Environment for Maritime Sector

Gabor Visky[1], Arturs Lavrenovs[1], Erwin Orye[1], Dan Heering[2], Kimberly Tam[3] and Olaf M. Maennel[4]
[1]NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia
[2]Estonian Maritime Academy, Tallinn University of Technology, Estonia
[3]University of Plymouth, UK
[4]Department of Computer Science, Tallinn University of Technology, Estonia
gabor.visky@ccdcoe.org
arturs.lavrenovs@ccdcoe.org
erwin.orye@ccdcoe.org
dan.heering@taltech.ee
kimberly.tam@plymouth.ac.uk

Abstract: The cyber attack surface in a maritime environment is constantly growing. More current information and computer technologies are being used on cargo and passenger ships to save on operational costs and increase navigational safety. Along with the growing reliance on automation, the risk of a disruption to a vessel's critical systems by drawing on the wrong inputs from sensors to change the behaviour of the actuators has significantly increased. Traditional operational technological systems are much more complicated to update than the automatic software updates we see in information technology systems. To better understand existing cyber threats in the maritime sector and increase cybersecurity resilience, this paper aims to replicate the digital components of a ship's bridge to examine scenarios when the bridge system loses connectivity, receives the wrong inputs from sensors, or the internal system becomes compromised. The simulator differentiates fundamentally from traditional simulators or digital twins in the maritime sector that focus on training seafarers. This environment generates data streams that are similar to those on board a ship. Those data streams can be analysed, modified and spoofed to observe the effects. The effects can be technical but it is equally necessary to analyse how human beings would react in specific circumstances. Our work provides the opportunity to isolate the ship network traffic, conduct penetration testing, find cybersecurity vulnerabilities on devices, and execute cyber attacks without the dangers associated with running such scenarios on a vessel in the open sea.

Keywords: maritime, cybersecurity, testbed

1. Introduction

Cyber threats and actual incidents in the maritime sector are constantly growing. Recent cyber incidents and accidents have highlighted how fragile the naval industry is, despite its importance in world trade. The industry depends increasingly on digitalisation, integration of systems, operations, and automation. The growing role of autonomous vehicles makes the problem more severe. The consequences of possible cyber attacks can include financial losses, safety issues, bad publicity, and compliance risks. The cases usually originate in technology, staffing, or cybersecurity operating procedures that lead to technology testing and education.

This paper proposes a multi-functional environment for cyber-related education and maritime-related cyber research that is flexible enough to adapt to specific needs. Although the proposed environment has enormous potential in education, this paper highlights the technical perspective and introduces the testbed functionality. The simulator aims not to provide sailing-related experience but focuses on the consequences of cyber attacks and how to react to those attacks. Furthermore, the environment offers a maritime-related climate for cyber experts to conduct experiments.

The environment has a network similar those found on vessels. The generated data streams traffic is used as a source for analysis and penetration testing. Using the simulator, we achieve similar results to those on actual vessels without violating the integrity of the expensive equipment on board a ship. Even though the proposed environment has considerable potential for education, this paper highlights the technical perspective and introduces the testbed functionality.

The first section focuses on the current situation in the maritime sector and its challenges. In Section 2, we provide relevant background on cybersecurity in the maritime sector. Section 3 reviews related research addressing the available solutions that can be used as a training or research environment. In Section 4, we describe the setup of the multi-purpose cyber environment that was built on the premises of the NATO

Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonia, and discuss its similarities and differences compared to a real ship. Section 5 presents the conclusions and highlights the future directions.

2. Background

In recent times, the importance of cyber defence has been continuously increasing in the maritime sector, as in other industries. The following section provides an overview of the sector's specific characteristics.

2.1 Cybersecurity in the maritime sector

Nowadays, the importance of the shipping industry for modern society is constantly growing. The volumes of goods carried by ships in 2019 reached 11.08 billion tons (*Explaining shipping*, 2021). It is estimated that over 80% of world trade is carried by the shipping industry (United Nations, 2021). The need to reduce operational costs has led the shipping industry to seek new and advanced technological solutions. In 2017, the International Maritime Organization (IMO) initiated a scoping exercise to determine how the safety, security and environmental soundness of Maritime Autonomous Surface Ships (MASS) operations might be addressed using IMO instruments (International Maritime Organization, 2021). The development of technologies and policies that make autonomy a feasible solution has enabled several organisations to make progress on such projects and will soon sail their first autonomous ships (Tam and Jones, 2018).

Along with the growing reliance on automation, the risk of external interference and the disruption of critical systems is greatly increased; malicious actors can interfere with the different control systems of the ship. They can cut off all external communications or obtain confidential data. Cybersecurity on board ships is gaining in importance due to recent incidents on ships at sea (Caprolu *et al.*, 2020).

In June 2017, the world's largest container shipping company, A.P. Møller-Maersk was one of the companies hit by the malware NotPetya (WIRED, 2018). In July 2018, one of the biggest shipping companies, China Ocean Shipping Company (COSCO), was victim of a cyber attack (Goud, 2018). Norsk Hydro was hit by an extensive cyber attack in March 2019 (SAFETY4SEA, 2019). Although these incidents were ransomware related and the role of the operators was high, it has been successfully demonstrated by researchers that both information technology (IT) and operational technology (OT) systems used on board have vulnerabilities that can be exploited or exposed unintentionally by crew members (Bhatti and Humphreys, 2017), (Pen Test Partners, 2020).

Those unique circumstances demanded creating an environment for research and education in this field so that the maritime sector will become more resilient to cyber attacks.

2.2 Aspects of cybersecurity

Cybersecurity refers to the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber attacks. In Information Technology (IT) it focuses on the practice of ensuring the confidentiality, integrity and availability of information (CIA triad). It comprises an evolving set of tools, risk management approaches, technologies, training, and best practices designed to protect networks, devices, programs, and data from attacks or unauthorised access (Gourlay, 2000).

Cybersecurity has several aspects: application security, information or data security, network security, disaster recovery/business continuity planning, operational security, cloud security, critical infrastructure security, physical security, and end-user education. Technology, people, and regulatory frameworks are always essential to solving problems in cybersecurity, and this is no different in the maritime field. These three elements are fundamentally interconnected. At the same time, research can improve how these function from a cybersecurity perspective for the maritime sector.

According to (Fortress Information Security, 2020), the maritime-specific cybersecurity challenges span technology, staffing, and cybersecurity operating procedures. The main purpose of this work is to provide an environment that can be used to educate the crew, research technologies and test operating procedures.

2.3 Technology-related challenges

Maritime organisations have a vast array of legacy operational technology (OT) and information technology (IT) systems deployed. The majority of those systems were not designed with cybersecurity in mind. In addition, the different OT system configurations and architectures on the various ships make it challenging to secure the network infrastructure and their topologies aboard a vessel.

The situation is becoming more severe since autonomous or remotely operated off-shore vehicles will contain even more OT components, interconnected with navigational and other subsystems. Since the control system of the whole industry cannot change overnight, new ships have to maintain compatibility with obsolete systems, and since they have the heritage of old solutions requested by legacy standards, the applicability of the newest cybersecurity solutions will be limited.

Despite growing automation on ships, communication links use satellite-based solutions that provide only limited bandwidth. These circumstances limit remote assistance and maintenance in the case of a cybersecurity problem.

Appropriate technologies (e.g. antivirus, firewalls, intrusion detection/prevention systems, endpoint security and others) should be selected and implemented to provide comprehensive cybersecurity protection for these OT systems. Still, ship-system producers keep sailing safety in the primary position, often at the cost of cybersecurity. In most cases, it is hard to select the proper defence solution for several reasons.

The applied technology is barely standardised, the communication standards are vendor-specific, and furthermore, with an approximated 40-year life cycle, operators on ships cannot update CPS on the same frequency we are doing with generic IT systems where software vendors are constantly pushing their updates. Therefore, it is difficult to neutralise potential vulnerabilities in this field and this leads to weak system resilience. Currently, there is a lack of environments in which we can research and educate the maritime sector to test the different components individually or the whole system.

2.4 Education-related challenges

Ships, ports, terminals and offshore facilities are increasingly dependent on networked information and communication technology (ICT) (Heering *et al.*, 2020). Seafarers must be ready to cope with a growing number of cyber threats on board ships, with cybersecurity awareness playing an essential role in emergency and crisis management. Maritime education and training institutions (MET) offer high-level facilities for training seafarers, such as maritime simulators. These tools aim at learning and practising different operations like sailing, docking, and the use of onboard devices like RADAR, Electronic Chart Display and Information System (ECDIS), and others. Cybersecurity education is usually outside the scope of the curriculum, and the facilities do not support this task.

The authors argue that a certified ship bridge simulator can be used for teaching and practising responses to cyber-related incidents. Besides this fact, the lack of a proper testing environment is a severe barrier to improving cybersecurity awareness. The key to more cyber-safe operations at sea lies in the proper implementation of cybersecurity awareness training for active and future seafarers by taking into account their responsibilities onboard the ship and their background knowledge of IT. Training and awareness are key elements to effective cyber risk management on ships.

3. Related work

3.1 Testbeds

Determining the vulnerabilities of industrial control systems using embedded devices is a complicated process because of the complex hardware and software interactions. Lund et al. (Lund *et al.*, 2018) shed light on the great importance of the central components like Integrated Navigation Systems (INS) and ECDIS for the safety and security of maritime operations, but claims that the topic has barely been studied.

One approach is to build a comparatively simple system that captures the relevant complexity (i.e., a testbed) (Davis *et al.*, 2006). A testbed is an essential tool, avoiding the need to experiment exclusively on live systems. The topic is highly researched in the field software testing, primarily in the context of vulnerability identification. Salunkhe et al. have published (Salunkhe *et al.*, 2018) systematic literature review results regarding the cyber-physical testbeds focused on simulation. According to their findings, the literature focuses on electrical grids, network and communication, but not on maritime related topics.

Frank et al. introduce the design considerations for cybersecurity testbeds (Frank *et al.*, 2017) for education. The main requirements were automated deployability, reusability, low cost, high availability and scalability. The paper introduces the main challenges of the testbed setup and installation, but the cases focus on the vulnerabilities of web application, which is not relevant on a ship.

3.2 Maritime-related solutions

Brinkmann and Hahn offer a testbed architecture for maritime systems (Brinkmann and Hahn, 2017). Their work introduces the physical testbed 'LABSKAUS' (Laboratory for Safety Critical Analysis On Sea) as part of the eMaritime Reference Platform (eMIR), which is a CPS, and provides various maritime specific components, such as a reference waterway, research boat, sensor infrastructure and a mobile bridge. According to the paper the development of safety-critical systems such as a highly automated and autonomous vessel brings the need to establish a test environment (or 'testbed') close to the real world in addition to simulative test environments. This solution can support the development, validation and certification process. The highly sophisticated testbed uses a sensorbox that contains sensors and actuators which correlate with the environment; for example, a waterway network or a hydrodynamic environment. The complex system supports the solution of technical questions, but does not have educational features.

Modelling and simulation technologies are also extensively used in the maritime industry. A digital twin is a digital representation of a physical object, asset or system: a ship, a car, a wind turbine, a power grid, a pipeline, or a piece of equipment, such as a thruster or an engine (Smogeli, 2017). Although they enable early and continuous simulation-based testing, cutting the expenses of the system integration (Smogeli, 2017), this solution cannot be used to identify vulnerabilities, since the digital twin setup differs from the actual devices installed on ships. At the same time, a system based on a digital twin can be used for cybersecurity education.

Tam et al. presents a Cyber-SHIP Lab (Hardware, Software, Information and Protections) as a next-generation research capability for maritime cybersecurity (Tam *et al.*, 2019). This facility offers a complex research capability considering the physical aspects as well as the digital, with a lab that is accurate at the hardware level and not based on simulation or emulation. According to the plans, Cyber-SHIP would accommodate ship controller devices, so ship-identical systems could be installed at a considerably higher budget. Multiple configurations of the equipment can be created to imitate different ships. Although the setup proposed in our paper has the same objectives (supporting research and education), but our solution uses simulation-based data source that offers a more simple setup but still close to the real world.

Although the relevant literature is rich, only a few papers are available about a maritime-related environment for education, research and penetration testing. Their research offers help for industry, government, and academia to understand and mitigate cyber threats in the maritime sector.

4. Multi-purpose cyber environment

As was introduced in the previous chapter, the maritime industry faces challenges in cybersecurity. These issues are also growing instead of getting easier to solve. The following section presents the multi-purpose cyber environment, a tool that can be used to ease the pain related to those problems.

The solution can be used for several different purposes. Besides the demonstration and educational functions, it offers data source functionality and environment vulnerability testing.

4.1 System setup

The environment is based on a Transas NTPRO 5000 Navigational Simulator that was designed exclusively for educating crew. A simulator environment contains the visualisation part that is responsible for the audio and visual experience, with several TVs, as it can be seen on Figure 1.

All the environmental parameters that can influence the simulated ship, such as visibility, wind and weather conditions, current and tide, can be set on the instructor machine, just like marine traffic and the position of other ships, that defines the RADAR picture and NMEA-Messages from real world data (e.g. Automatic Identification System (AIS)).

Figure 1: Multi Purpose Cyber Environment

The seafarer, who operates the simulated ship can control it via its fundamental components – the wheel, buttons and telegraph – and can see the actual status of the vessel on the screen of the coning machine. All the parameters are calculated by the simulator server. The crew can use the MFD as on a real ship. Since the laboratory is used for demonstration purposes as well, an extra monitor is added on which the screen of the MFD can be seen. As Figure 2. shows, the original setup was extended using a Gateway Machine, Researcher's Computer, Data Collection Unit and additional MFD for research purposes.

In a simulator environment, the central components (i.e. MFD and ECDIS) are identical to the devices installed on ships, but the computers contain simulator-related software components as well. These software components (RADAR and MFD Server) generate a ship-like network traffic according to the simulated values; therefore, the network traffic of the sensors and RADARs exists only in these computers and are not available from outside of the device.

In contrast to a real ship, the sensors measure the different physical values that are converted into a digital format and transferred via NMEA-0183 protocol to the sensor integration unit – though given different names such as Data Distribution Unit, Data Acquisition Unit, Data Collection Unit (DCU), Sensor Concentration Unit and so on – that converts these values into an IP based data communication format, usually TCP. (In some cases, the sensors have direct serial connections to the workstations) Since the RADAR data (picture) is different from the sensor data, the RADAR is treated differently: it is connected directly to the INS. RADAR can have an independent network or it can use the same network but a different protocol, for example UDP.

The main purpose of this research was to create an environment, where the ship network traffic appears, and the control devices are exactly the same (without simulator-related software pieces) like on a vessel. This solution provides the opportunity to isolate the ship-network traffic, conduct penetration testing on devices, or simulate cyber attacks. To achieve this goal, a Gateway Machine is used to host the RADAR and MFD servers, emulate the ship's RADAR and the DCU from which the ship-related data is available. The simulator sends the simulated data to the Gateway Machine, and the MFD and RADAR application also connects to it and reads the sensor values and RADAR pictures.

Since the simulator offers a wide range of ship types, the solution provides configurable network traffic that is very close to the actual ship's network traffic.

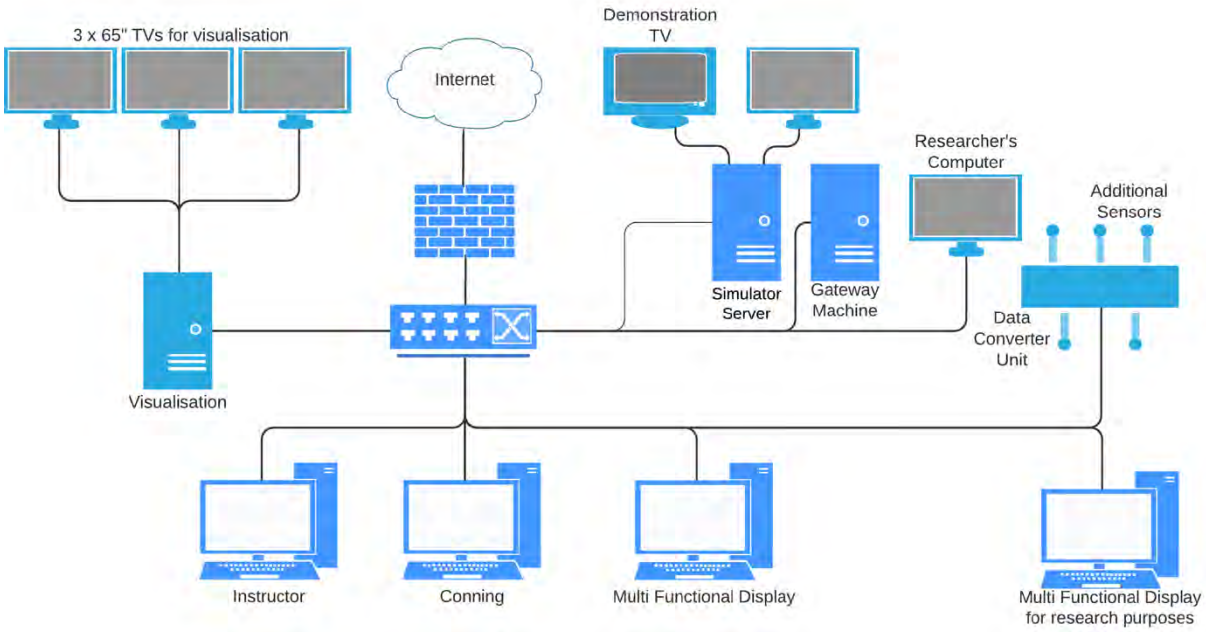

Figure 2. System setup.

4.2 Use cases

The multi-purpose cyber environment can be used mainly in the field of technology and education. This paper focuses on technology-related use cases that will be introduced in detail in this chapter.

4.2.1 Vulnerability testing environment

Nowadays, a ship can have several isolated networks for different purposes. The navigational network, the ship control network, the WiFi network used during loading and unloading the cargo, and the propulsion controlling network are all isolated networks (sometimes physically). The networks are logically interconnected by different crew members, who operate different devices based on data from different sources. As the level of integration between ships is increasing, these networks could no longer be separated. With less system isolation to protect systems, environments for simulating complex networks become more useful to the maritime sector.

The obsolete, twisted-pair and serial data transmission based on IEC 61162-1/NMEA-0183, and more recently the NMEA-2000 protocols are widely used on vessels. Since the devices that use these protocols must be integrated on modern ships, the legacy protocol was encapsulated into TCP/IP packets. Although this solution was simple, it brought a considerable amount of cyber-related problems into the picture. The modern ships using TCP/IP networks use legacy NMEA-0183 protocol packets encapsulated into TCP packets to transport their sensor data. The multi-functional environment can be used for generating this kind of network traffic, which can be analysed and reused in different ways.

The highly sophisticated switch offers Encapsulated Remote SPAN (ERSPAN) capability. As the name says, it delivers generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains. This feature together with the installed VNC clients enables full remote and network traffic analysis via a Virtual Private Network (VPN).

The Transas NTPRO-5000 – on which the environment is based – offers several different ships with its sensor and actuator sets for selection and the available sensor data generated according to the selected ship's sensor set. In the ship's network segment a research computer is installed for network traffic analysis, creation, and modification purposes. This solution offers an environment, where the ship-identical network data is available for the tested device, together with a modified or artificially generated one.

The environment also helps develop and test cyber defence solutions, such as antivirus, intrusion detection systems, and so on, since all the necessary devices are available for measurement and behaviour analysis in the setup.

4.2.2 Offensive cyber testing environment

There exist dozens of different types of cyber attacks, and defending against them is a tedious task with no single overall solution available. Since ships can be considered a system of systems, their defence, especially via the IT infrastructure and port management systems, is demanding. A ship's controlling device is an industrial control system (ICS). These are specialist information systems that differ significantly from traditional information systems used in the IT world (Drias *et al.*, 2015). Some attacks are not applicable against a ship; for example, phishing attacks, URL interpretation attacks, or web attacks.

In a ship, one primary defence against cyber attacks is air-gapping ship controls, navigation, and sensors from the rest of the IT systems, networks and the internet. Correctly implemented air-gapping creates a challenge for the attacker. If there is no possibility of a network connection, the remaining way to compromise the system is to deliver malware via a physical medium such as a thumbdrive, which is connected to and physically transferred between the air-gapped system and other ship or off-ship systems that are compromised and ready to deliver the malicious payload.

A scenario with an inside attacker significantly expands the attack surface on the air-gapped system. An insider might purposefully craft and deliver malware via physical media, or even do it off-ship or instruct somebody else to deliver it. An insider might break the air-gapping by physically connecting to another ship network that can have deployed malware on other connected computers making it less noticeable. Air-gapping could be broken permanently, temporarily (e.g., to deliver malware), or intermittently – installing a communication device that could receive commands from and send data to an off-ship location. In the simplest case, it could be a mobile router or modem with a mobile data roaming plan that works across the globe and can communicate in ports or near the shore, or any of the vast variety of point-to-point communication devices enabling communication in more fixed locations or between moving ones (e.g., from another ship).

In the simplest case, these communication devices can be connected directly to one of the computers in the air-gapped network and be used by already functioning malware. In this case, the communication device only provides a communication channel for the malware, the computer provides power and the network stack. The malware injects network packets or manipulates the system's inputs or outputs. This type of deployment is the most visible at the system level – it might be visually displayed, visible in the systems network configuration and the malware might also be detected by defences on the infected system.

Other cases can combine a communication device with a networking device that can inject (e.g., VPN router providing OSI Layer 2 access to an attacker) or modify (e.g., transparent firewall or similar device on the line) packets in the air-gapped network. These deployments can function without deployed malware, and therefore can be harder to detect but also can have less functionality. The most obvious scenario is establishing a foothold and communication channel inside the network of the systems, usually a switched Ethernet network.

Individual systems have their own set of controls and sensors that are directly connected to the system via a shared communication bus or point-to-point connections, which is commonly aggregated by a controller. Most of the controls or sensors can be replaced by compromised ones or a network intermediary device on the line that injects or modifies the data stream. The best point for the injection of a physical malicious control channel (or pre-programmed device or software) is the control board which allows the data stream of multiple inputs or outputs to be modified at the same time.

Without purposeful inspection, malware injected physical devices or breaches of air-gapping are hard to find as usually nobody is looking for those as long as everything functions properly. Therefore, the attacker can be dormant for months or years waiting for a specific moment or an opportunity to achieve an objective – disable the ship to get it stranded or take over control to crash it into another ship, the shore or a port.

The controller component (processor unit), such as ECDIS or MFD or a sensor, uses the multi-purpose cyber environment to test against cyber attacks. All the described potential attacks can be classified as either network (packet injection, modification, replay) or system (malware). This allows us to simulate and research all the possible outsider and even more diverse insider attacks.

4.2.3 Maritime-related experiences

The widely used legacy NMEA-0183 industrial protocol does not have sophisticated error correction, nor encryption; therefore, TCP packets containing NMEA-0183 messages can be faked or injected easily. A possible attack scenario could be a malware attack, where the malware is installed and sends TCP packets with valid sensor data. This kind of infection can be carried out in the supply chain or during software or chart updates on the ship.

Despite the fact that the periodicity of the sensor data is predictable, it is not checked in the ship's controller devices, so the displayed value can be overwritten if new -incorrect- data arrives right after the correct value. There are no resources describing how to detect abnormal behaviour in the messages with the valid payload. A possible solution could be an extension of an intrusion detection system that analyses and checks the data itself. This solution could also compare different sensor's data like speed data from speed sensor and location data from the GPS.

5. Summary and future works

The multi-purpose cyber environment introduced here aims to provide both education and research in cybersecurity issues for a specific vessel. Although this paper introduced only the technical and research perspective of the environment, education-related usage is the subject of a follow-up paper.

The solution increases cybersecurity research capabilities to include maritime cybersecurity, particularly for analysing systems, hardware and software components, protection development, and testing existing procedures.

Further development is needed to separate the ship-related and the simulator-related network traffic in order to create a more realistic environment.

References

Bhatti, J. and Humphreys, T. E. (2017) Hostile Control of Ships via False GPS Signals: Demonstration and Detection, *NAVIGATION*, 64(1), pp. 51–66.

Brinkmann, M. and Hahn, A. (2017) Testbed architecture for maritime cyber physical systems, in *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*. *2017 IEEE 15th International Conference on Industrial Informatics (INDIN)*, Emden: IEEE, pp. 923–928.

Caprolu, M. *et al.* (2020) Vessels Cybersecurity: Issues, Challenges, and the Road Ahead, *IEEE Communications Magazine*, 58(6), pp. 90–96.

Davis, C. M. *et al.* (2006) SCADA Cyber Security Testbed Development, in *2006 38th North American Power Symposium*. *2006 38th North American Power Symposium*, Carbondale, IL, USA: IEEE, pp. 483–488.

Drias, Z., Serhrouchni, A. and Vogel, O. (2015) Analysis of cyber security for industrial control systems, in *2015 International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications (SSIC)*. *2015 International Conference on Cyber Security of Smart cities, Industrial Control System and Communications (SSIC)*, Shanghai, China: IEEE, pp. 1–8.

Explaining shipping (2021). URL https://www.ics-shipping.org/explaining/ (accessed 6.25.2021).

Fortress Information Security (2020) *White Paper: Building A Sustainable Maritime OT Cyber Security Program*. URL https://fortressinfosec.com/building-a-sustainable-maritime-ot-cyber-security-program/ (accessed 5.22.2021).

Frank, M., Leitner, M. and Pahi, T. (2017) Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education, in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*. *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Orlando, FL: IEEE, pp. 38–46.

Goud, N. (2018) *Cyber Attack on COSCO*, *Cybersecurity Insiders*. URL https://www.cybersecurity-insiders.com/cyber-attack-on-cosco/ (accessed 5.17.2021).

Gourlay, L. (2000) *Chambers guide to English for I.T. and the internet*. Edinburgh: Chambers.

Heering, D., Maennel, O. and Vanables, A. (2020) Shortcomings in cybersecurity education for seafarers. Preprint.

International Maritime Organization (2021) *Autonomous ships: regulatory scoping exercise completed*. URL https://www.imo.org/en/MediaCentre/PressBriefings/pages/MASSRSE2021.aspx (accessed 6.25.2021).

Lund, M. S. *et al.* (2018) Integrity of Integrated Navigation Systems, in *2018 IEEE Conference on Communications and Network Security (CNS)*. *2018 IEEE Conference on Communications and Network Security (CNS)*, Beijing, China: IEEE, pp. 1–5.

Pen Test Partners (2020) *Speed 2 – The Poseidon Adventure – Part One*. URL https://www.pentestpartners.com/security-blog/speed-2-the-poseidon-adventure-when-cruise-ships-attack-part-1/ (accessed 7.19.2021).

SAFETY4SEA (2019) Norsk Hydro lost about $35-40 million after cyber attack, *SAFETY4SEA*, 1 April. URL https://safety4sea.com/norsk-hydro-lost-about-35-40-million-after-cyber-attack/ (accessed 5.17.2021).

Salunkhe, O. *et al.* (2018) Cyber-Physical Production Testbed: Literature Review and Concept Development, *Procedia Manufacturing*, 25, pp. 2–9.

Smogeli, Ø. (2017) Digital Twins at Work in Maritime and Energy.

Smogeli, Ø. (2017) FEATURE FEBRUARY 2017, p. 7.

Tam, K., Forshaw, K. and Jones, K. (2019) Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities, in *Conference Proceedings of ICMET Oman*. *International Conference on Marine Engineering and Technology Oman*, Muscat, Oman: IMarEST.

Tam, K. and Jones, K. (2018) Cyber-Risk Assessment for Autonomous Ships, in *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, Glasgow: IEEE, pp. 1–8.

United Nations (2021) *Review of Maritime Transport 2020.* S.l.: United Nations.

WIRED (2018) *The Untold Story of NotPetya, the Most Devastating Cyberattack in History*. URL https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 6.25.2021).