Phish & Ships and Other Delicacies from the Cuisine of Maritime Cyber Attacks

Jan Bauer[•] Joris Kutzner[•], Philipp Sedlmeier[°], Anisa Rizvanolli[°], Elmar Padilla[•]
[•]*Cyber Analysis & Defense*, *Fraunhofer FKIE*, Wachtberg, Germany
{firstname.lastname}@fkie.fraunhofer.de
[°]*Ship and Information Management*, *Fraunhofer CML*, Hamburg, Germany
{firstname.lastname}@cml.fraunhofer.de

Abstract—**Attacks on our critical infrastructures in the areas of water and energy supply, information and communication technology, but also transportation are increasing worldwide and the incidents have long since moved beyond their physical origins into cyberspace. Recent geopolitical changes have further raised awareness of the vulnerability of our fragile infrastructures and highlighted the urgent need to protect them from cyber threats. This also applies to the maritime transportation system, with its ships as elementary assets. Hence, the advancing digitization and interconnectivity on board maritime vessels require security measures to counteract this increasing risk of cyber attacks. These measures include the conception and development of effective prevention mechanisms, but also techniques for attack detection, in-depth testing of existing bridge components, as well as specialized training for the ship's personnel. Especially for the latter, an environment is required that reflects real-world conditions and allows to perform cyber attacks, e.g., *phishing* campaigns, in a user-friendly way. Despite the need for such an environment, there are few training grounds that meet these requirements in practice. In this paper, we therefore present a laboratory that combines real bridge hardware equipment with digital cyber security tools in order to develop test and training scenarios with respect to maritime cyber security.**

Index Terms—**Maritime Cyber Security (MCS), Integrated Bridge System (IBS), Security Testbeds, Human Factor**

I. Introduction

The Maritime Transportation System (MTS) with its increasing reliance on digital systems that are connected via different Information and Communications Technologies (ICTs) plays a key role in the global economy with roughly 80 % of global trade [1]. The fact that nearly two-thirds of the world's total petroleum and other liquid energy supply is carried by ship emphasizes that most global supply chains are existentially dependent upon the maritime sector. However, the increased connectivity and dependence on technologies create an attack surface for various cyber attacks, not only with regard to onshore enterprise ICT [2], but also concerning all types of maritime vessels [3]–[7] as elementary units of the critical infrastructure represented by the MTS. Such attacks could target Integrated Bridge Systems (IBSs) and maritime systems responsible for navigation directly, or hit them by accident, leading to severe consequences for the ship's crew, its environment, or even global economy - similar to the *Ever Given*'s grounding in the Suez Canal in March 2021.

Identifying vulnerabilities, detecting suchlike cyber incidents, and responding appropriately is thus crucial for the secure operation of maritime vessels. Beyond that, a future-proofed cyber security strategy includes the implementation of adequate prevention, protection, and recovery strategies. Ships are expensive assets with a long life-time. The current merchant fleet is on average 22years old [8] and many ships will probably be in operation for at least the next decade. At the time when these ships were designed, the cyber security aspect had not come into focus. Therefore, the main steps of a successful and effective cyber security strategy should be adapted to fit the specific age of a ship and its system.

To face this challenge and to support maritime actors, the International Maritime Organization (IMO) urged administrations to address cyber security in Safety Management Systems (SMSs) from 2021 onward [9]. The resolution puts cyber and non-cyber risks on the same level and thus triggers the definition and adaptation of processes and operational measures for effective reactions in case of cyber attacks.

With regard to the preventive security measures of future systems, the International Association of Classification Societies (IACS) recently published the two unified requirements E26 [10] and E27 [11], which are to be made mandatory for approval of classed ships commissioned for construction in or after 2024. These requirements virtually enforce the inclusion of cyber security aspects as early as during the design phase of a ship and its components.

Insurers can be another driving force for the implementation of measures for maritime cyber security if they monetize the measures already in place in their insurance tariffs [12]. Yet, both, classification societies and insurers, require knowledge of vulnerabilities and attacks as well as the opportunities to test systems and to validate security capabilities.

Furthermore, while the current autonomy trend is also progressing in the maritime sector, *crewed* shipping will be predominant for decades to come [8], [13]. This concerns human Maritime Education and Training (MET), which still lacks cybersecurity awareness [14]. In addition, practical experience shows that the so-called human factor must not be neglected in security considerations under any circumstances. The urgency for cybersecurity is further amplified by the current geopolitical situation with its state-sponsored cyber threats [15]. Overall, there is a need for a realistic and safe testing environment for executing maritime cyber attacks, for identifying possible weaknesses and vulnerabilities, as well as for conducting appropriate MET of maritime personnel. However, creating such an environment is challenging, both due to costs and the lack of availability of user-friendly cyber attack and test tools tailored to maritime systems.

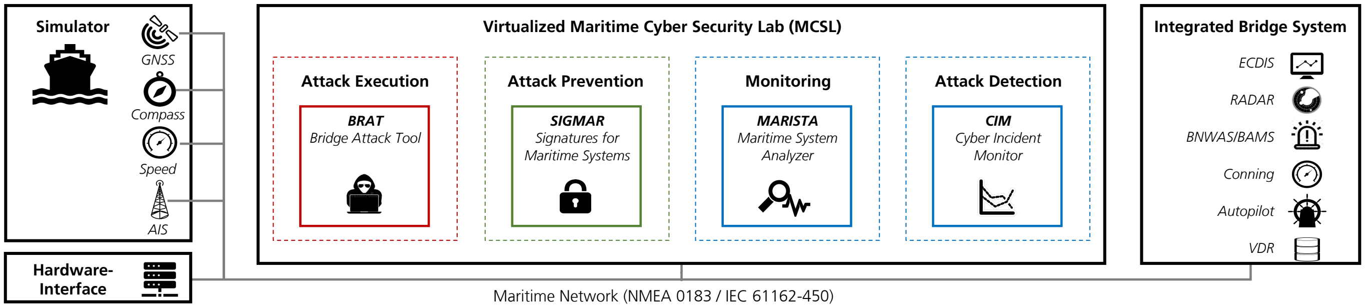


Fig. 1. Conceptual overview of virtualized, network-based, real-time Maritime Cyber Security Lab (MCSL), its connections to the simulator, a hardware interface, and the IBS, as well as exemplarily chosen asset components, serving as preliminary work for the MaCy testbed.

To address this challenge, we created *MaCy*, a *Ma*ritime *Cy*ber Security Lab that is equipped with real hardware components of modern IBSs, built according to the specifications of leading classification societies. We can either execute real cyber attacks or simulate them realistically in order to examine their impact on the operational safety and set up training scenarios for cyber security. By incorporating real hardware, the laboratory enables researchers and maritime industry professionals alike to simulate cyber attacks and to evaluate their effects in a controlled environment. It allows to develop, test, and assess the effectiveness of different cyber security measures, e.g., those to comply with IACS and IMO requirements on Maritime Cyber Risk Management in SMS [9].

Additionally, the laboratory can be leveraged to showcase the impact of cyber attacks and to increase the awareness of existing cyber threats among maritime stakeholders and ship personnel. Through practical exercises and scenarios, their cyber security skills can be further developed and trained and individuals can be guided on how to effectively behave in the case of a cyber incident.

The contributions of this paper can be summarized as follows. First, we give an overview of existing maritime security testbeds including our own preliminary work in Sec. II. Then, we motivate the goals of the MaCy project and introduce details on the laboratory in Sec. III. Finally, we provide a brief outlook on future research demands in Sec. IV

II. Maritime Security Testbeds

Due to the unique systems distributed across a vessel and combined in the IBS, specialized security testbeds with a dedicated computing and communication infrastructure are necessary. The task of such testbeds is to replicate the real systems on board ships as realistically as possible in order to serve as a scientific platform for security experiments and research in a controlled, safe environment and have the potential to be ultimately extended to so-called cyber ranges [7], [16].

Although the benefits of testbeds for research, development, and testing are long known from related domains, such as industrial control systems [17], there are generally only very few maritime testbeds, as a literature review with a focus on Integrated Navigation System (INS) shows [16]. The 16 publications found in the period from 2010 to 2020 result in only two testbeds that primarily address safe navigation and International Regulations for Preventing Collisions at Sea (COLREGs), but do not consider any security aspects. Only in recent years, real ship testbeds designed for cyber security purposes have emerged. These testbeds will be briefly presented in the following. First, the focus will lie on the authors' own preliminary work (Sec. II-A). Afterward, directly related testbeds will be discussed (Sec. II-B).

A. Maritime Cyber Security Lab

On the basis of the maritime simulator *Bridge Command* [18], we previously developed the virtualized *Maritime Cyber Security Lab (MCSL)*, a testing environment that enables the simulation and analysis of maritime cyber attacks and their impacts [19]. A conceptual overview of this environment is visualized in Fig. 1. Bridge Command [18] is an interactive open-source ship simulator with a graphical user interface, which is increasingly used for scientific purposes, e.g., [20], [21]. This simulator supplies various sensor data from a ship's sensors, such as Global Navigation Satellite System (GNSS) or Automatic Identification System (AIS) information, and has been extended as shown in Fig. 1 in such a way that the generated data is transmitted in a standard-compliant manner to an external Electronic Chart Display and Information System (ECDIS) instance via a virtualized on-board network.

Therefore, the data is converted into NMEA 0183 sentences and delivered over a "Lightweight Ethernet" (LWE), i.e., IEC 61162-450 [22] messages via conventional Ethernet, as common for IBSs [6], [23]. The use of standard-compliant networking and the real-time operability of the environment also allows external devices such as a GPS sensor to be integrated into MCSL via a hardware interface. The IBS functionalities, ECDIS and radar, are essentially provided by *OpenCPN* [24], an open-source chart plotter. Route information generated by users in OpenCPN can then be transmitted over the network to an autopilot extension in the simulator, so that there is bi-directional data traffic in the maritime network, to which the actual MCSL with its modules connects, cf. Fig. 1. These modules include:

- The BRidge Attack Tool (BRAT) [25], an offensive security module which facilitates internal network attacks and the evaluation of cyber attack countermeasures. BRAT is extended by the Radar Attack Tool (RAT) [5] to execute targeted network attacks against navigation radar systems.
- Two cryptography-based approaches for the retrofitting of authentication for the protection of data communication

in maritime systems, which were prototypically implemented and evaluated with SIGnatures for MARitime systems (SIGMAR) [26] or MARitime multi-Message Authentication Code (MARMAC) [27], serve as defensive security modules.

- The module MARItime SysTem Analyzer (MARISTA) is developed for the purpose of continuous monitoring as the basis for detecting attempts to compromise the maritime system and ongoing cyber attacks. It also allows the processing and visualization of network traffic, e.g., to identify existing communication patterns and to "learn" the normal behavior of the system.
- Cyber Incident Monitor (CIM) [28] is a detection framework that contains a multivariate Intrusion Detection System (IDS) and operates protocol-, topology-, and content-based to detect suspicious network behavior and alerts bridge crews in case of attack indication. Moreover, CIM offers an ergonomically designed Human Machine Interface (HMI), tailored for guiding nautical operators to respond adequately in the event of a cyber attack.

B. *Related Testbeds*

Driven by the need for maritime cybersecurity, more related ship testbeds have recently emerged. These testbeds use simulator-based environments (such as MCSL) or are supported by maritime hardware.

Simulative testbeds often provide a cost-effective and flexible solution but introduce a certain level of abstraction, influencing the quality of the respective simulation. In this context, Visky et al. [29] present a cyber environment for research and MET purposes based on a commercial navigational simulator provided by Transas. In contrast, both, the *Maritime Cyber Security Testbed (MaCySTe)* [21], [30] and the *XLab-UUV* [31] for simulating large Unmanned Underwater Vehicles (UUVs), build on open-source software, namely Bridge Command and OpenCPN, similar to MCSL (cf. Sec. II-A). As a result, portable virtualization of testbeds for flexible research and experimentation is enabled.

With their *Grace Maritime Cyber Testbed System* [32], Fathom5 provides various commercial hardware modules that are very close to real ship systems and are designed for security investigations as well as practical cyber war gaming. The module portfolio ranges from steering and propulsion systems over ballast water systems to navigation modules and includes Information Technology (IT) as well as many Operational Technology (OT) components. Furthermore, especially to be emphasized among the hardware-centric testbeds, is the *Cyber-SHIP Lab* [33], which combines the physical and digital assets of IBSs. As it offers multiple configurations of the IT and OT devices to represent differently equipped vessels, it provides a valuable cyber security research and education platform with a broad scope from penetration testing to MET.

III. Approach and Project's Goal

This section highlights the opportunities of the MaCy project with respect to launching cyber attacks and analyzing their impact as well as the design of cyber security scenarios for MET, so that both can support the development of security measures that improve the safe operation of a maritime vessel. To begin with, we bring maritime cyber threats that can be found in practice into focus (Sec. III-A), motivating MaCy's focus on the human factor (Sec. III-B). Then, we derive the project goal from this and introduce the components of the laboratory (Sec. III-C), before we subsequently present the attack and training scenarios enabled by it (Sec. III-D).

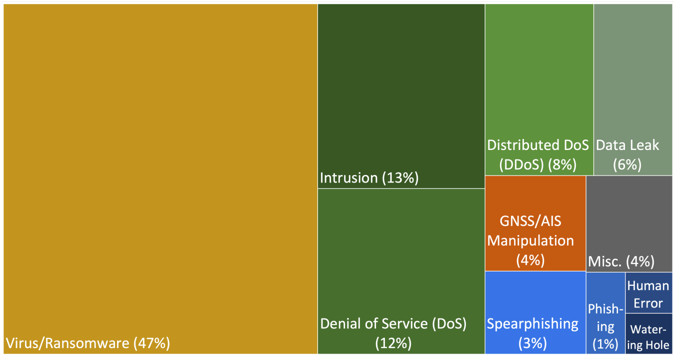
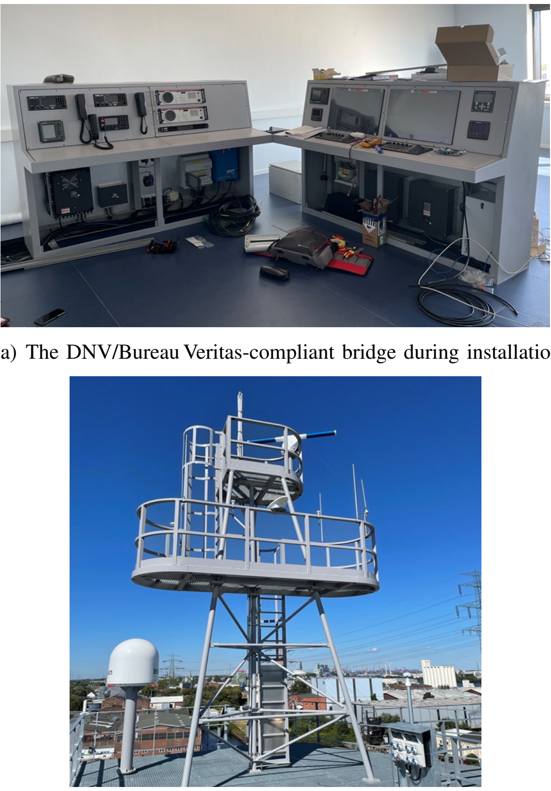


Fig. 2. Percent distribution of the 364 reported cyber incidents in the ADMIRAL database [34] over the total period of coverage (1980-2023, retrieved on 2023-06-20). Note that the types of incidents can be grouped as follows: The green shades include incidents that are alleged to result from Internet-based attacks on exposed ICT or even OT services, red are attacks on GNSS and AIS, while the blue shades represent incidents related to human factor. The bulk of incidents (yellow) result from malware threats.

A. *Insights from Maritime Practice*

While it is recommended [35] or sometimes even mandatory [36] to report cyber incidents at sea to external authorities, there is no universal obligation to do so. Therefore, only a few incidents are likely to become public and the number of unreported incidents is expected to be high. Nevertheless, insights into practice are provided by reports from consulting companies, e.g., [37], the increasing demand of maritime companies for security experts, which is reflected in job advertisements, several scientific papers on this subject [38]–[40], or the French Maritime Computer Emergency Response Team (M-CERT) initiative with systematic recording of reported on the Internet [34]. All these sources confirm the trend of a rapid and continuous increase of cyber incidents in recent years.

According to M-CERT's Advanced Database of Maritime cyber Incidents Released for Literature (ADMIRAL), most of the incidents originate from malware (*Virus/Ransomware* with 47 %) – predominantly non-targeted like the famous NotPetya incident, which hit Maersk severely in 2017 [2] – and conventional cyber attacks, presumably from the Internet (with roughly 39 %). The latter category of cyber incidents results from the aggregation of *Data Leak* with 6 %, (distributed) *Denial of Service (DoS)* attacks with 20 %, and *Intrusion* with 13 %, cf. Fig. 2. This is in line with the findings of Meland et al. [39], who see the cause of incidents in 78 % of the cases in exposed ICT or OT We can assume that a large proportion of malware incidents can be attributed to exposed services, hit by untargeted malware.



(a) The DNV/Bureau Veritas-compliant bridge during installation.

(b) Antenna platform on the roof of the building.

Fig. 3. Overview of the MaCy laboratory at the Fraunhofer CML building in Hamburg, Germany.

Whereas the malware and Internet attacks that make up the gross are typically not targeted against maritime assets in particular, especially ships, the category *GNSS/AIS Manipulation* at 4 % contains highly targeted and more sophisticated attacks against a ship's sensors and actuators or the IBS itself. Leveraging BRAT [25] and adopting it to the MaCy environment, we investigate this type of threat in the project, similarly as also conducted in the related testbeds presented in Sec. II-B. The RAT [5], currently designed for the Navico BR24 radar protocol, will also be adapted and applied in the project to address cyber attacks against maritime radar, e.g., [30], as well.

In addition to the above threats, there are *Other Delicacies from the Cuisine of Maritime Cyber Attacks* that are rarely considered in maritime cyber security testbeds, namely attacks exploiting the human factor. Social engineering, which targets the human factor, is a common attack technique often used as the first step in a complex kill chain. According to the popular MITRE ATT&CK framework [41], an extensive knowledge base of adversary tactics and techniques, it is predominantly applied in the reconnaissance and the initial access phase. Social engineering includes information gathering, e.g., from social media, water-holing attacks, impersonation, and in particular the widespread *phishing* and spear-phishing attacks. Other threats result from human error or deliberate malicious action. However, because other attack techniques usually follow within the kill chain *after* they took advantage of the human factor, many incidents are usually assigned to other categories. For instance, this would be the case if a careless user is responsible for the infection with malware by inserting a corrupted medium or misconfigures a firewall so that the exposure of an internal system service can subsequently be exploited for a DoS attack. As a consequence, it only accounts for a small proportion of 6 % in the ADMIRAL database, and the analysis by Schwarze et al. [38] only comes to 16 % of the cyber incidents under consideration, albeit with an upward trend. Nevertheless, the human factor and its impacts must not be neglected in security testbeds.

B. *Focussing on the Human Factor*

Because humans will remain on board ships for decades to come, yet constitute a substantial possible attack surface, it is essential for cyber protection at sea to consider this factor. Hence, it is a goal of MaCy to integrate the human into the security laboratories as well. This way, on the one hand, we can foster awareness of cyber threats, design special cyber MET, and put it into practice. On the other hand, it also offers valuable opportunities for scientific analysis. For example, the human detectability or stealthiness of cyber attacks can be explored and their impact evaluated, which is particularly insightful for maritime-specific deceptive attacks. In addition, conducting specialized MET in a realistic environment offers the opportunity for security scientists to work together with nautical professionals and collect valuable feedback directly, which helps to enhance digital auxiliary tools. This allows to jointly develop cyber response measures, define adequate recommendations for action in the event of a cyber attack, and to investigate their effectiveness.

C. *MaCy Components & Architecture*

To achieve the goals of human integration into the security laboratory, MaCy is replicating an actual ship bridge. Representative components were selected, installed, and commissioned in the laboratory. An overview of MaCy's hardware equipment is shown in Fig. 3. The aforementioned bridge can be seen in Fig. 3(a). This consists of a Furuno-manufactured Radar and ECDIS and radios for VHF and MF/HF, as well as NAVigational TEleX (NAVTEX) equipment. Furthermore, the bridge is equipped with devices for GNSS, AIS, and satellite communication (SatCom), as well as a satellite compass. Just as on an actual ship, there is also a Voyage Data Recorder (VDR), which collects the accruing data. In addition, there is a platform on the roof of the building with the corresponding antennas, always providing the laboratory with real-time data, cf. Fig. 3(b). All components are connected within the IBS network, outlined in its (default) network architecture in Fig. 4.

By using real hardware, a more holistic simulation of cyber incidents is possible. Additionally, users and their human errors can be addressed more effectively than with a virtual laboratory, which is the main concern of the part of MaCy presented here. Other projects that utilize hardware that can be found on an actual ship are the *Grace System* [32] and *Cyber-SHIP* [33], as mentioned in Sec. II-B. However, MaCy's antenna platform with its receivers provides unique capabilities with respect to the analysis of real-world attacks from the domain of Cyber and ElectroMagnetic Activities (CEMA),

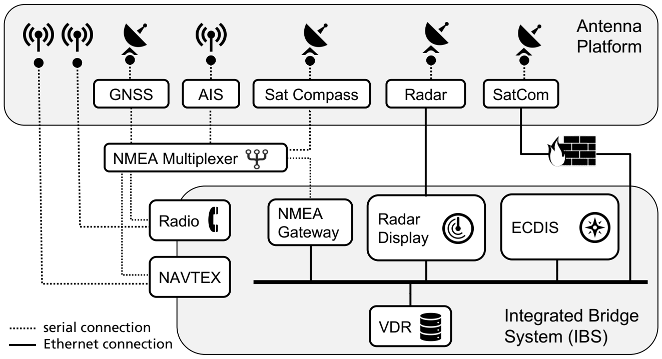


Fig. 4. Schematic overview of the MaCy's hardware components and its default network architecture connecting the antenna platform (Fig. 3(b)) with the IBS (Fig. 3(a)).

e.g., VHF jamming, AIS manipulation [42], or GNSS spoofing [43]. In MaCy, the modules of our previously developed virtualized MCSL (cf. Sec. II-A) are now combined with real hardware, whereby a more complex and realistic environment is created. Consequently, cyber attacks from practice can be validated and the quality of training the ship's personnel can be improved significantly.

D. Attack Scenarios & Use Cases

Looking at the illustrated network architecture of MaCy in Fig. 4, this represents the default and IMO-compliant configuration that can be changed flexibly. This allows for the assessment of different architectures regarding resilience against cyber attacks, e.g., network segmentation according to IEC 61162-460 [44]. However, this default configuration can be changed deliberately and temporarily in order to simulate realistic attack vectors, which in practice enable an external attacker to gain access and cause harm to the system. Possible scenarios that are examined in the project also include, for example, human misconfiguration, e.g., firewall configuration errors with unintentional exposing of devices to the Internet. It is worth noting that according to the Open Web Application Security Project (OWASP) Top Ten [45] of most critical security risks in the general context of ICT, security misconfiguration is in fifth place (A05:2021). Further scenarios are the deliberate bridging of network segments as well as a compromised IoT device that is added to the network for convenience reasons, e.g., to transmit navigational status information to the shipping company for the purpose of remote monitoring of cargo. Particularly the latter scenario reflects a modification of the network structure, which is not compliant with the IMO guidelines but can often be found in practice. For this, the modifiable network structure provided by MaCy enables the reproduction of the vulnerabilities they cause and how to remedy them. Building on these network-based attack vectors, further movements can then be made along the kill chain, using BRAT and RAT (cf. Sec. II-A) with their portfolio of man-in-the-middle and on-the-side attacks.

In addition to the aforementioned network-based attacks, other human-centric attack and training scenarios are intended. This includes both non-targeted off-the-shelf phishing campaigns that lead to a system infected with ransomware, and also targeted attacks, such as spear-phishing, which specifically attacks ships and their crew members. According to the ADMIRAL database, most of the maritime cyber security incidents are of the type *Virus/Ransomware* [34], [40]. This kind of incident is very likely often caused by human error or negligence since the malware is typically delivered via emails or a drive-by download attack through malicious links [39]. Another attack vector that takes advantage of the human factor and is responsible for an increasing number of cyber incidents is a USB flash drive that can deliver malicious software when connected to the USB port of the VDR [46]. To train maritime personnel in this regard, phishing or malware infection can be simulated within the laboratory.

Besides the exploration of attack vectors and the creation of proof-of-concept demonstrations and MET scenarios, further use cases are in the field of visual assistance systems. Such systems could provide the ship operator with vivid feedback on, for example, anomalies in network traffic, thereby generating increased alertness to cyber incidents that require the crew to take specific actions. The prototypical CIM of MCSL (cf. Sec. II-A) will therefore be adapted and continuously extended within the MaCy project.

IV. Discussion & Outlook

The unique feature of MaCy is the use of a real standard-compliant ship's bridge for a security lab. In addition, the project shifts from internal attacks (assumed in MCSL) to the explicit consideration and analysis of external attack surfaces, with a focus on vectors attributed to the human factor, but also those beyond.

The knowledge of such attack vectors could be further enhanced in future work through a honeypot function of the laboratory. Honeypots are systems serving as decoys to lure potential adversaries into attacking and breaking their security [47]. Their main purpose is to attract malicious activity, thus distracting from critical systems, and to generate early warnings. However, honeypots are not very common in the maritime sector so far [48] and their development is the subject of current research [47]. MaCy provides the opportunity to serve as a highly realistic honeypot system and, thus, enables the collection of information about attackers, their tactics, and techniques. This information is invaluable for security research. It can also be fused with information from other sources, such as publicly available social media data, for maritime Cyber Threat Intelligence (CTI) [48] to gain intelligence on adversaries and on who to attribute incidents to. This is needed, e.g., for maritime cyber insurance [12].

V. Conclusion

Motivated by an analysis of cyber incidents in maritime practice and their growing occurrence, this paper highlighted the urgent need for security in the maritime domain. Adequate protection of ships first requires a better knowledge of vulnerabilities, attack surfaces, and potential impacts of attacks. Derived from this insight, effective security measures can then be developed. In the ongoing MaCy project, a realistic security testbed is being realized for this purpose. Among MaCy's different facets, mainly the human factor was addressed in this paper, and resulting cyber threats were presented. For this purpose, an overview of practical attack vectors exploiting the human factor was given and the prospects of MaCy with respect to the simulation of realistic cyber incidents were shown to improve the cyber security skills of maritime personnel as well as the operation of ocean-going vessels.

ACKNOWLEDGMENTS

This work is part of the research project *Maritime Cyber Security Lab (MaCy)* and funded under the umbrella of Fraunhofer's innovation impulse *Smart Ocean*. The authors are responsible for the contents of this publication. Furthermore, the authors would like to thank Jan Solle and Antoine Saillard for their continuous technical support.

REFERENCES

[1] G. C. Kessler and S. D. Shepard, *Maritime Cybersecurity: A Guide for Leaders and Managers*, 2nd ed. Daytona Beach, FL, USA: independently published, 2022.

[2] SAFETY4SEAS, "Maersk line: Surviving from a cyber attack," The Editorial Team, May 2018, https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/ (accessed 2023-07-21).

[3] K. Tam and K. Jones, "Factors affecting cyber risk in maritime," in *Proc. of Cyber SA*, Oxford, United Kingdom, 2019.

[4] M. Caprolu, R. D. Pietro, S. Raponi, S. Sciancalepore, and P. Tedeschi, "Vessels Cybersecurity: Issues, Challenges, and the Road Ahead," *IEEE Commun. Mag.*, vol. 58, no. 6, 2020.

[5] K. Wolsing, A. Saillard, J. Bauer, E. Wagner, C. van Sloun, I. B. Fink, M. Schmidt, K. Wehrle, and M. Henze, "Network Attacks Against Marine Radar Systems: A Taxonomy, Simulation Environment, and Dataset," in *Proc. of LCN*, Edmonton, AB, Canada, 2022.

[6] M. S. Lund, J. E. Gulland, O. S. Hareide, Ø. Jøsok, and K. O. C. Weum, "Integrity of integrated navigation systems," in *Proc. of CNS*, Beijing, China, 2018.

[7] G. Potamos, A. Peratikou, and S. Stavrou, "Towards a Maritime Cyber Range training environment," in *Proc. of CSR*, Rhodes, Greece, 2021.

[8] United Nations Conference on Trade and Development (UNCTAD), "Review of Maritime Transport 2022," New York, NY, USA, 2022.

[9] IMO MSC.428(98), "Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems," June 2017.

[10] IACS-UR-E26, "E26 – Cyber resilience of ships," IACS Req., Apr. 2022.

[11] IACS-UR-E27, "E27 – Cyber resilience of on-board systems and equipment," IACS Req., Apr. 2022.

[12] L. Drazovich and S. Wetzel, "Cyber Insurance in the Maritime Transportation System," in *Proc. of MarCaS*, Daytona Beach, FL USA, 2023.

[13] C. Wienberg, "Maersk's CEO Can't Imagine Self-Sailing Box Ships in His Lifetime," https://www.bloomberg.com/news/articles/2018-02-15/maersk-ceo-can-t-imagine-self-sailing-box-ships-in-his-lifetime (accessed 2023-07-12).

[14] D. Heering, O. M. Maennel, and A. N. Venables, "Shortcomings in Cybersecurity Education for Seafarers," in *Proc. of MARTECH*, Lisbon, Portugal, 2020.

[15] R. Cichocki, "State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine," *TransNav*, vol. 17, no. 3, 2023.

[16] A. Oruc, V. Gkioulos, and S. Katsikas, "Towards a cyber-physical range for the integrated navigation system (ins)," *Journal of Marine Science and Engineering*, vol. 10, no. 1, 2022.

[17] M. Conti, D. Donadel, and F. Turrin, "A Survey on Industrial Control System Testbeds and Datasets for Security Research," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, 2021.

[18] Bridge Command, "An interactive 3d ship & radar simulator," https://www.bridgecommand.co.uk (accessed 2023-06-06).

[19] M. von Rechenberg, M. Schmidt, C. Hemminghaus, J. Bauer, and E. Padilla, "When a BRAT fools your bridge: A Cyber Security Test Environment for Integrated Bridge Systems," in *LCN Demos (virt.)*, Edmonton, AB, Canada, 2021. [Online]. Available: https://www.ieeelcn.org/prior/LCN46/lcn46demos/Demo_8_1570761147.pdf

[20] A. Amro, A. Oruc, V. Gkioulos, and S. Katsikas, "Navigation Data Anomaly Analysis and Detection," *Information*, vol. 13, no. 3, 2022.

[21] G. Longo, A. Orlich, S. Musante, A. Merlo, and E. Russo, "MaCySTe: A virtual testbed for maritime cybersecurity," *SoftwareX*, vol. 23, 2023.

[22] IEC 61162-450:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 450: Multiple talkers and multiple listeners – Ethernet interconnection," International Electrotechnical Commission (IEC), 2018.

[23] Ø. J. Rødseth, M. J. Christensen, and K. Lee, "Design challenges and decisions for a new ship data network," in *Proc. of the Int. Symposium Information on Ships (ISIS 2011)*, Hamburg, Germany, 2011.

[24] OpenCPN.org, "OpenCPN Chart Plotter Navigation," https://opencpn.org (accessed 2023-06-06).

[25] C. Hemminghaus, J. Bauer, and E. Padilla, "BRAT: A BRidge Attack Tool for cyber security assessments of maritime systems," *TransNav*, vol. 15, 2021.

[26] C. Hemminghaus, J. Bauer, and K. Wolsing, "SIGMAR: Ensuring Integrity and Authenticity of Maritime Systems using Digital Signatures," in *Proc. of ISNCC-TSP (virt.)*, Dubai, UAE, 2021.

[27] L. Ruhland, M. Schmidt, J. Bauer, and E. Padilla, "Keeping the Baddies Out and the Bridge Calm: Embedded Authentication for Maritime Networks," in *Proc. of ISNCC-TSP (virt.)*, Shenzhen, China, 2022.

[28] M. von Rechenberg, N. Rößler, M. Schmidt, K. Wolsing, F. Motz, M. Bergmann, E. Padilla, and J. Bauer, "Guiding Ship Navigators through the Heavy Seas of Cyberattacks," in *Proc. of MARESEC*, Bremerhaven, Germany, 2022.

[29] G. Visky, A. Lavrenovs, E. Orye, D. Heering, and K. Tam, "Multi-Purpose Cyber Environment for Maritime Sector," in *Proc. of ICCWS*, Albany, NY, USA, 2022.

[30] G. Longo, A. Merlo, A. Armando, and E. Russo, "Electronic Attacks as a Cyber False Flag Against Maritime Radars Systems," in *Proc. of MarCaS*, Daytona Beach, FL USA, 2023.

[31] K. Wolsing, A. Saillard, E. Padilla, and J. Bauer, "XLab-UUV – A Virtual Testbed for Extra-Large Uncrewed Underwater Vehicles," in *Proc. of MarCaS*, Daytona Beach, FL USA, 2023.

[32] Fathom5, "Grace Maritime Cyber Testbed System," https://www.fathom5.co/grace (accessed 2023-06-06).

[33] K. Tam, K. Forshaw, and K. Jones, "Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities," in *Proc. of ICMET Oman*, Muscat, Oman, 2019.

[34] Maritime Computer Emergency Response Team (M-CERT), "ADMIRAL," 2023. [Online]. Available: https://gitlab.com/m-cert/admiral

[35] GOV.UK, "Guidance – Where to Report a Cyber Incident," https://www.gov.uk/guidance/where-to-report-a-cyber-incident (accessed 2023-07-12).

[36] Sjøfartsdirektoratet Norwegian Maritime Authority, "RSV 18-2022 - Reporting cyber incidents," Aug. 2022, Journal No. 2022/37521.

[37] Pen Test Partners, "Maritime Cyber Security," https://www.pentestpartners.com/maritime-cyber-security/ (accessed 2023-07-12).

[38] M. Schwarz, M. Marx, and H. Federrath, "A structured analysis of information security incidents in the maritime sector," 2021, arXiv 2112.06545.

[39] P. Meland, K. Bernsmed, E. Wille, Ø. J. Rødseth, and D. Nesheim, "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav*, vol. 15, no. 3, 2021.

[40] G. Potamos, S. Theodoulou, E. Stavrou, and S. Stavrou, "Building maritime cybersecurity capacity against ransomware attacks," in *Proc. of Cyber Science*, Cardiff, Wales, 2022.

[41] MITRE Corperation, "ATT&CK Matrix for Enterprise," https://attack.mitre.org (accessed 2023-07-12).

[42] M. Balduzzi, A. Pasta, and K. Wilhoit, "A Security Evaluation of AIS Automated Identification System," in *Proc. of ACSAC*, New Orleans, LA, USA, 2014.

[43] J. Bhatti and T. E. Humphreys, "Hostile Control of Ships Via False GPS Signals: Demonstration and Detection," *Journal of the Institute of Navigation*, vol. 64, no. 1, 2017.

[44] IEC 61162-460:2018, "Maritime navigation and radiocommunication equipment and systems – Digital interfaces – Part 460: Multiple talkers and multiple listeners – Ethernet interconnection – Safety and security," 2018.

[45] Open Web Application Security Project (OWASP), "OWASP Top Ten," website, Oct. 2021. [Online]. Available: https://owasp.org/www-project-top-ten/

[46] R. Hopcraft, A. V. Harish, K. Tam, and K. Jones, "Raising the standard of maritime voyage data recorder security," *Journal of Marine Science and Engineering*, vol. 11, no. 2, 2023.

[47] J. Pijpker and S. McCombie, "A Ship Honeynet to Gather Cyber Threat Intelligence for the Maritime Sector," in *Proc. of MarCaS*, Daytona Beach, FL USA, 2023.

[48] N. Pitropakis, M. Logothetis, G. Andrienko, J. Stefanatos, E. Karapistoli, and C. Lambrinoudakis, "Towards the creation of a threat intelligence framework for maritime infrastructures," in *Proc. of CyberICPS*, Luxembourg City, Luxembourg, 2020, pp. 53–68.