Cyber-SHIP: Developing Next Generation Maritime Cyber Research Capabilities

Kimberly Tam, Kevin Forshaw, Kevin D Jones
University of Plymouth, Plymouth, UK
kimberly.tam@plymouth.ac.uk, kevin.forshaw@pymouth.ac.uk,
kevin.jones@plymouth.ac.uk

Synopsis

As a growing global threat, cyber-attacks can cost millions of dollars or endanger national stability and human lives. While relatively well understood in most sectors, it is becoming clear that, although the maritime sector is becoming more digitally advanced (e.g., autonomy), it is not well protected against cyber or cyber-physical attacks and accidents. To help improve sector-wide safety and resiliency, the University of Plymouth (UoP) is creating a specialised maritime-cyber lab, which combines maritime technology and traditional cyber-security labs. This is in response to the lack of research and mitigation capabilities and will create a new resource capability for academia, government, and industry research into maritime cybersecurity risks and threats. These lab capabilities will also enhance existing maritime-cyber capabilities across the world, including risk assessment frameworks, cybersecurity ranges/labs, ship simulators, mariner training programmes, autonomous ships, etc. The goal of this paper is to explain the need for next generation maritime-cyber research capabilities, and demonstrate how something like the proposed Cyber-SHIP Lab (Hardware, Software, Information and Protections) will help industry, government, and academia understand and mitigate cyber threats in the maritime sector. The authors believe a next generation cyber-secure lab should host a range of real, non-simulated, maritime systems. With multiple configurations to mirror existing bridge system set-ups, the technology can be studied for individual system weakness as well as the system-of-systems vulnerabilities. Such as lab would support a range of research that cannot be achieved with simulators alone and help support the next generation of cyber-secure marine systems.

Keywords — Maritime, cybersecurity, research

1. Introduction

As of 2019, the global implementation of robust maritime cyber-security policy is essentially non-existent. One of the first analysis of the sector's maritime-cyber security capabilities was in 2013 when the EU reported that there was an international lack of maritime cyber-security awareness, and that existing protocols catered to purely physical aspects of security and safety (ENSIA 2011). Since then several generic cyber-hygiene articles have been published to address rising concern in companies and international organisations like the International Maritime Organization (IMO 2018). However, generic cyber-hygiene is insufficient for robust security. Moreover, existing cyber solutions fit poorly with the maritime-specific issues and the growth of technology continues to introduce new risks. With this growing threat, it is clear that there is a lack of the capability to fully analyse and mitigate the growing number of maritime-cyber risks.

One of the challenges to fully understanding and mitigating maritime cyber risks is the bespoke nature of the equipment. The range of ship types, sizes, and ages in the global fleet mean that the diversity of equipment configuration from ship-to-ship can vary greatly. This makes maritime cyber more difficult to understand, because common analysis and risk assessment tools cannot just be re-applied to a new context. As these systems are also connected in unique configurations, with both Information Technology and Operational Technology (IT/OT) working in the same environment, understanding and securing the system-of-systems is also difficult. Just as security is different between rail and air, even though both transportation sectors rely on similar systems, maritime needs its own dedicated research capabilities. One unique aspect of maritime cyber security is the blend of IT and OT. The bulk of security efforts is normally focussed on IT, but as

 http://doi.org/10.24868/icmet.oman.2019.005

there are many physical operations in maritime (e.g., propulsion, cargo movement) OT needs to be considered as well. This is why the University of Plymouth is creating research capabilities to consider the physical aspects as well as the digital, hence a lab that is accurate to the hardware level and not a simulation or emulation. Unfortunately, it is also not easy for those outside the maritime community to contribute to maritime cyber research. Data is difficult to acquire, and the equipment necessary is much more expensive than more traditional security labs. Given this, the problems the University of Plymouth aims to address by creating the Cyber-SHIP lab are:

- Risk assessment/management of maritime cyber threats (cyber, and cyber-physical)
- Find/fix vulnerabilities from hardware, software, and human-computer interactions
- Work with stakeholders to improve resiliency and cyber-safety of individual systems
- Analyse the cybersecurity of a collection of bridge systems, connected in real world configurations
- Discover maritime-cyber threats that can be used to educate future mariners and Navies
- Determine future cyber threats to assets, economy, human lives, and environment.

The rest of the paper is as follows, Section 2 describes existing tools and practices (e.g., why simulations are not sufficient for maritime-cyber research), evolving technology trends and state-level threats. Section 3 uses the background to explain why the maritime sector needs next generation maritime-cyber research capabilities, and how the University of Plymouth is creating that capability. Section 4 describes future work to be done, to work with other organisations to understand and reduce cybersecurity threats in maritime and Section 5 concludes the article.

2. Background

Many organisations rely on maritime operations. In terms of volume, maritime trade and passengers accounts for 90% of all worldwide transportation (ICS 2018). Other important functions include military activity (i.e., Navy). Both of which are essential to a modern countries' national infrastructure, safety, and economy. This section looks at current tools and practices for researching maritime-cyber threats and training individuals to mitigate the threats. Next, it will discuss the current technological and cyber-risks trends along with the human element of cyber-threats. Once these have been, established Section 3 will discuss next generation research and training capabilities to meet these growing maritime-cyber threats.

	Simulation	Emulation	Live Systems
Positive	• Quick to develop • Cheaper • Training tools	• More realistic • Repeatable Experiments	• Entierly realistic for training & research
Negative	• Limited by conceptual model	• Costly • Not entirely realistic	• Real world consequences can be costly

Table 1: Strengths & weaknesses of different approaches for maritime training and research

2.1 Existing Tools and Practices

Training and research facilities can be categorized by whether they primarily use simulation, emulation, or the in-situ systems used (see Table 1).

2.1.1 Simulations and Training

Many universities and organisations use sophisticated simulators today with a focus on training. In technical terms, simulation is the replication of general system behaviours using a conceptual model. The benefit of simulators is that, when set up correctly, they provide near-real experiences for training without all the hazards of the real world. Currently the ratio of real world to simulation training is skewed toward more simulation time, mirroring aviation, which is about 1:30 to 1:15 real training to simulation time (Salman 201). However, simulators are limited to their programming and have made it difficult to simulate cyber-attacks for new cyber-aspects of training or maritime-cyber research (Moorthy et al. 2005). While simulators can be continuously made more realistic, the increased cost lowers the appeal of simulators for research purposes. Other purposes for simulations, such as the "digital twin", are relatively new and in-development, and will be discussed further in the following subsection.

2.1.2 Emulation and Cyber-Ranges

Globally there has been an increase in cyber-ranges, or cybersecurity labs, which are computer labs designed specifically to handle the research of dangerous software (e.g., viruses, malware). There are a number of these ranges/labs in several countries, commercially, academically, and for military purposes (Davis and Magrath 2013). Majority of these use simulation or emulation. Unlike the software simulation of a few system model behaviours, emulation replicates one system in another more faithfully. It has been found that emulation, and cyber-ranges that use emulation, tend to be more useful for training and research. That said the common downfall of emulation is that the added infrastructure and abilities cost more (Davis and Magrath 2013).

Additionally, for maritime, one downside of cyber-ranges is their almost exclusive view on information technology, with little to no focus on operational technology. While emulation can be semi-realistic, it cannot achieve total realism. This is troublesome when connecting multiple systems together as they may not be able to communicate (e.g., not timing-accurate) (Griffin et al. 2002). A significant benefit of the Cyber-SHIP is it can study connected systems, as well as individual ones.

2.1.3 Real World (in-situ) Systems

To test real world systems (but not simulation or emulation), security-based penetration testing can be highly useful for research. Real systems also provide the most realistic training possible for learners. However, particularly in maritime, if a mistake is made with the real equipment, a lot of physical and technical damage could be caused (Allianz 2019; Lewis 2002). Ships could collide with sandbars and crucial shipping data can be leaked. This is why, traditionally, simulation has been used for structured human training and either simulation or emulation has been used for research. Conversely, pen-testing has mainly been used for quality assurance and information risk mitigation (Arkin et al. 2005; Calder and Watkins 2010).

The increase of cybersecurity threats in the digital age means that the maritime sector needs new research capabilities to maintain safety standards. This is why the authors propose a next generation maritime-cyber research capability, which combines cyber-ranges with real maritime equipment, specifically those found on a ship's bridge. This is to provide researchers with the benefits of real-world equipment, but adding safety and experiment capabilities with minimal, strategic, uses of emulation and simulation. This is also intended to start as a specialised facility catering to the maritime sector, a niche no one is currently filling in this way. Using real hardware and software in a cyber-secure lab environment will enable many research opportunities, leading to updated training (see Table 1).

2.2 Evolving Technology

With the arrival of the digital age, systems are becoming more sophisticated and more connected. A short summary of some key technological developments for the maritime sector is provided, as describing the future digital trends for maritime is meant to provide context to why next generation research capability is needed. References to more detailed research will be provided for those interested in further detail. Given these trends and the current capabilities, the authors illustrate how maritime-cyber threats will keep growing.

2.2.1 Digital Twin and Virtual Reality

The use of simulation in the maritime sector is shifting away from primarily training to other purposes. The digital twin concept (Tao, et al., 2018) uses simulation to re-create a real ship digitally to aid ship design, construction, and monitor performance. While this may have major advantages on researching efficiency and a ship's lifecycle, it is less relevant for cybersecurity. Augmented reality and fully virtual realities also use simulation (Tam & Jones 2019c). Unlike full virtual reality, augmented reality has both real and virtual elements. In maritime, this has been proposed to provide more information for local or remote crews to control ship systems (Baldauf and Procee 2014; Frydenberg et al. 2018). As this blends new technology with human-in-the-loop decisions and actions, the Cyber-SHIP lab would be one possible facility to study cyber vulnerabilities that could lead to false or malicious, information being provided to human crew and the potential outcomes from those kinds of attacks.

2.2.2 Internet-of-Things

The concept of the IoT (Internet-of-Things) is that many devices communicate significant amounts of data via the Internet. As that definition is broad, IoT networks can be massive. This is true of maritime devices as well. As computing power becomes cheaper and devices more useful and durable, more personal devices are being used and more ship/port specific devices are being connected (Cankar and Stanovik 2018; Ha et al. 2018; Pizzo et al. 2018; Tam and Jones 2019b). One of the strengths of the proposed Cyber-SHIP Lab, and the fact that it uses real systems, is its ability to study connected systems, either IoT or more traditional networks. This would be a new capability that previous simulation and emulation methods have not achieved, for this level of cyber-related research.

2.2.3 Autonomous

In some ways, autonomous ships and ports are built on top of IoT technology, as the autonomy requires more digital monitoring (e.g., more sensors), increasing the number of possible cyber vulnerabilities (Tam and Jones 2018). Therefore, again, analysing the communications between computing systems is critical for next generation research capabilities. The main difference between autonomous and IoT is that more than Internet-based networks may be used (Zolich et al. 2019). Unlike IoT, future research into autonomous ships and ports will have to study the cyber-physical threats more, as more of the devices connected will be used for physical operations as well (e.g., navigation, propulsion, cargo management) instead of primarily for monitoring and sharing data. Semi-autonomous technology may also use virtual reality, as described earlier in Section 2.2.1.

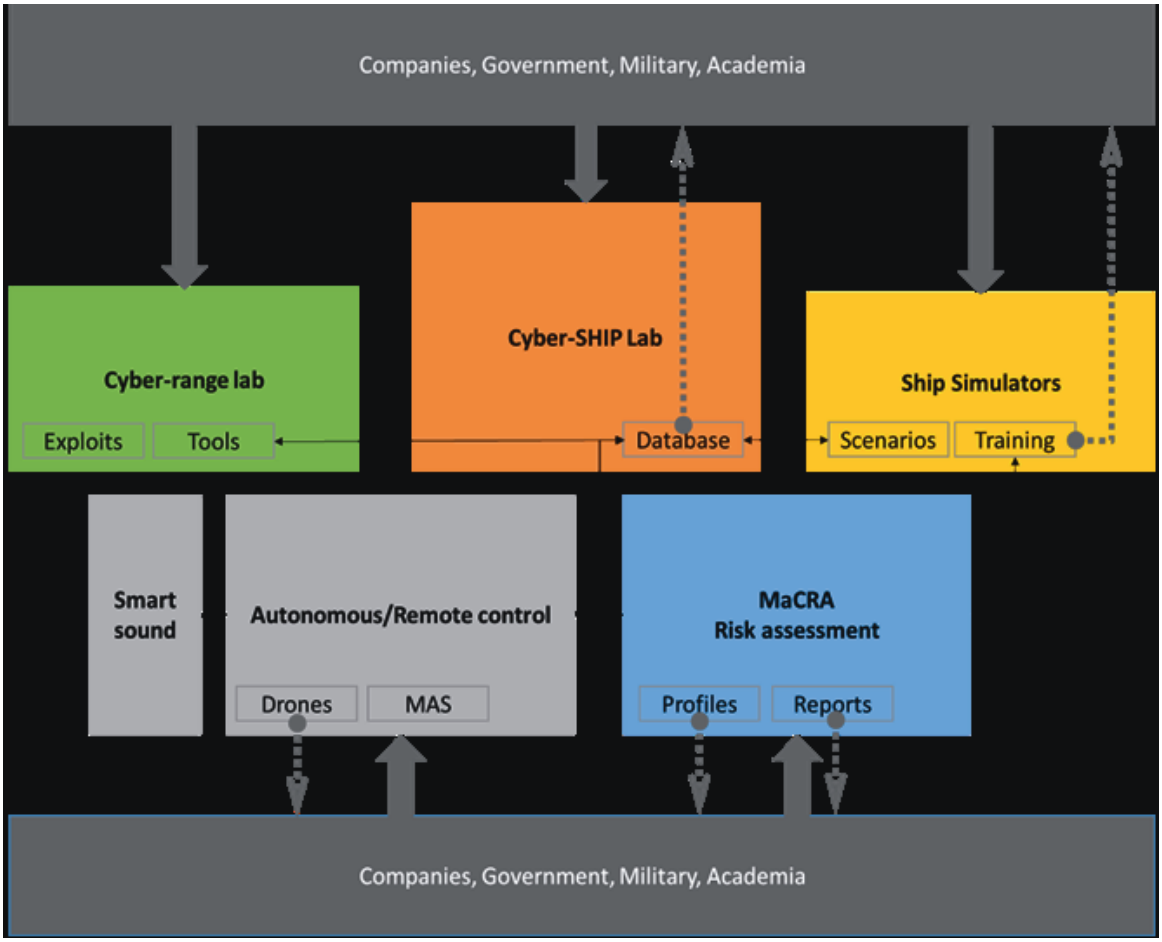

Figure 1: Overview of Research Capabilities with the proposed Cyber-SHIP Lab

2.2.4 IT/OT convergence

Lastly, there has been a trend of converging IT and OT, particularly in maritime. This follows the general trend observed in other topics of systems becoming more connected. IT/OT convergence, however, is a little different, as there are more operational system involved, increasing the number of cyber-physical vulnerabilities and threats possible (Man et al. 2018). As this and the other digital trends in this section show, maritime cyber threats are growing and evolving with technology itself and how the technology is used. Of the four digital trends presented, the OT aspect will likely require the most emulation when researching maritime cybersecurity of IT/OT systems.

As discussed in this paper, current research and teaching facilities would struggle to accommodate to these digital trends, as facilities are not set up to accommodate for multiple connected systems, especially IT and OT systems together.

2.3. Cyber Threats

The body of work on general cyber threats is vast; in contrast, maritime cyber threats are not as well defined. This section is not an exhaustive study, but instead discusses some of the most relevant studies relating to cyber threats in maritime across industry and military. Cyber-attacks can have many outcomes, cyber (e.g., data theft), physical (e.g., collision, real theft), financial (e.g. loss of customer data, delays in shipment) and more. Attacks can also be fast, with computers an attack can happen in less than a second, or be long lasting. For example, spying or loss of intellectual property data can affect short-term and long-term competitiveness of businesses and cause national security problems if leaks occurred during government or military espionage incidents (Choo 2011). There are also many types of human threats from pranksters to terrorists (BIMCO 2016; Tam and Jones, 2019b). In maritime most cyber-related incidences so far seem to have been accidental rather than attacks (Maersk 2017; Rajamanickam 2018); however, recent attack by state-actors have also shown that the military must be ready for a number of cyber-attacks on maritime vessels and infrastructure (C4ADS 2019; Climpanu 2019).

3. Next Generation Research Capabilities

Many rely on maritime operations across industry, military, and academia; therefore, there are many facilities for researching and teaching globally. Earlier sections have demonstrated (1) the rising cyber-security threat (2) digital age vulnerabilities and (3) the limitations of current capabilities. In this section the authors describe the current capabilities at the University of Plymouth with respect to maritime and cyber, and then describe the proposed Cyber-SHIP Lab as a next generation research capability for cybersecurity in maritime.

3.1 Current UoP Capabilities

This section does not describe the UoP simulators and cyber-range, as they are currently standard (see Section 2.1). This section discusses several unique maritime-cyber facilities at the university. This includes the Plymouth Smart Sound and Maritime Cyber Risk Assessment (MaCRA) framework and how they will work with Cyber-SHIP to provide new research capabilities together.

3.1.1 Smart Sound

Smart Sound Plymouth is a proving area for designing, testing and developing cutting-edge products and services for the advanced marine sector. Covering over 1,000km^2 of ocean off Plymouth Sound, the proving area's impressive variety of water depth, sea states and weather conditions is ideally suited for conducting sea trials, including sub-sea tests with access to offshore water depths of 75m. The University of Plymouth has partnered with the Marine Business Technology Centre (MBTC), and others, pooling a number of physical assets to aid technological development. For example, UoP is providing access to its unmanned surface vessels, shown in Figure 1. Smart Sound Plymouth is ideally suited for building and supporting the next generation of marine technologies. Since it is dangerous to do cyber-research in open waters, possibly affecting other ships, most of the dangerous research can be done in the Cyber-SHIP. Experiments that pass safety standards in the lab can then be repeated in the real, but safely controlled and fully instrumented (e.g., monitored), smart sound environment.

3.1.2 MaCRA

This maritime cyber risk assessment framework has been designed specifically to quantify and prioritise cyber risks in maritime. The MaCRA framework inputs data on system vulnerabilities, potential outcomes, as well as attacker abilities and target defences (Tam and Jones 2019b). It then outputs graphical or numerical risk profiles that can be customised to the analyst to answer specific or broad maritime-cyber risk queries (see Figure 2). Connecting MaCRA to the proposed lab would increase the framework's risk profile details, and help prioritize threat-mitigation research when analysing Cyber-SHIP bridge configurations.

3.2 New Cyber-SHIP Capabilities

This section describes the proposed lab in more high-level detail, as well as the aim of the lab. Once the next generation lab is established, future work will analyse the architecture in full detail.

3.2.1 Setup

The establishment of the Plymouth Cyber-SHIP (Software, Hardware, Information, and Protection) Lab would be a transformational step towards

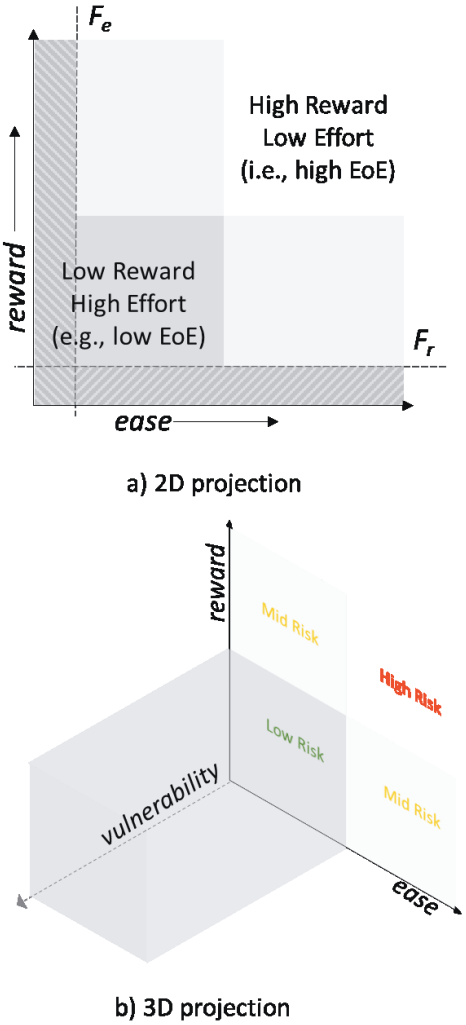

Figure 2: Risk Projections in MaCRA

developing a new research capability for maritime cyber-security. It would also add new capabilities to existing facilities (e.g., ship simulators, cyber-ranges, Smart Sound). The approach proposed in this article addresses a number of complex and interlinked issues affecting the maritime industry. Both technological and human behavioural aspects must be taken into account for effective mitigation of threats, as must with the huge variation in vessel types, which can be subjected to cyber-attacks in different ways for various motivations.

Understanding and addressing all of these parameters is the crux of the innovation in this approach. Providing a space where industry, military, and academia can pool together resources and research efforts would be beneficial toward increasing maritime cybersecurity across the sector. Moreover, as a non-competitor in the shipping market, an academic lab is also in a position to begin gathering anonymized data for further research ranging from secure military research, to public academic research in universities and organizations that do not have the means to generate this data. To do this, real bridge equipment will be gathered in a secure lab, where in-depth tools (e.g., pen-testing) can be used to discover and analyse cyber vulnerabilities from the hardware, to

software, and digital-human interactions. A secure lab would have traditional network protections to prevent damage to outside entities, as well unique capabilities such as a faraday cage or signal simulation to test spoofing and jamming, which can be damaging and is illegal outside a secure lab. Software tools will also be made for vulnerability and risk research and for running experiments.

The Cyber-SHIP Lab will assemble key equipment found on a ship's bridge to test resilience from a systems-of-systems perspective. As mentioned, one the downfalls of simulation and emulation is that, although individual systems can be re-created, it is difficult to then connect these modelled systems as most simulations and emulations are not timing-accurate down to the hardware level.

By connecting the real hardware together, with limited simulation and emulation used to interact with the system as a connected whole, the Cyber-SHIP would be capable of researching more than individual systems. This is important in the diverse IT/OT maritime environment, but particularly for ships, which connects a number of different systems. While the lab is unlikely to be able re-create every available bridge setup, based on international regulations (IMO 2003; IMO 2018), the lab should be configurable to most common setups. A variety of examples for each aspect of bridge equipment, in rack-based infrastructure, will allow rapid and complex configurations to aid experimentation as well as match a wide variety of real world setups.

As a shared capability, organisations across academia, government, military, and industry would also be able to provide, temporarily or in the long term, missing systems for their own research without needing to invest in their own lab.

3.2.2 New Cyber-SHIP Aims

Once assembled, the Cyber-SHIP lab will enable new cybersecurity research into individual systems and connected systems, from the hardware to human user level, enabling the development of mitigation measures both technically and for human factors perspective. The lab as it stands now will be developed and delivered in partnership with key partners including equipment manufacturers, solution developers, shipping and port operators, ship builders, classification agencies, government branches (e.g. transport, maritime incidents) and insurance companies. This is to ensure that a number of bridge configurations can be achieved with a single lab, and demonstrates the wide range of interests from different niches in the sector.

It is important to recognise that, although researching maritime cybersecurity is crucial, it is not currently an easy area of research. As maritime cyber data is scarce, commercially sensitive, or pertains to national security, and the equipment necessary to represent shipping environments is much more expensive than more traditional security labs, it may be overlooked as a research field. Providing a space where government industry and academia can pool resources and research efforts will be of significant benefit to all those involved with maritime. While this maritime-cyber lab aims to provide next generation research capabilities, it is not intended as a stand-alone solution. As seen in Figure 1, the Cyber-SHIP lab is meant to be integrated with other existing facilities. In this case, the lab is able to connect to other UoP facilities, including its cyber-range and ship's bridge simulator (Figures 3 and 4 respectively).

Figure 3: UoP cyber-range

Figure 4: UoP ship simulator (bottom)

A lab like this would also benefit from sharing data with risk assessment frameworks for maritime operations across the sector, and help facilities designated for the future of autonomous ships, including drones. Following this is a more in-depth discussion on future work regarding the Cyber-SHIP lab in isolation and with other existing capabilities in both maritime and cybersecurity.

4. Future Work and Limitations

The largest negative to the Cyber-SHIP Lab approach is the cost (see Table 1), both initial and updates. It is possible that, as systems update to become more cyber-secure and provide better forensic data (Tam and Jones, 2019a), this lab may be less useful in 20-30 years. However, without some next generation research capabilities, it would be difficult for systems to become sufficiently cyber secure fast enough to meet today's threats and those in the near future. This is the rationale behind Cyber-SHIP.

Once this facility has been established, future work can be done to layout the architecture in detail. In the future, this lab may branch out to include more systems as well (e.g., port). The lifecycle of the proposed lab should mirror a real ship, and if the research output was of sufficient quality, an updated lab may not be needed. Future work may also take what is learned in such a lab to update human training. More technically, future work should look at each systems individually (e.g., navigation, sensors, IoT devices) and as a part of the ship's system-of-systems for vulnerabilities. Future research should also examine human-to-machine (e.g., augmented reality) interactions individually, but also as a whole, particularly as the amount of data humans need to process increases. The Cyber-SHIP lab will also help developers create automated audit/pentesting tools and AI solutions for intrusion detection and other malicious cyber-activity in systems.

5. Conclusions

The Cyber-SHIP Lab is designed to supply next generation research capabilities into maritime-cyber, particularly for analysing hardware, software, information, and developing protections. Unlike existing research capabilities, the lab enables system-of-systems research on connected devices, instead of individual systems in isolation. Development of Cyber-SHIP is meant to meet growing trends in maritime technology and will enable ongoing testing and validation of software and hardware systems to counter the threat of cyber-attacks to industry, government, and academia, also by bringing resources together. The lab is also designed to enhance current research facilities, simulators and cyber-ranges, while providing a much-needed capability that neither of these can provide for future security needs.

References

Allianz, 2019. Safety & Shipping Review, London. Allianz.

Arkin B, Stender S, McGraw G. 2005. Software penetration testing. New York. IEEE Security & Privacy.

Baldauf M, Procee S. 2014. Augmented REality in Ships Bridge Operation. London, Human Factors.

BIMCO, 2016. The Guidelines on Cyber Security onboard Ships Version 2.0. London. UNITED KINGDOM International Chamber of Shipping, INTERTANKO, BIMCO,CLIA, and INTERCARGO.

C4ADS, 2019. Above us only Stars: Exposing GPS Spoofing in Russia and Syria. Washingon DC USA. Center for Advanced Defense Studies.

Calder A, Watkins S. 2010. Information Security Risk Management for ISO27001/ISO27002. 1st edition. Cambridgeshire. IT Governance Publishing.

Cankar M, Stanovik S. 2018. Maritime IoT Solutions in Fog and Cloud. New York. IEEE/ACM International Conference on Utility and Cloud Computing Companion.

Choo K. 2011. The cyber threat landscape: Challenges and future research directions. Computers & Security.

Climpanu C. 2019. Report deems Russia a pioneer in GPS spoofing attacks. [Online] Available at: www.zdnet.com/

Davis J, Magrath S. 2013. A Survey of Cyber Ranges and Testbeds. Australia. Cyber Electronic Warfare Division.

ENSIA. 2011. Cyber Security Aspects in the Maritime Sector. St. Paul: www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1.

Frydenberg S, Nordby K, Eikenes JO. 2018. Exploring designs of augmented reality systems for ship bridges in artic wters. London. Human Factors.

Griffin J. 2002. Timing-accurate Storage Emulation. Louis USENIX File and Storage Technologies.

Ha S. 2018. A Novel Solution for NB-IoT Cell Coverage Expansion. New York. Global IoT Summit.

ICS. 2018. Shipping and world trade. London. ICS

IMO. 2003. Code of practice on security in ports. London.

IMO. 2018. International Maritime Organisation. [Online]

Lewis J. 2002. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. DC. CSIS.

Maersk. 2017. A. P. Moller Maersk improves underlying profit and grows revenue in first half of the year. [Online] Available at: https://edit.maersk.com/.

Man Y, Lundh M, MacKinnon S. 2018. Managing unruly technologies in the engine control room: from problem patching to an architectural thinking and standardization. s.l.: WMU Journal of Maritime Affairs.

Moorthy K, Vincent C, Darzi A. 2005. Simulation based training Is being extended from training individuals to teams. BMJ (Clinical research ed.) vol. 330,7490 (2005): 493-4. doi:10.1136/bmj.330.7490.493.

Pizzo S. 2018. IoT for Buoy Monitoring System. IEEE International Workshop on Metrology for the Sea. Learning to Measure Sea Health Parameters (MetroSea).

Rajamanickam V. 2018. COSCO's cyber attack and the importance of maritime cybersecurity. Available at: www.freightwaves.com/news/technology/.

Salman AKMDW. 2013. The Maritime Commons: Digital Repository of the World Maritime University. World Maritime University Dissertations.

Tam K, Jones K. 2018. Cyber-Risk Assessment for Autonomous Ships. New York. IEEE C-MRIC Cyber SA.

Tam K, Jones K. 2019a. Forensic Readiness within the Maritime Sector. New York. IEEE C-MRIC Cyber SA.

Tam K, Jones K. 2019b. MaCRA: A Model-Based Framework for Maritime Cyber-Risk Assessment. New York. WMU Maritime Affairs.

Tam K, Jones K. 2019c. Review of Cyber-security in emerging technology. International Conference of Maritime Science & Technology [accepted].

Tao, F. 2018. Digital twin-driven product design framework. Journal of Production Research.

Zolich, A. 2019. Survey on Communication and Networks for Autonomous Marine Systems. New York. Journal of Intelligent & Robotic Systems.