CYBERSECURITY PEDAGOGY & PRACTICE JOURNAL

**Volume 2, No. 1**
April 2023
ISSN: 2832-1006

In this issue:

**4.** **Educational Cyber Ranges: A Mixed-Method Study of Significant Learning Experiences using Cyber Ranges for Cybersecurity Education**
Cheryl Beauchamp, Regent University
Holly Matusovich, Virginia Tech

**26.** **A Survey of Privacy Metrics for Smart Homes**
Nooredin (Noory) Etezady, University of New Mexico

**38.** **Measurement, reporting, and monitoring in organizational security governance from the security professional's perspective Comparison of**
Kevin Slonka, Saint Francis University
Sushma Mishra, Robert Morris University
Peter Draus, Robert Morris University
Natalya Bromall, Robert Morris University

**50.** **CyberEducation-by-Design**
Paul Wagner, University of Arizona

**66.** **Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution**
Geoff Stoker, University of North Carolina Wilmington
Jeff Greer, University of North Carolina Wilmington
Ulku Clark, University of North Carolina Wilmington
Christopher Chiego, California State University Maritime Academy

**77.** **Command and Control – Revisiting EATPUT as an IS Model for Understanding SIEM Complexity**
Anthony Serapiglia, Saint Vincent College

iscap
Information Systems & Computing Academic Professionals

The **Cybersecurity Pedagogy and Practice Journal** (**CPPJ**) is a double-blind peer-reviewed academic journal published by **ISCAP** (Information Systems and Computing Academic Professionals). Publishing frequency is two times per year. The first year of publication was 2022.

CPPJ is published online (https://cppj.info). Our sister publication, the proceedings of the ISCAP Conference (https://proc.iscap.info) features all papers, panels, workshops, and presentations from the conference.

The journal acceptance review process involves a minimum of three double-blind peer reviews, where both the reviewer is not aware of the identities of the authors and the authors are not aware of the identities of the reviewers. The initial reviews happen before the ISCAP conference. At that point, papers are divided into award papers (top 15%), and other accepted proceedings papers. The other accepted proceedings papers are subjected to a second round of blind peer review to establish whether they will be accepted to the journal or not. Those papers that are deemed of sufficient quality are accepted for publication in the CPPJ journal.

While the primary path to journal publication is through the ISCAP conference, CPPJ does accept direct submissions at https://iscap.us/papers. Direct submissions are subjected to a double-blind peer review process, where reviewers do not know the names and affiliations of paper authors, and paper authors do not know the names and affiliations of reviewers. All submissions (articles, teaching tips, and teaching cases & notes) to the journal will be refereed by a rigorous evaluation process involving at least three blind reviews by qualified academic, industrial, or governmental computing professionals. Submissions will be judged not only on the suitability of the content but also on the readability and clarity of the prose.

Currently, the acceptance rate for the journal is under 35%.

Questions should be addressed to the editor at editorcppj@iscap.us or the publisher at publisher@iscap.us. Special thanks to members of ISCAP who perform the editorial and review processes for CPPJ.

# CYBERSECURITY PEDAGOGY AND PRACTICE JOURNAL

## Editors



## 2023 Review Board

# Considering Maritime Cybersecurity at a Non-Maritime Education and Training Institution

Geoff Stoker
stokerg@uncw.edu

Jeff Greer
greerj@uncw.edu

Ulku Clark
clarku@uncw.edu

Congdon School
University of North Carolina Wilmington
Wilmington, NC 28412 USA

Christopher Chiego
cchiego@csum.edu
California State University Maritime Academy
Vallejo, CA 94590 USA

## Abstract

The maritime industry, with its economically and strategically important role and critical infrastructure, appears to have a cybersecurity posture that lags other sectors (Akpan et al., 2022; Heering et al., 2021; National Academy of Public Administration, 2021). This lag is exacerbated by the current cybersecurity workforce shortage (Cyber Seek, 2022) which likely impacts maritime as much as all other industries. In this paper, we review the state of cybersecurity education within the maritime community and consider the possible value that cybersecurity students from non-maritime education and training (MET) institutions could bring to bear on maritime cybersecurity. We explore what additional knowledge these students might need in order to be ready to enter the maritime cybersecurity workforce and readily contribute.

**Keywords:** Cybersecurity, Maritime, Education

### 1. INTRODUCTION

International trade relies heavily on maritime operations. Both the International Maritime Organization (IMO, 2021b) and the United Nations (UN Conference on Trade and Development, 2021) estimate that 80+% of the world's trade by tonnage moves across the water. Like other industries and parts of the world economy, the maritime community is in the midst of significant *intelligent* digitally driven change as part of the Fourth Industrial Revolution (4IR) or Industry 4.0 (Schwab, 2017).

These changes are many and range across a broad spectrum – from the emergence of *smart* ports (Figure 1) to their full integration into the global supply chain (Figure 2, Zarzuelo et al., 2020) to the autonomous navigation of ships when underway (Noel et al., 2019). The digital

footprint (Figure 3) spreads deep and wide throughout ships, ports, terminals, crew devices, etc., in a non-uniform and inconsistent manner across maritime operations worldwide (International Association of Ports and Harbors [IAPH], 2020).

While the addition of digital systems and the digitization of the many existing physical systems involved in maritime operations often leads to efficiencies that save money, reduce time, increase safety, and lessen environmental impact, the shift also creates new risks as these digitized systems are more exposed to potential cyber-attacks. While the potential risk of cyber-attack to maritime operations has been recognized for several decades, even being used as a Hollywood plot device before the turn of the millennium (de Bont, 1997), the industry has faced challenges in responding to the cybersecurity threat (Akpan et al., 2022; Caponi & Belmont, 2015; Chang et al., 2019; DiRenzo et al., 2015; Gliha, 2017; National Academy of Public Administration, 2021; Pyykkö, 2020; U.S. Government Accountability Office, 2014).

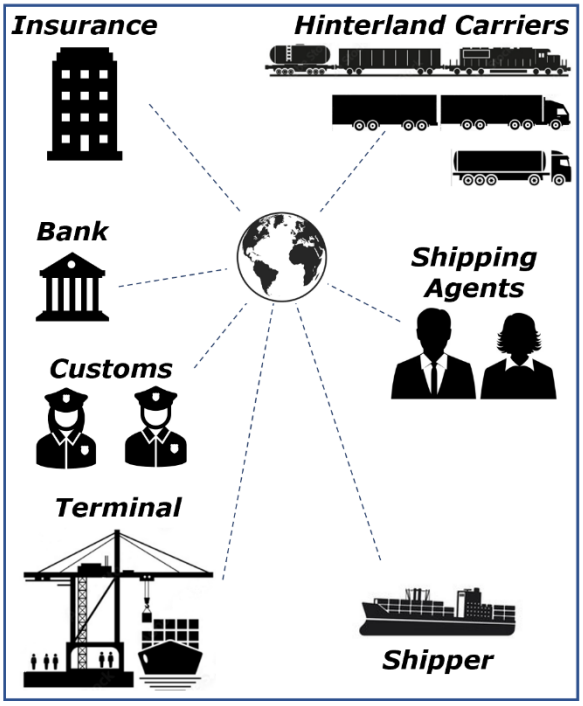



**Figure 1 – stylized view of a smart port**

The maritime industry encompasses almost everything connected to oceans, seas, and waterways including ports, shipyards, terminals, fishing, aquaculture, seafood processing, and many more areas. However, the focus of this paper is primarily around shipping transport, terminals, ports, and other aspects of the international shipping trade.

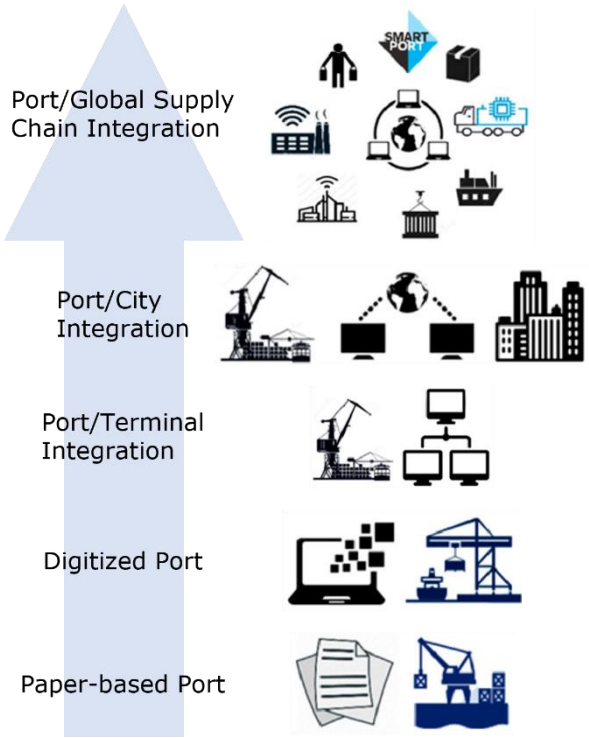



**Figure 2 – Evolution of local, regional, global port operations (modified Fig. 1. de la Peña Zarzuelo et al., 2020)**

Several major cyber-attacks in the 2010s focused the attention of the maritime industry on the critical importance of cybersecurity. In 2017, shipping industry leader Maersk saw its systems infected by the NotPetya malware, which nearly brought down the company's entire network. Thanks to a fortunately-timed disconnected computer with key data, Maersk was able to eventually reboot its network, albeit at a cost of disruptions estimated to have cost $300 million.

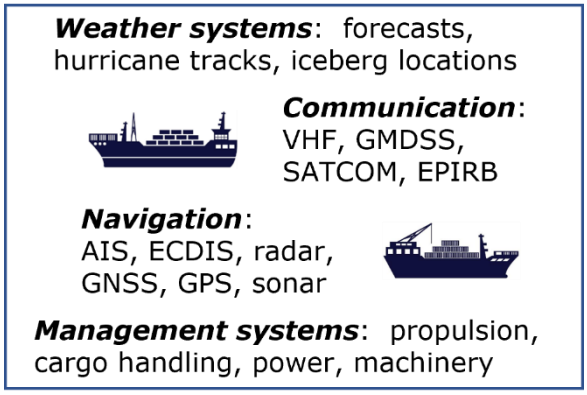



**Figure 3 – sample of systems in maritime operations (acronym list Appendix A)**

Additional attacks in 2018 on China Ocean Shipping (COSCO) Group and in 2020 on a wide range of other maritime targets further confirmed the threats to the networks of large shipping companies (Loomis et al., 2021). Whole supply chains were impacted by these attacks, some of which were targeted at the industry specifically while others stemmed from accidental infection with malware.

Other industry vulnerabilities have also been targeted by hackers in recent years, including those found in the network at the port of Antwerp in 2013 which was infiltrated to facilitate drug smuggling (Loomis et al., 2021) and a German ship's navigation system which was remotely hacked in 2017 while transiting the Red Sea. Experimental hacking demonstrations have also underscored the vulnerabilities of the maritime domain, which presents many different avenues for potential cyberattacks (Demchak and Thomas, 2021).

Despite this wide range of vulnerabilities across many parts of the industry, the maritime sector is finding it difficult to recruit a maritime-focused cybersecurity workforce (Satira, 2021). As with other industries, the maritime community is feeling the impact of this cybersecurity workforce shortage despite the earnest efforts of governments, businesses, and academia to mitigate the problem. In early 2021, the White House announced (O'Brien, 2021) the release of the National Maritime Cybersecurity Plan which included a section prioritizing the creation of a maritime cybersecurity workforce that tasked the Department of Homeland Security (DHS) and the United States Coast Guard (USCG) with developing more career paths for maritime cybersecurity in both the private and public sectors (White House, 2020). In an October 2021 report on the future of Maritime Cybersecurity, the Atlantic Council noted that, "There is a pressing need to create a cybersecurity-capable workforce, ensuring cyber literacy among the next generation of mariners and operators," (Loomis et al., 2021, p. 36) and counseled for collaboration among academia, the federal government, and international maritime organizations to encourage cybersecurity education. As we discuss below, however, there are major gaps in the resources and opportunities available to make this happen.

Among the education community, the cybersecurity area has received increasingly accelerated attention over the past 25+ years. Efforts to create and bolster cybersecurity-related offerings have been encouraged by initiatives like the National Security Agency (NSA) administered National Centers of Academic Excellence in Cybersecurity (NCAE-C) Program begun in 1999 (Center of Academic Excellence in Cybersecurity Community, 2022b), the Joint Task Force (JTF) on Cybersecurity Education launched in 2015 that resulted in the development of the 2017 cybersecurity (CSEC2017) curricular guidelines (JTF, 2022), and the 2018 approval by the Accreditation Board for Engineering and Technology (ABET) of program-specific criteria for cybersecurity at the baccalaureate level (ABET, 2022a).

The NCAE-C currently has 389 institutions (Center of Academic Excellence [CAE] in Cybersecurity Community, 2022a) participating as a CAE in Cyber Defense (CAE-CD), Cyber Operations (CAE-CO) and/or Cyber Research (CAE-R) and ABET currently lists 26 institutions with accredited cybersecurity 2-yr or 4-yr programs (ABET, 2022b).

The maturing curricular offerings for cybersecurity generally and the current need in the maritime community for more cybersecurity expertise specifically motivated the writing of this paper and the consideration of the questions:

- Can undergraduate students studying cybersecurity at non-MET institutions enter the maritime cybersecurity workforce after graduation and readily contribute?
- To better prepare students for maritime industry participation, what might a curriculum track include to provide some maritime-specific cybersecurity focus?

In section 2 of this paper, we conduct a literature review of maritime cybersecurity education; section 3 investigates the common touch points between cybersecurity presented within the maritime community and that presented in non-MET cybersecurity programs; section 4 explores potential additions to non-MET cybersecurity programs to make students more maritime workforce ready; in section 5 we elaborate on one of the recommendations in section 4; section 6 concludes.

## 2. STATE OF MARITIME CYBERSECURITY EDUCATION

Within the maritime community, there are active efforts to improve the level of cybersecurity knowledge and practice like the IMO's adopting resolution MSC.428(98) on Maritime Cyber Risk Management in Safety management Systems (IMO, 2017) and the International Chamber of

Shipping (ICS) publishing of The Guidelines on Cyber Security Onboard Ships (ICS, 2021).

There are MET-adjacent institutions with notable cybersecurity expertise. For example, the United States Naval Academy (USNA) is both a member of the NCAE-C Program as well as accredited by ABET (ABET, 2022a; USNA, 2020) with their cyber operations program, and the United States Coast Guard Academy (USCGA) is currently seeking ABET accreditation for their cyber systems program (USCGA, 2022). However, at METs across the globe, there are indications of cybersecurity education gaps.

Burke and Clott (2016), due in part to increasing automation and the evolution of autonomous ship operation, saw a need and argued for "significant education in information technology with an emphasis on cyber security for ship designers, ship operators, all shoreside personnel" (p. 5). Ahvenjärvi et al. (2019) conducted a review of the International Convention on Standards for Training, Certification and Watchkeeping for Seafarers (STCW) and a survey of members from the International Association of Maritime Universities (IAMU) and concluded that both cybersecurity and cyber safety need to be better addressed in MET.

Alop (2019) examined the challenges posed to maritime education by the rapidly unfolding digital 4IR and concluded there is a need to change the paradigm. A survey of maritime professionals was conducted by Alcaide and Llave (2020), Sep-Dec 2018, to ascertain the mariners' level of cybersecurity knowledge. With 102 usable responses, they claimed the results indicated that "the lack of knowledge of maritime experts consulted exceeds 75%, where it is essential to highlight, among other topics: procedures (detect, act, communicate, recover, etc.); simulacra [drills]; cyber security/threats" (p. 553).

Through review of teaching materials and interviews with personnel at four MET institutions, Bacasdoon (2021) found that while cybersecurity was being taught, the topics, degree of depth, and modality differed considerably from one MET institution to the next. He developed a framework within which cybersecurity education and training could be effectively presented to seafarers. Bacasdoon also found, via a survey with 403 results, that seafarers generally perceived the MET institution cybersecurity topics being covered to be needed and considered important to the successful execution of their jobs.

In November 2021, the National Academy of Public Administration published a largely critical report assessing the U.S. Merchant Marine Academy (USMMA) that provided 67 recommendations to position USMMA to better handle the future challenges of functioning in an increasingly complex operating environment. Included was the recognition that "the maritime workforce of the future will need proficiency in data science, machine learning, and cybersecurity;" (p. 73).

Heering, et al. (2021), examining published maritime cybersecurity research on MET programs for seafarers, found a lack of sufficient depth of instruction and reported that "there are no requirements for MET institutions to include cybersecurity awareness or cyber hygiene practice in the curricula," (p. 49). They did note, however, that this may be attributable to the slow process of changes in international maritime regulations that inhibit agility in shifting MET curricula and courses.

This review of existing maritime cybersecurity education-related literature leads us to conclude that, in the current environment, MET institutions face challenges in rapidly addressing the pressing cybersecurity education needs. Thus, there likely is value in bringing cybersecurity expertise to the maritime community from non-MET higher education institutions to complement efforts being made within MET institutions.

## 3. CYBERSECURITY EDUCATION COMMONS

We believe that students at many cybersecurity programs outside of MET institutions are likely to already be well-positioned to engage with maritime cybersecurity. This conjecture is based on the close ties that can be seen between published maritime industry cybersecurity guidance and published non-maritime specific guidance, on industry-neutral cybersecurity vocabulary promoted by maritime organizations, and on several informal conversations with current maritime cybersecurity personnel.

In an apparent effort to adopt useful and established cybersecurity tools, as well as a common cybersecurity language, the maritime community has embraced existing non-maritime specific cybersecurity efforts like the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (NIST, 2018). In their published cybersecurity guidance, both the IAPH (2020) and the IMO (2021a) directly reference the five concurrent and continuous functions of the NIST

framework core (Figure 4), while the ICS (2021) explicitly acknowledges taking the five functions into account during the development of their guidelines. This is a framework with which cybersecurity students from most programs are almost certainly already familiar.

Using risk-based activities to complement compliance actions when securing network and device hardware/software has become more commonplace (Lin & Saebeler, 2019) and risk-based approaches are likely to be less industry specific than compliance-based ones. The NCAE-C program document (NSA, 2019) that lists the details of CAE cyber defense (CAE-CD) knowledge units (KU) reflects the non-industry specific teaching of risk-related cybersecurity.


**Figure 4 – framework core five concurrent and continuous functions (NIST, 2022)**

The Cybersecurity Foundations (CSF) KU, one of three mandatory foundational KUs that must be satisfied be every CAE-CD designated institution, explicitly requires risk management, basic risk assessment, and residual risk be covered. The non-technical core KU, Security Risk Analysis (SRA), which is likely covered by most CAE-CD schools, plainly states an intent "to provide students with sufficient understanding of risk assessment models, methodologies and processes such that they can perform a risk assessment of a particular system and recommend mitigations to identified risks," (NSA, 2019, p. 29). Fundamental knowledge of risk-based approaches to cybersecurity is usable across all sectors.

A review of the enumerated key vocabulary in the published ICS and IAPH cybersecurity guidance reveals no maritime-unique terms. Of the 96 terms listed and defined – 40 in the ICS guidelines glossary (2021) and 56 in the IAPH white paper (2020) – 84 are unique and 12 overlap (see Appendix B). Current post-secondary cybersecurity students in NCAE-C, or similar quality, programs should find most, if not all, of these 84 terms to be familiar. Most of them are explicitly mentioned in the 2020 CAE-CD KU document (NSA, 2019).

Over the past several months, we have engaged in informal discussions regarding maritime cybersecurity with several current maritime professionals. They have varying degrees of awareness of and responsibility for cybersecurity within their respective organizations and hold jobs like Coast Guard cybersecurity specialist and port security analyst. These professionals confirmed the centrality of the NIST framework for maritime operations and supply chain partners, as well as other NIST special publications (SP) like SP 800-171r2 (Ross et al., 2020) for protecting unclassified information and SP 800-53r5 (Joint Task Force, 2020) which outlines security and privacy controls. Each also indicated a belief that students with a broad understanding of cybersecurity topics could readily contribute to the maritime community without industry-specific knowledge. Of course, having maritime-specific knowledge was better than not having it, but lack of industry-specific information would not preclude them from contributing and such knowledge likely could be readily picked up on the job.

## 4. READYING NON-MET CYBERSECURITY STUDENTS FOR MARITIME

An opportunity appears to exist for cybersecurity programs to further develop students by readying them for industry-specific specialization, like maritime, where intersecting interests and potential value are present. We take as a premise that the educational objective for industry sector specialization is to pull forward knowledge that is typically received via on-the-job training (OJT). If provided in the classroom under controlled conditions, the possibility exists for accelerated learning and for cyber defenders to show up better prepared on day one of employment.

Analyzing the results of our review of maritime cybersecurity education, we make six recommendations in support of maritime cybersecurity specialization education. These recommendations are made envisioning a relatively short two - four course maritime specialty, focus, concentration, or track within an existing cybersecurity program.

First, a generalized introduction to the maritime industry would provide students interested in maritime with an orientation to the sector that would later support better contextual learning.

Recommended educational content includes broadly covering topics like ships and ship operations, ports and port operations, life at sea, crew roles, an overview of digital systems employed for maritime enterprise mission achievement, etc. Furthermore, the maritime sector has a unique threat profile; understanding the types of actors interested in cyberattacks on the maritime sector, including the interaction with forms of piracy, are important in understanding the overall threat (Jones et al., 2016). This introduction will be useful for developing and understanding a maritime mental model or framework. Establishing this mental model/ framework would help prepare students to defend a maritime enterprise more successfully.

Second, given the regulated nature of the maritime industry, introducing students to the rules of the game is important. Existing regulations are currently being updated to include cybersecurity by controlling authorities like the U.S. Coast Guard, the IMO, flag states of convenience for vessel registration, etc. Gaining a basic understanding of relevant regulations and their scope will better prepare students for the compliance side of maritime cybersecurity.

Third, knowledge, skills, and abilities (KSAs) are mapped to cybersecurity work roles in the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (National Initiative for Cybersecurity Careers and Studies, 2022; Peterson et al., 2020). This concept can be extended to the roles in a maritime enterprise. It is widely acknowledged that every enterprise employee is responsible for cybersecurity. Therefore, it is important for students to understand cybersecurity KSAs for employee types within an enterprise. This information will help students understand how to set up training programs to enhance enterprise cybersecurity.

Fourth, there are enterprise behaviors unique to the maritime industry the awareness of which will be valuable for students. For example, personnel on board a ship are typically temporary contract workers employed for six or nine months. Therefore, ships experience a higher personnel turnover rate than most land-based enterprises and this, in turn, creates additional cyber risk. Another example is that ship IT infrastructure is serviced in remote ports of the world by third-party contracted service technicians. These technicians have direct access to ship IT infrastructure and present a potential cyber risk.

Fifth, collaborations between MET and non-MET institutions can help complement the strengths of each. METs often have specialized equipment, from simulation rooms to a variety of training watercraft, that could be used by non-MET students and faculty to gain hands-on experience. Non-MET institutions can bring their cybersecurity expertise and facilities to bear by offering advanced training opportunities and a wider geographic footprint of opportunities. Faculty from MET and non-MET institutions could exchange ideas and best practices developed in different contexts and work together on enhancing their respective curricula.

Sixth, the creation of new, tangible classroom teaching aids will provide students with an active versus passive lecture-based learning experience. The creation of a maritime mental model/framework, the expected result of the first recommendation, helps place follow-on maritime cybersecurity instruction within a useful context. Interactive aids that bring the enterprise into the classroom, likely the best alternative we have to actual work experience, will help cybersecurity students visualize the relevant, associated attack surfaces. Being able to view an image of the digital enterprise being defended and its operating environment versus imagining an abstract, nondescript enterprise will likely accelerate student understanding.

Crafting a maritime focus within an existing cybersecurity program using the guidance offered by these six recommendations should provide a solid head start to any student interested in the maritime industry. In the next section, we elaborate on the sixth recommendation and its potential for industry-focused cybersecurity.

## 5. INTERACTIVE AIDS FOR FOCUSED CYBERSECURITY

Many cybersecurity students are taught the theory of NIST's cybersecurity framework (Figure 4) and likely apply the theory to one or more case studies. However, the industry in the case study is unlikely deliberately chosen and the assignment is likely primarily a mental exercise focused primarily on the framework rather than balanced with gaining understanding of and insight into an industry.

The type of teaching aid we envision with our fifth recommendation in the previous section is one that allows students to *see* the environment they are defending. Our guiding precept – coined Greer's Rule of Thumb – is that: *it is impossible*

*to defend what cannot be visualized and described*.

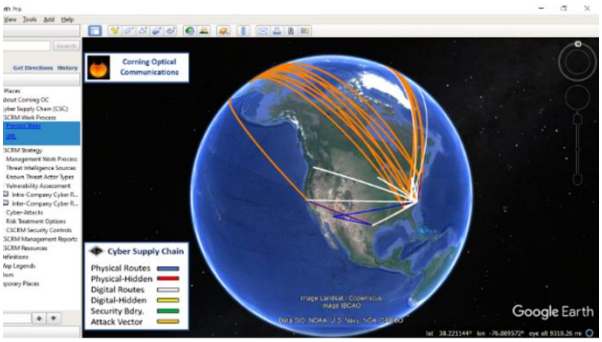
This requirement seems best met by the development of an interactive environment like the integrated virtual learning environment for cybersecurity education (IVLE4C, Greer et al., 2022). Whereas traditional cyber ranges are network centric, IVLE4C presents a holistic view of all elements in an enterprise's attack surface. The initial version of IVLE4C was a low-cost option developed using Microsoft Office and Google Earth Pro (Figure 5), but it already provides something with which students will be able to clearly visualize the enterprise they are defending, and it is easily adaptable to visualizing maritime enterprises like ports and terminals.

Students need to understand how the particular enterprise type and particular enterprise behaviors impact the corresponding attack surface structure. Each attack surface element has inherent vulnerabilities that can be exploited if left untreated. The objective of risk management is to change the attack surface elements into trust boundaries at a level sufficient to meet enterprise cybersecurity requirements. It is also useful for students and cybersecurity professionals who will have varying levels of information when working to defend a modern digital enterprise.

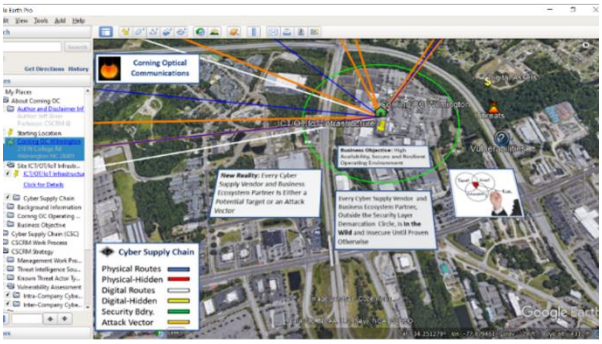
Any given maritime enterprise, a complex system of systems, needs to be analyzed in terms of assets of value, threats, and known vulnerabilities. These are the three elements required to form a picture of risk. Students need to be taught how to enumerate risks in a register. Once recorded in a register, students need to be taught how to assess them using a heat matrix, ranking identified risks from high to low. An interactive aid, like IVLE4C, will help cybersecurity students more quickly learn this process and appreciate how theoretical frameworks directly relate to the physical operating environment.

A risk register serves as an artifact for designing a risk treatment plan. Students need to be taught how to utilize the standard ISO 31000 Risk Management Framework options to treat each recorded risk. Once a risk treatment plan is complete, students need to be taught how to implement it using sound project management practices. This can be accomplished by teaching a student how to develop a plan of action and milestones (POAM). Conducting all these steps while referencing and interacting with a visualization of the defended enterprise should accelerate students' understanding of the industry of focus.

Modeling an enterprise is not a new idea in cybersecurity education. It is also not new in maritime where simulators are commonly used for teaching navigation. What is underdeveloped is the application of modeling in developing enterprise cybersecurity solutions in the maritime industry and other critical infrastructure sectors. Creating a virtual environment where students can work at the enterprise system of systems level across multiple critical infrastructure sectors will facilitate advanced cognitive and cybersecurity skills development that are needed by future cybersecurity leaders.




Global View




Enterprise Operating Site

**Figure 5 – IVLE4C v1 global view and enterprise operating site view**

## 6. CONCLUSIONS

In this paper, we examined the current state of cybersecurity and cybersecurity education within the maritime community as reflected in the academic and professional literature. We found that the industry's cybersecurity posture lags other sectors and that a gap appears to exist in cybersecurity education within current MET curricula. Given the pressing challenge of the cybersecurity workforce shortage, it seems plausible that the maritime industry as well as

governmental agencies in the maritime sector would benefit from the cybersecurity education produced by non-MET institutions as well.

In answer to the two questions posed in the introduction, we suggest that students in non-MET cybersecurity programs are well-positioned with their existing knowledge to contribute to the maritime community's cybersecurity efforts. By incorporating maritime-specific knowledge into their education, these students could readily contribute to the maritime sector immediately after graduation. We further suggest six ways to incorporate a maritime focus into an existing cybersecurity curriculum and then elaborate on the suggestion related to interactive teaching aids designed to bring the enterprise into the classroom.

## 7. REFERENCES

Accreditation Board for Engineering and Technology. (2022a, July). ABET approves accreditation criteria for undergraduate cybersecurity programs. https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/

Accreditation Board for Engineering and Technology. (2022b, July). Accredited Programs. https://amspub.abet.org/aps/category-search?disciplines=91&disciplines=94

Ahvenjärvi, S., Czarnowski, I., & Mogensen. J. (2019, August). Addressing Cyber Security in Maritime Education and Training (CYMET). FY2018 IAMU Research Project. http://archive.iamu-edu.org/download/final-report-of-research-project-fy2018/

Akpan, F., Bendiab, G., Shiaeles, S., Karamperidis, S., & Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. Network, 2(1), 123-138. https://www.mdpi.com/2673-8732/2/1/9/pdf

Alcaide, J. I., & Llave, R. G. (2020). Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45, 547-554. https://cyberonboard.com/wp-content/uploads/Critical-Infrastructures-Cybersecurity-and-the-Maritime-Sector.pdf

Alop, A. (2019, April). The challenges of the digital technology era for maritime education and training. In 2019 European Navigation Conference (ENC) (pp. 1-5). IEEE. https://www.researchgate.net/publication/333152469_The_Challenges_of_the_Digital_Technology_Era_for_Maritime_Education_and_Training

Bacasdoon, J. (2021). A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches. https://commons.wmu.se/all_dissertations/1680/

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. Intellectual Property & Technology Law Journal, 27(1), 16. https://www.sfmx.org/wp-content/uploads/2017/03/Maritime-Cybersecurity-10-2014.pdf

Center of Academic Excellence in Cybersecurity Community. (2022a, July). CAE institution map. https://www.caecommunity.org/cae-map

Center of Academic Excellence in Cybersecurity Community. (2022b, July). What is a CAE in Cybersecurity? https://www.caecommunity.org/about-us/what-cae-cybersecurity

Chang, C. H., Wenming, S., Wei, Z., Changki, P., & Kontovas, C. A. (2019, November). Evaluating cybersecurity risks in the maritime industry: a literature review. In Proceedings of the international association of Maritime Universities (IAMU) Conference. http://researchonline.ljmu.ac.uk/id/eprint/11929/1/IAMU%202019%20Park%20et%20al.pdf

Cyber Seek. (2022, July). Cybersecurity Supply/Demand Heat Map. https://www.cyberseek.org/heatmap.html

de Bont, J. (Director). (1997). Speed 2: Cruise Control [Film]. Blue Tulip Productions; 20th Century Fox. https://www.imdb.com/title/tt0120179/

de la Peña Zarzuelo, I., Soeane, M. J. F., & Bermúdez, B. L. (2020). Industry 4.0 in the port and maritime industry: A literature review. Journal of Industrial Information Integration, 20, 100173. https://www.Sciencedirect.com/science/article/pii/S2452414X20300480

Demchak, C. and Thomas, M. (2021, October 15) Can't Sail Away From Cyber Attacks: 'Sea-Hacking' From Land. War on the Rocks. https://warontherocks.com/2021/10/cant-sail-away-from-cyber-attacks-sea-hacking-from-land/

DiRenzo, J., Goward, D. A., & Roberts, F. S. (2015, July). The little-known challenge of maritime cyber security. In 2015 6th International Conference on Information, Intelligence, Systems and Applications (IISA) (pp. 1-5). IEEE. http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf

Gliha, D. (2017). Maritime Cyber Crime-21st Century Piracy. Annals of the Faculty of Law of the University of Zenica, 20, 228-238. https://heinonline.org/HOL/Page?handle=hein.journals/zenici20&div=15&g_sent=1&casa_token=&collection=journals

Greer, J., Stoker, G., & Clark, U., (2022). Proposing the Integrated Virtual Learning Environment for Cybersecurity Education (IVLE4C). Cybersecurity Pedagogy and Practice Journal1(1) pp 54-65. http://cppj.info/2022-1/n1/CPPJv1n1p54.pdf

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In Developments in Maritime Technology and Engineering (pp. 49-61). CRC Press. https://www.researchgate.net/profile/Dan-Heering/publication/353924133_Shortcomings_in_cybersecurity_education_for_seafarers/links/611a34d00c2bfa282a49e898/Shortcomings-in-cybersecurity-education-for-seafarers.pdf

International Association of Ports and Harbors. (2020, June). Port Community Cyber Security. https://sustainableworldports.org/wp-content/uploads/IAPH-Port-Community-Cyber-Security-Report-Q2-2020.pdf

International Chamber of Shipping. (2021). The Guidelines on Cyber Security Onboard Ships v4. https://www.ics-shipping.org/wp-content/uploads/2021/02/2021-Cyber-Security-Guidelines.pdf

International Maritime Organization. (2017, June 16). Resolution MSC.428(98). Maritime Cyber Risk Management in Safety Management Systems. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/Resolution%20MSC.428(98).pdf

International Maritime Organization. (2021a, June 14). Guidelines on Maritime Cyber Risk Management. MSC-FAL. 1/Circ. 3/Rev. 1. https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/Facilitation/MSC-FAL.1-Circ.3-Rev.1.pdf

International Maritime Organization. (2021b). Introduction to IMO. https://www.imo.org/en/About/Pages/Default.aspx

Joint Task Force, National Institute of Standards and Technology. (2020, September). Security and privacy controls for information systems and organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Joint Task Force on Cybersecurity Education. (2022, July). ACM/IEEE/AIS SIGSEC/IFIP Cybersecurity Curricular Guideline. https://cybered.hosting.acm.org/wp/

Jones, K. D., Tam, K., & Papadaki, M. (2016). Threats and impacts in maritime cyber security. IET Engineering & Technology Reference.

Lin, W. & Saebeler, D. (2019). Risk-based v. compliance-based utility cybersecurity a false dichotomy. Energy Law Journal, 40(2), 243-282. https://www.eba-net.org/assets/1/6/8._[Lin_and_Saebeler][Final][243-282].pdf

Loomis, W., Singh V. V., Kessler, G., and Bellekens, X. (2021, October) Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity. Atlantic Council Scowcroft Center for Strategy and Security.

National Academy of Public Administration. (2021, November). Organizational Assessment of the U.S. Merchant Marine Academy: A Path Forward. https://s3.us-west-2.amazonaws.com/napa-2021/NAPA-Panel-Report-FINAL.pdf

National Initiative for Cybersecurity Careers and Studies. (2022, July). Workforce Framework for Cybersecurity (NICE Framework). https://niccs.cisa.gov/workforce-development/nice-framework

National Institute of Standards and Technology. (2022). Cybersecurity framework. https://www.nist.gov/cyberframework

National Institute of Standards and Technology. (2018, April 16). Framework for improving critical infrastructure cybersecurity. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

National Security Agency. (2019, June 7). 2020 CAE cyber defense (CAE-CD) knowledge units. https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf

Noel, A., Shreyanka, K., Gowtham, K., & Satya, K. (2019, November). Autonomous ship navigation methods: a review. Proceedings of

the International Conference on Marine Engineering and Technology (ICMET) Oman. https://www.researchgate.net/profile/Shameem-Bm/publication/338338942_Autonomous_Ship_Navigation_Methods_A_Review/links/5e4aa5cd92851c7f7f425403/Autonomous-Ship-Navigation-Methods-A-Review.pdf

O'Brien, R. C. (2021, January 5). Statement from National Security Advisor Robert C. O'Brien Regarding the National Maritime Cybersecurity Plan. https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-regarding-national-maritime-cybersecurity-plan/

Peterson, R., Santos, D., Smith, M., Wetzel, K., & Witte, G. (2020, November). NIST SP 800-181r1. Workforce Framework for Cybersecurity (NICE Framework). https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf

Pyykkö, H., Kuusijärvi, J., Silverajan, B., & Hinkka, V. (2020). The Cyber Threat Preparedness in the Maritime Logistics Industry. Proceedings of 8th Transport Research Arena, 27-30. https://www.corealis.eu/wp-content/uploads/2020/05/TRA2020_Cybersecurity_article_Pyykko_et_al..pdf

Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., & Guissanie, G. (2020, February). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

Satira, Brian. (2021, May 12). Navigating the Waters of Maritime Cybersecurity. Helpnet Security. https://www.helpnetsecurity.com/2021/05/12/maritime-cybersecurity/

Schwab, K. (2017). The fourth industrial revolution. Currency. https://jmss.vic.edu.au/wp-content/uploads/2021/06/The_Fourth_Industrial_Revolution.pdf

United Nations Conference on Trade and Development. (2021). Review of maritime transport. https://unctad.org/topic/transport-and-trade-logistics/review-of-maritime-transport

U.S. Coast Guard Academy. (2022, July). Cyber systems accreditation. https://www.uscga.edu/cyber-systems/

U.S. Government Accountability Office. (2014). Maritime critical infrastructure protection: DHS needs to better address port cybersecurity. https://www.gao.gov/assets/gao-14-459.pdf

U.S. Naval Academy. (2020, November 6). USNA cyber operations program granted NSA designation. https://www.usna.edu/NewsCenter/2020/11/USNA_CYBER_OPERATIONS_PROGRAM_GRANTED_NSA_DESIGNATION.php

White House. (2020, December). National Maritime Cybersecurity Plan to the National Strategy for Maritime Security. https://trumpwhitehouse.archives.gov/wp-content/uploads/2021/01/12.2.2020-National-Maritime-Cybersecurity-Plan.pdf

**Editor's Note:**

*This paper was selected for inclusion in the journal as an ISCAP 2022 Meritorious Paper. The acceptance rate is typically 15% for this category of paper based on blind reviews from six or more peers including three or more former best papers authors who did not submit a paper in 2022.*

## Appendix A – Acronyms of Common Maritime Systems

AIS – automatic identification system
ECDIS – electronic chart display and information system
EPIRB – emergency position-indicating radio beacon
GMDSS – global maritime distress and safety system
GNSS – global navigation satellite systems
GPS – global positioning system
SATCOM – satellite communications
VHF – very high frequency

## Appendix B – Cybersecurity Key Terms

This appendix lists the 84 unique terms pulled from the combined list of 96 terms (12 overlapping) from the 40 terms of the ICS' Guidelines on Cyber Security Onboard Ships v4 (2021) and the 56 terms of the IAPH's Port Community Cyber Security (2020).

| | | |
|---|---|---|
| Access control | Data breach | Operational technology (OT) |
| Adware | Defence in breadth | Patches |
| Advanced Persistent Threat (APT) | Defence in depth | Phishing |
| Antivirus (AV) | Digitisation | Principle of least privilege |
| Authentication | Digitalisation | Ransomware |
| Authorization | Encryption | Recovery |
| Accounting | Event and Incident response | Removable media |
| Availability | Executable software | Risk assessment |
| Back door | Firewall | Risk management |
| Backup | Firmware | Sandbox |
| Business Impact Analysis | Flaw | Service provider |
| Bring your own device (BYOD) | Incident | Social engineering |
| Chain of custody | Industrial Internet of Things (IIoT) | Software whitelisting |
| Computer Emergency Response Team (CERT) | Information Technology (IT) | Spam |
| Computer Security Incident | Information sharing and communications | Spear phishing |
| Confidentiality | Insider threat | Spoofing |
| Contingency plan | Integrity | Spyware |
| Cookie | Intrusion Detection System (IDS) | Supply chain risk |
| Cyber attack | Intrusion Prevention System (IPS) | Threat |
| Cyber ecosystem | Information Sharing and Analysis Center (ISAC) | Threat and vuln management |
| Cyber governance | Least privilege | Threat assessment |
| Cyber incident | Local Area Network (LAN) | Threat profile |
| Cyber risk management | Malware | Typo squatting |
| Cyber security | Maturity | Virtual Local Area Network (VLAN) |
| Cyber security plan | Manufacturer | Virtual Private Network (VPN) |
| Cyber security policy | Monitoring | Virus |
| Cyber security program | Multifactor Authentication (MFA) | Vishing |
| Cyber system | Operational resilience | Wi-Fi |