https://doi.org/10.53656/ped2023-6s.07

Maritime Cybersecurity
Морска киберсигурност

MODELLING OF MARITIME CYBER SECURITY EDUCATION AND TRAINING

Dr. Gizem Kayisoglu,
Dr. Pelin Bolat,
Dr. Emre Duzenli
Istanbul Technical University (Turkey)

Abstract. The existence of sophisticated and integrated cyberspace aboard ships with information technology (IT) and operational technology (OT) makes cybersecurity a crucial concern for the maritime sector. The marine sector has benefited greatly from information and communication technologies, but they have also made ship systems and maritime infrastructure more susceptible to cyberattacks. Cyberattacks on ships have the potential to result in fatalities, severe financial losses, environmental damage, and other negative effects. A model course or specification for maritime cyber security education and training through the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) 1978 has not yet been published by the International Maritime Organization (IMO), despite the fact that MSC.428 mandates cyber security risk management in the safety management system on ships to combat cyber-attacks and improve cyber resistance in maritime environments. The Analytic Hierarchical Process (AHP) technique is used in this work to offer a model for a curriculum for cyber security in the Maritime Education and Training (MET) system. It is possible to identify each competency's priority in the MET system's cyber security curriculum by comparing the relative weights assigned to each one. The results of the research provide the Met Institutions with the ability to be proactive and include cyber security knowledge and abilities into proposed curricula.

Keywords: maritime cyber security; MET; maritime cyber education; SEM

1. Introduction

Networking information and communication technology and operational technology on board ships is becoming more common as technology advances, and often connects to the Internet. While the goal of implementing cyber systems is to reduce the navigator's workload, doing so comes with the trade-off of increased complexity and vulnerability, both of which may necessitate a reevaluation of the skillset required to navigate safely and efficiently. To improve the navigator's skill through heightened system awareness, modern examples of how cyber-attacks can distort situational awareness and impede operations are required. Onboard ships, seafarers must be prepared to deal with an increasing number of cyber risks, with cybersecurity knowledge playing a vital part in emergency and crisis management. Unfortunately, current maritime education and training (MET) programs do not offer seafarers enough understanding of cybersecurity to enable them to recognize and mitigate the current cyber threat scenario.

There are important cybersecurity institutions in close proximity to the MET. The United States Naval Academy (USNA) has a cyber-operations program that is both NCAE-C Program-affiliated and ABET-accredited[1, 10], and the United States Coast Guard Academy (USCGA) is applying for ABET accreditation for its cyber systems program[9]. The world over, however, signs of cybersecurity education deficiencies can be seen at METs.

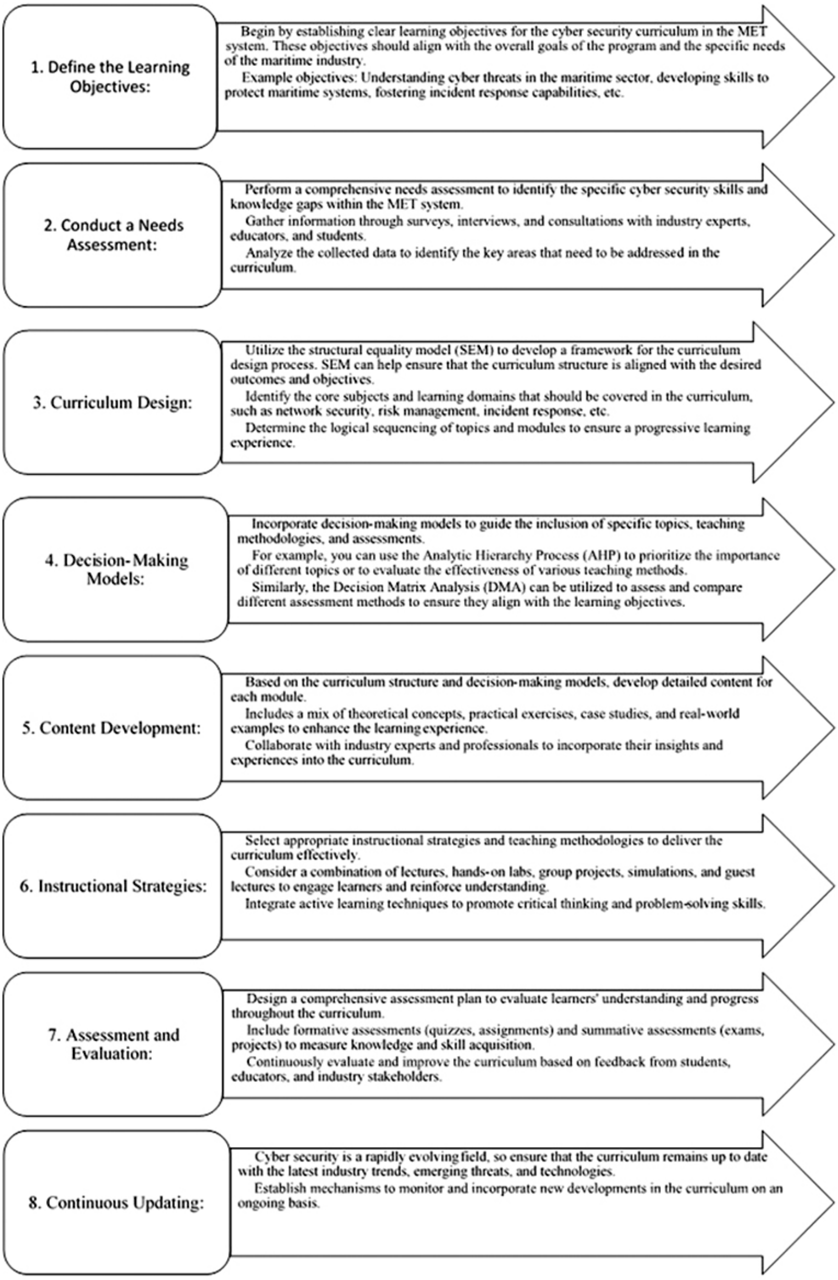
In the literature, there are limited studies focusing on maritime cyber security education and training. Heering et al., (Heering et al. 2021) offer a structured survey of published maritime cybersecurity research, as well as an overview of the cybersecurity component of MET for sailors. According to the findings, there are presently no regulations for MET institutions to include cybersecurity awareness or cyber hygiene practice in their curricula. Shapo & Levinskyi (Shapo & Levinskyi 2021) stated that, on the one hand, it's important to enhance and broaden maritime schools' instruction in the following areas of information technology: the Industrial Internet of Things; wireless data transfer technologies; hardware for large-scale computer control systems; satellite data transfer systems, technologies, and protocols; big data; artificial intelligence; virtual and augmented reality; remote control; and pc programming. However, education about cyber security measures, tools, and procedures is essential. Specific hardware facilities and e-learning technologies are required for the actualization of each of these goals. Hareide et al., (Hareide et al. 2018) illustrate some of the entry points through which a cyber-attack can compromise a ship and discuss the likelihood and repercussions of such an attack. To better understand how to demystify cyber dangers and increase navigators' proficiency, they give a case study in their research. Scanlan et al. (2022) discuss a number of approaches that have been taken to address difficulty for maritime cyber security education. Their main goals include spreading knowledge about cyber risk and teaching people how to handle it safely in the maritime industry. There is no one answer to this problem; rather, multiple alternatives are offered. To guarantee digital systems are used in a secure manner, there needs to be an industry-wide effort. One answer could be to take another look at business relationship management/enterprise resource planning and determine what role it can play in laying a solid groundwork for the necessary skill requirements within the industry. To help shipping businesses keep a trained staff, an updated BRM/ERM might set a baseline of abilities and awareness in connection to cybersecurity.

Cyber-attacks onboard ships can cause navigational accidents, critical economic costs, environmental pollution, and loss of human life. Although the International Maritime Organization (IMO) has issued MSC.428 – which stipulates cyber security risk management in the safety management system on ships to combat cyber-attacks and improve cyber resistance in maritime environments – the IMO has yet to publish a model course or a specification for maritime cyber security education and training through the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) 1978. In this paper, a model is proposed to provide a curriculum for cyber security in the Maritime Education and Training (MET) system, which complies with the STCW code. For this purpose, competences, understanding, knowledge, proficiency, methods for demonstrating competence, and criteria for evaluating competence under a function are developed in the maritime community by examining the current situation of maritime cyber security with the help of academic and industrial literature, as well as codes, instructions, and regulatory frames for maritime cyber security. Additionally, determined competences in curriculum for maritime cyber security are compared by using Analytic Hierarchical Process (AHP) method. By comparing the relative weights of each competence, their prioritization in the curriculum for cyber security in the MET system can be determined. These rankings provide guidance on the relative importance and priority of each competence in the curriculum, allowing for informed decision-making during the curriculum design process. The output of the study enables the MET Institutions to be proactive and include cyber security information and skills in the curriculum proposals.

2. Methodology

Designing a curriculum for cyber security in the Maritime Education and Training (MET) system requires careful consideration of various factors. Casey (2008) proposes steps for a curriculum development as in Figure 1. In this study, in addition to the steps shown in Figure 1, mainly, table framework in the STCW code, which shows the specification of minimum standards of competence for related proficiency of seafarers, is considered for the purpose of development a curriculum tailor-made cyber security in MET. After the development of curriculum, determined competences in curriculum for maritime cyber security are compared by using AHP method for determining prioritizations of the competences in the curriculum for cyber security in the MET system. These rankings provide guidance on the relative importance and priority of each competence in the curriculum, allowing for informed decision-making during the curriculum design process.

The main purpose of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) is to establish minimum training, certification, and watchkeeping standards for seafarers globally[7]. The convention sets out the requirements for seafarers' competence, knowledge, and skills to ensure safe navigation, protection of the marine environment, and the well-



1. Define the Learning Objectives:

Begin by establishing clear learning objectives for the cyber security curriculum in the MET system. These objectives should align with the overall goals of the program and the specific needs of the maritime industry.

Example objectives: Understanding cyber threats in the maritime sector, developing skills to protect maritime systems, fostering incident response capabilities, etc.

2. Conduct a Needs Assessment:

Perform a comprehensive needs assessment to identify the specific cyber security skills and knowledge gaps within the MET system.

Gather information through surveys, interviews, and consultations with industry experts, educators, and students.

Analyze the collected data to identify the key areas that need to be addressed in the curriculum.

3. Curriculum Design:

Utilize the structural equality model (SEM) to develop a framework for the curriculum design process. SEM can help ensure that the curriculum structure is aligned with the desired outcomes and objectives.

Identify the core subjects and learning domains that should be covered in the curriculum, such as network security, risk management, incident response, etc.

Determine the logical sequencing of topics and modules to ensure a progressive learning experience.

4. Decision-Making Models:

Incorporate decision-making models to guide the inclusion of specific topics, teaching methodologies, and assessments.

For example, you can use the Analytic Hierarchy Process (AHP) to prioritize the importance of different topics or to evaluate the effectiveness of various teaching methods.

Similarly, the Decision Matrix Analysis (DMA) can be utilized to assess and compare different assessment methods to ensure they align with the learning objectives.

5. Content Development:

Based on the curriculum structure and decision-making models, develop detailed content for each module.

Includes a mix of theoretical concepts, practical exercises, case studies, and real-world examples to enhance the learningexperience.

Collaborate with industry experts and professionals to incorporate their insights and experiences into the curriculum.

6. Instructional Strategies:

Select appropriate instructional strategies and teaching methodologies to deliver the curriculum effectively.

Consider a combination of lectures, hands-on labs, group projects, simulations, and guest lectures to engage learners and reinforce understanding.

Integrate active learning techniques to promote critical thinking and problem-solving skills.

7. Assessment and Evaluation:

Design a comprehensive assessment plan to evaluate learners' understanding and progress throughout the curriculum.

Include formative assessments (quizzes, assignments) and summative assessments (exams, projects) to measure knowledge and skill acquisition.

Continuously evaluate and improve the curriculum based on feedback from students, educators, and industry stakeholders.

8. Continuous Updating:

Cyber security is a rapidly evolvingfield, so ensure that the curriculum remains up to date with the latest industry trends, emerging threats, and technologies.

Establish mechanisms to monitor and incorporate new developments in the curriculum on an ongoing basis.

Figure 1. Steps for Curriculum Development (Casey 2008)

Table 1. Curriculum for Cyber Security in MET
Table: Specification of minimum standard of competence for officers in charge of ship cyber security or designated duty officers in a periodically cyber security of ship

Function: Cyber Security at the operational level / management level

Competence	Knowledge, understanding and proficiency	Methods for demonstrating competence	Criteria for evaluating competence
1. Knowledge of Cyber Threat Landscape:	• Understand the types of cyber threats faced by the maritime sector, including malware, social engineering, phishing attacks, and insider threats. • Identify emerging cyber threats and stay updated on the evolving threat landscape.	• Written exams: Assess students' understanding of different types of cyber threats and their characteristics through written exams that include multiple-choice questions, short answers, and essays. • Research papers: Assign research papers where students explore and analyze current and emerging cyber threats in the maritime sector, providing in-depth knowledge and insights.	• Accuracy and depth of knowledge regarding different types of cyber threats in the maritime sector. • Understanding of the characteristics, vectors, and potential impact of cyber threats. • Ability to explain the relevance of cyber threats to the maritime industry.
2. Understanding Maritime Cyber Systems:	• Gain knowledge of the different cyber systems used in the maritime industry, such as navigation systems, communication systems, propulsion systems, and cargo management systems. • Comprehend the vulnerabilities and potential risks associated with these systems.	• Practical demonstrations: Organize practical sessions where students can interact with different maritime cyber systems, understand their functionalities, and identify potential vulnerabilities. • Case studies: Present real-life case studies of cyber incidents in the maritime domain and ask students to analyze the impact on maritime cyber systems and propose preventive measures.	• Proficiency in explaining the functionalities and components of maritime cyber systems. • Identification of vulnerabilities and potential risks associated with specific maritime cyber systems. Application of knowledge to analyze the potential impact of cyber threats on maritime operations.
3. Cyber Risk Assessment and Management:	• Learn to conduct cyber risk assessments to identify potential vulnerabilities and assess the potential impact of cyber threats on maritime operations. • Develop skills to implement risk mitigation strategies and controls to minimize cyber risks.	• Risk assessment exercises: Provide hypothetical scenarios or real-world examples where students conduct cyber risk assessments, identify vulnerabilities, assess risks, and develop risk mitigation strategies. • Risk management projects: Assign individual or group projects where students develop comprehensive cyber risk management plans for specific maritime systems, including risk identification, analysis, and mitigation strategies.	• Ability to conduct effective cyber risk assessments, identifying vulnerabilities and assessing risks. • Development of comprehensive risk mitigation strategies and controls. • Understanding of risk management principles and their application in the maritime context.

4. Technical Security	– Network Security: • Understand the principles and best practices of securing maritime networks, including firewalls, intrusion detection systems, secure configurations, and access controls. Gain knowledge of network segmentation and isolation techniques to prevent unauthorized access and protect critical systems. – Security of Industrial Control Systems (ICS): • Understand the unique security challenges associated with ICS used in the maritime industry, such as SCADA (Supervisory Control and Data Acquisition) systems and onboard automation systems. Learn to implement security measures to protect ICS from cyber threats and potential disruptions.	– Network Security: • Network security simulations: Use network simulation tools or virtual environments to create scenarios where students configure and secure maritime networks, implement firewalls, and manage access controls. • Practical exercises: Assign hands-on exercises where students demonstrate their ability to secure network devices, configure security protocols, and detect and respond to network security incidents. – Security of Industrial Control Systems (ICS): • ICS security assessments: Provide opportunities for students to assess the security of ICS used in the maritime industry by identifying vulnerabilities, analyzing attack vectors, and recommending security measures. • Practical lab exercises: Set up hands-on lab sessions where students configure and secure ICS components, apply patches, and implement access controls to protect industrial control systems.	– Network Security: • Competence in configuring and securing maritime networks, including firewalls, access controls, and secure configurations. • Ability to detect and respond to network security incidents. • Understanding of network segmentation and isolation techniques for improved security. – Security of Industrial Control Systems (ICS): • Proficiency in assessing the security of maritime ICS components and systems. • Ability to recommend and implement security measures for protecting ICS in the maritime industry. • Understanding of best practices for securing and monitoring ICS in the maritime context.
5. Incident Detection and Response:	• Learn techniques for detecting and responding to cyber incidents in the maritime domain, including incident handling procedures, incident classification, and incident escalation processes. • Develop skills to effectively contain, investigate, and mitigate cyber incidents to minimize the impact on maritime operations.	• Incident response simulations: Conduct simulated cyber-security incident scenarios, where students demonstrate their ability to detect, analyze, and respond to incidents using incident response procedures and tools. • Incident response plans: Assign students to develop detailed incident response plans that outline steps to be taken in different types of cyber security incidents, including containment, investigation, and recovery.	• Capability to identify and classify different types of cyber security incidents in the maritime domain. • Application of incident handling procedures, including containment, investigation, and recovery. • Effective decision-making and response coordination during simulated incident scenarios.
6. Security Awareness and Training:	• Promote a culture of cyber security awareness among maritime personnel, including the recognition of social engineering techniques, phishing attacks, and safe online practices.	• Awareness campaigns: Assign students to develop cyber-security awareness campaigns targeting maritime personnel, including informative posters, educational videos, or interactive workshops.	• Demonstration of knowledge and understanding of social engineering techniques, phishing attacks, and safe online practices. • Effective communication of cyber security awareness messages to maritime personnel.

6. Security Awareness and Training:	• Provide training on how to respond to potential cyber security incidents and report suspicious activities.	• Phishing simulations: Conduct simulated phishing exercises to assess students' ability to recognize and respond appropriately to phishing emails, educating them about potential social engineering threats.	• Ability to respond appropriately to potential cyber security incidents and report suspicious activities.
7. Regulatory Compliance:	• Familiarize oneself with relevant international and national regulations and guidelines concerning maritime cyber security, such as the International Maritime Organization (IMO) guidelines and industry standards. • Understand the requirements for cyber security audits, compliance assessments, and reporting.	• Compliance audits: Assign students to conduct mock cyber-security audits to assess compliance with relevant regulations, standards, and guidelines, evaluating adherence to established security practices. • Compliance reports: Ask students to prepare reports or presentations summarizing the key cyber-security compliance requirements and how they apply to the maritime industry.	• Understanding of relevant international and national regulations, guidelines, and standards for maritime cyber security. • Knowledge of compliance requirements for cyber security audits, assessments, and reporting. • Adherence to established cyber-security practices in accordance with regulatory frameworks.
8. Ethical and Legal Considerations:	• Develop an understanding of ethical and legal issues related to cyber security in the maritime sector, including privacy, data protection, intellectual property, and international legal frameworks.	• Ethical case studies: Present ethical dilemmas related to cyber security in the maritime sector and ask students to analyze the situation, evaluate options, and propose ethical solutions. • Legal research projects: Assign research projects where students explore legal frameworks related to maritime cyber security and present findings on the implications for industry practices.	• Ability to analyze and evaluate ethical and legal issues related to cyber security in the maritime sector. • Understanding of privacy, data protection, intellectual property, and international legal frameworks. • Application of ethical decision-making principles in addressing cyber security challenges.
9. Cyber-Security Incident Exercise and Simulation:	• Participate in hands-on exercises and simulations to apply knowledge and skills in responding to simulated cyber security incidents in a realistic maritime environment. • Gain practical experience in incident handling, decision-making, and collaboration with relevant stakeholders.	• Tabletop exercises: Conduct tabletop exercises simulating cyber security incidents in the maritime context, allowing students to practice their incident response skills and decision-making abilities in a controlled environment. • Post-exercise analysis: Facilitate debriefing sessions where students reflect on their performance during incident simulations, identify areas for improvement, and propose strategies to enhance incident response capabilities.	• Effective participation and performance in simulated cyber-security incident scenarios. • Application of incident response procedures, decision-making, and collaboration with relevant stakeholders. • Reflection on post-exercise analysis, identification of areas for improvement, and proposed strategies for enhancing incident response capabilities.

being of seafarers. STCW code defines standards and requirements for international maritime education, training, and certification in the specific tables for the purpose how seafarers gain skill and competence regarding professionalism. Accordingly, in this study, by setting the STCW table for cyber security in MET, a model is created for the purpose of defining specification of minimum standard of competence for officers in charge of ship cyber security or designated duty officers in a periodically cyber security of ship. The table includes columns regarding “competence”, “knowledge, understanding, and proficiency”, “methods for demonstrating competence”, and “criteria for evaluating competence” under a function.

Accordingly, in this study, the curriculum for cyber security in MET is developed by utilizing STCW code table as in Table 1. In this context, in order to develop the columns regarding “competence”, “knowledge, understanding, and proficiency”, “methods for demonstrating competence”, and “criteria for evaluating competence” for maritime cyber security, both DNV-GL class guideline for cyber secure[3], international security standards[4,5,6], the NIST Cyber Security Framework (NIST 2018), and other codes of best practices for maritime cyber security[2, 8] (Boyes & Isbell 2017) are taken as references.

AHP Analysis

Thomas Saaty (1980) created the Analytic Hierarchy Process (AHP) for use in the military, and it is a representation of the hierarchical structure of a system. As shown in Figure 2, the factors are summarized in a hierarchy that is built by several levels according to the system's objective. These levels include the breakdown of the main goal into a collection of classes and subclasses, and the ultimate level. Class in a hierarchy is an attribute or criterion, while a subclass is referred to as a subcriterion or subattribute. In a multi criterion decision making (MCDM), the options are included in the highest tier of the tree. The interactive nature of the

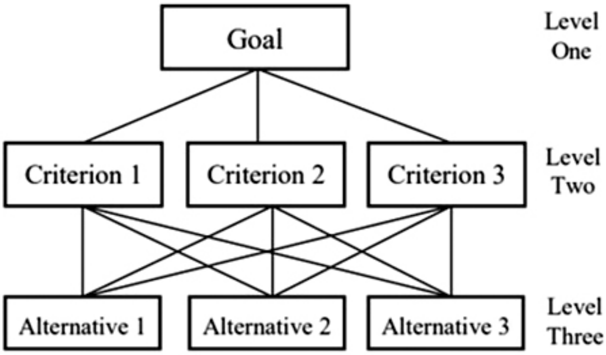
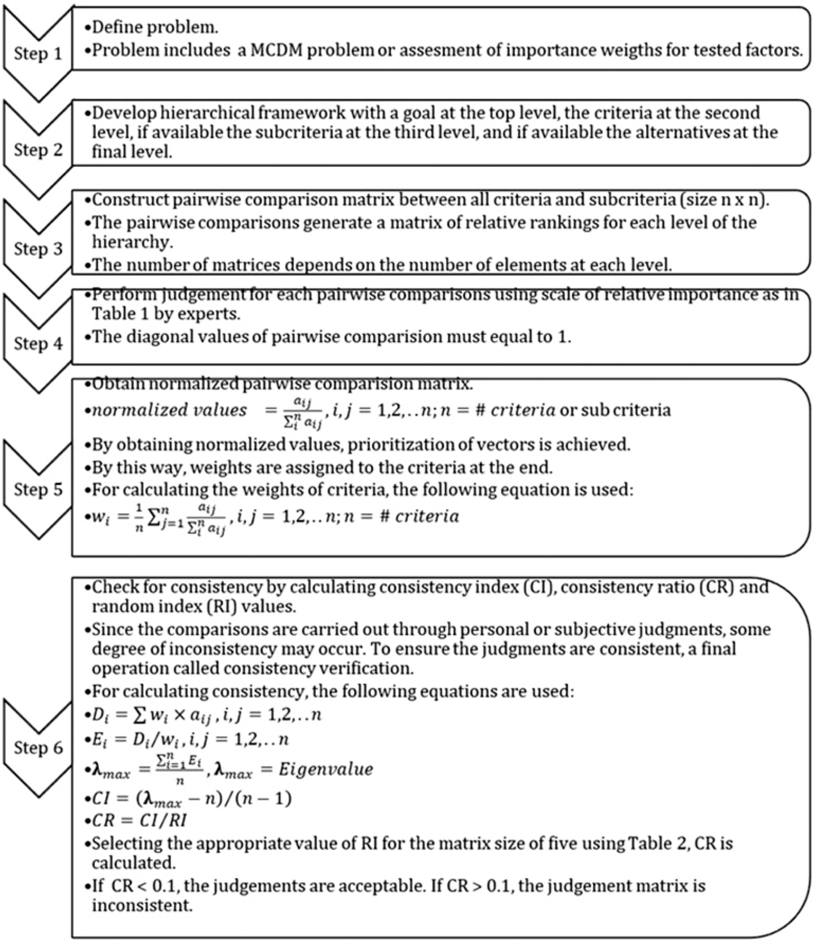


Figure 2. Sample Hierarchical Structure for AHP (Taherdoost 2018)

solution process for various, objective programming formulations makes AHP a common choice as the methodological procedure. Experts compare criteria and options by comparing them head-to-head (Taherdoost 2018).

The AHP is meant to use expert judgment to give relative importance to the various elements under consideration. In this approach, components are given relative importance in order to achieve two distinct goals. To begin, AHP is used to rank the factors and isolate the most important ones. It is useful for setting up directional metrics, notably in business. Second, by zeroing in on the most important metrics, more informed business decisions can be made, more correct information



Step 1

- Define problem.
- Problem includes a MCDM problem or assesment of importance weigths for tested factors.

Step 2

- Develop hierarchical framework with a goal at the top level, the criteria at the second level, if available the subcriteria at the third level, and if available the alternatives at the final level.

Step 3

- Construct pairwise comparison matrix between all criteria and subcriteria (size n x n).
- The pairwise comparisons generate a matrix of relative rankings for each level of the hierarchy.
- The number of matrices depends on the number of elements at each level.

Step 4

- Perform judgement for each pairwise comparisons using scale of relative importance as in Table 1 by experts.
- The diagonal values of pairwise comparision must equal to 1.

Step 5

- Obtain normalized pairwise comparision matrix.
- $normalized\ values\ = \frac{a_{ij}}{\sum_i^n a_{ij}}, i, j = 1,2,..n; n = \#\ criteria$ or sub criteria
- By obtaining normalized values, prioritization of vectors is achieved.
- By this way, weights are assigned to the criteria at the end.
- For calculating the weights of criteria, the following equation is used:
- $w_i = \frac{1}{n}\sum_{j=1}^n \frac{a_{ij}}{\sum_i^n a_{ij}}, i, j = 1,2,..n; n = \#\ criteria$

Step 6

- Check for consistency by calculating consistency index (CI), consistency ratio (CR) and random index (RI) values.
- Since the comparisons are carried out through personal or subjective judgments, some degree of inconsistency may occur. To ensure the judgments are consistent, a final operation called consistency verification.
- For calculating consistency, the following equations are used:
- $D_i = \sum w_i \times a_{ij}, i, j = 1,2,..n$
- $E_i = D_i / w_i, i, j = 1,2,..n$
- $\boldsymbol{\lambda}_{max} = \frac{\sum_{i=1}^n E_i}{n}, \boldsymbol{\lambda}_{max} = Eigenvalue$
- $CI = (\boldsymbol{\lambda}_{max} - n)/(n-1)$
- $CR = CI/RI$
- Selecting the appropriate value of RI for the matrix size of five using Table 2, CR is calculated.
- If CR < 0.1, the judgements are acceptable. If CR > 0.1, the judgement matrix is inconsistent.

Figure 3. Flowchart for A HP Methodology (Bolat et al. 2020)

for commercial operations can be decided, and more reliable assessments of different marketing tactics can be made (Cheng & Li 2001).

Figure 3 shows a flowchart depicting the processes of AHP implemented in this paper (Bolat et al. 2020).

An AHP Analysis for the Framework of the Curriculum for Cyber Security in the MET System

In this study, for data collection, opinions of five experts in maritime cyber security are used. The evaluation is made according to the Saaty's scale (1-9) for pairwise comparisons stated in (Bolat, et al. 2020). For analysis, experts' scores are averaged.

Step 1: Identify the criteria and alternatives

Criteria:

- Relevance to the maritime industry (1)
- Importance for ensuring cyber security (2)
- Feasibility of implementation (3)
- Potential impact on operations (4)
- Alignment with regulatory requirements (5)

Alternatives:

- Knowledge of Cyber Threat Landscape (1)
- Understanding Maritime Cyber Systems (2)
- Cyber Risk Assessment and Management (3)
- Network Security (4)
- Incident Detection and Response (5)
- Security of Industrial Control Systems (ICS) (6)
- Security Awareness and Training (7)
- Regulatory Compliance (8)
- Ethical and Legal Considerations (9)
- Cyber Security Incident Exercise and Simulation (10)

Step 2: Create a pairwise comparison matrix

Using a scale of 1-9, where 1 means equal importance and 9 means extremely important, a pairwise comparison matrix for the criteria are created as below:

Criteria

	1	2	3	4	5
1	1	3	5	5	3
2	1/3	1	3	3	1
3	1/5	1/3	1	3	1
4	1/5	1/3	1/3	1	1
5	1/3	1	1	1	1

Step 3: Calculate the priority vector for the criteria

The priority vector for the criteria is created by normalizing the values in each column and then taking the average of the rows:

Criteria	Priority Vector
1	0.453
2	0.276
3	0.114
4	0.086
5	0.071

Step 4: Create pairwise comparison matrices for each alternative

Using the same scale of 1-9, pairwise comparison matrices for each alternative is created:

Alternative 1: Knowledge of Cyber Threat Landscape

Competence

	1	2	3	4	5	6	7	8	9	10
1	1	3	7	5	5	3	7	5	3	3
2	1/3	1	5	3	3	1	5	3	1	1
3	1/7	1/5	1	3	3	1	3	3	1	1
4	1/5	1/3	1/3	1	3	1	5	3	1	1
5	1/5	1/3	1/3	1/3	1	1	3	3	1	1
6	1/3	1	1	1	1	1	3	3	1	1
7	1/7	1/5	1/3	1/5	1/3	1/3	1	1	1	1
8	1/5	1/3	1/3	1/3	1/3	1/3	1	1	1	1
9	1/3	1/1	1/1	1/1	1/1	1/1	1	1	1	1
10	1/3	1/1	1/1	1/1	1/1	1/1	1	1	1	1

Step 5: Calculate the priority vectors for each alternative

The values in each column of the pairwise comparison matrices are normalized for each alternative and then the average of the rows is calculated to obtain the priority vectors:

– Alternative 1: Knowledge of Cyber Threat Landscape

➢ Priority Vector: [0.210, 0.087, 0.047, 0.047, 0.047, 0.047, 0.047, 0.037, 0.037, 0.037]

Step 6: Calculate the weighted sum of each alternative

The priority vector of each alternative is multiplied by the corresponding priority vector of the criteria, and the results are summed:

– Alternative 1: Knowledge of Cyber Threat Landscape

➢ Weighted Sum: (0.210 * 0.453) + (0.087 * 0.276) + (0.047 * 0.114) + (0.047 * 0.086) + (0.047 * 0.071) = 0.106

Step 7: Calculate the relative weights of each alternative

The weighted sum of each alternative is divided by the sum of all weighted sums:

➢ Relative Weight of Alternative 1: (Weighted Sum of Alternative 1) / (Sum of Weighted Sums)

All above-mentioned steps for each alternative (2 to 10) is repeated.

Step 8: Results of the AHP analysis for each alternative

– Alternative 1: Knowledge of Cyber Threat Landscape
➢ Relative Weight: 0.106
– Alternative 2: Understanding Maritime Cyber Systems
➢ Relative Weight: 0.067
– Alternative 3: Cyber Risk Assessment and Management
➢ Relative Weight: 0.089
– Alternative 4: Network Security
➢ Relative Weight: 0.125
– Alternative 5: Incident Detection and Response
➢ Relative Weight: 0.137
– Alternative 6: Security of Industrial Control Systems (ICS)
➢ Relative Weight: 0.068
– Alternative 7: Security Awareness and Training
➢ Relative Weight: 0.090
– Alternative 8: Regulatory Compliance
➢ Relative Weight: 0.125
– Alternative 9: Ethical and Legal Considerations
➢ Relative Weight: 0.063
– Alternative 10: Cyber Security Incident Exercise and Simulation
➢ Relative Weight: 0.130

Results

By comparing the relative weights of each alternative, their prioritization in the curriculum for cyber security in the MET system is determined. Based on the analysis, the alternatives are ranked as follows:

1. Incident Detection and Response (Relative Weight: 0.137)
2. Cyber Security Incident Exercise and Simulation (Relative Weight: 0.130)
3. Network Security (Relative Weight: 0.125)
4. Regulatory Compliance (Relative Weight: 0.125)
5. Security Awareness and Training (Relative Weight: 0.090)
6. Cyber Risk Assessment and Management (Relative Weight: 0.089)
7. Knowledge of Cyber Threat Landscape (Relative Weight: 0.106)
8. Security of Industrial Control Systems (ICS) (Relative Weight: 0.068)
9. Understanding Maritime Cyber Systems (Relative Weight: 0.067)
10. Ethical and Legal Considerations (Relative Weight: 0.063)

These rankings provide guidance on the relative importance and priority of each alternative in the curriculum, allowing for informed decision-making during the curriculum design process.

3. Conclusion

As the ongoing digital change persists and even quickens, so too will the sector's changing educational requirements. Cyber risk management is a fundamental part of this. Although the International Maritime Organization (IMO) and others have taken action to increase the industry's ability to deal with this threat, the preparation of seafarers to fulfill their duties remains vital to any effective response. Many in the shipping sector will need to upgrade their knowledge and expertise to keep the industry safe and secure.

Getting the word out and raising awareness about this is a major obstacle. The current cyber skills gap may be the first sign of a future skills landscape that is increasingly data- and automation-driven.

It takes a lot of work to prepare an industry to deal with threats it has never encountered before. While technology advancement is essential for mitigating these threats, a shift in mindset is also required to guarantee these challenges receive the resources and attention they need. As a result, there exist gaps in knowledge and expertise as a result of the industry's changing educational requirements. Those currently employed in the field have many responsibilities and little spare time to devote to additional education. Time constraints need adaptability in the methods used, yet the results must be substantial.

In this study, a curriculum for maritime cyber security is proposed under STCW code by using exist literature, regulations, national and international standards, and incidents about maritime cyber security. Then, determined competences in curriculum for maritime cyber security are compared by using Analytic Hierarchical Process (AHP) method for determining prioritizations of the competences in the curriculum for cyber security in the MET system. These rankings provide guidance on the relative importance and priority of each competence in the curriculum, allowing for informed decision-making during the curriculum design process. The output of the study enables the MET Institutions to be proactive and include cyber security information and skills in the curriculum proposals.

Seafarers and others in the maritime industry will need to adapt to a new reality in which vessels are increasingly autonomous. Many of the cyber-security education programs and approaches outlined here might be considered as a "dry run" for the more substantial shifts that will occur in the coming years.

NOTES

1. ABET, 2022. ABET Approves Accreditation Criteria for Undergraduate Cybersecurity Programs. Web site. Available from: https://www.abet.org/abet-approves-accreditation-criteria-for-undergraduate-cybersecurity-programs/.
2. ANSSI, 2015. Managing Cybersecurity for Industrial Control Systems. Web site. ANSSI. Available from: https://www.ssi.gouv.fr/en/guide/managing-

cybersecurity-for-industrial-control-systems/. FRANCE: French Network and Information Security Agency. Web site. Available from: https://www.ssi.gouv.fr/uploads/2014/01/Managing_Cybe_for_ICS_EN.pdf.

3. DNVGL, 2020. DNVGL-CG-0325 Cyber Secure.
4. IEC 62443-3, 2008. Security for Industrial Process Measurement and Control. Network and System Security. BS IEC British Standard.
5. ISO/IEC 27001, 2017. Information technology - Security techniques - Information security management systems – Requirements (ISO/IEC 27001:2013 including Cor 1:2014 and Cor: 2:2015).
6. ISO/IEC 27033-3, 2010. Information Technology; Security Techniques; Network Security Part 3: Reference networking scenarios – Threats, design techniques and control issues. BS ISO/IEC British Standard.
7. STCW 2010, 2010. Standards of Training Certification and Watchkeeping.
8. THE FINNISH SHIPOWNERS' ASSOCIATION, 2021. Maritime Cybersecurity – Best Practices For Vessels. Web site. Finnish National Emergency Supply Organization, The Maritime Transport Pool. Available from: https://www.huoltovarmuuskeskus.fi/files/a9cb864dbec0780649661775ea66b6f1db076efb/cybersecurity-best-practices-for-vessels.pdf.
9. UNITED STATES COAST GUARD ACADEMY, 2022. Cyber Systems. Web site. United States Coast Guard Academy. Available from: https://uscga.edu/academics/majors/cysys/.
10. U.S. NAVAL ACADEMY, 2020. USNA Cyber Operations Program Granted NSA Designation. Web site. U.S. Naval Academy. Available from: https://www.usna.edu/NewsCenter/2020/11/USNA_CYBER_OPERATIONS_PROGRAM_GRANTED_NSA_DESIGNATION.php.

Acknowledgement

This study is supported by Maritime Security and Cyber Threats Research Laboratory at Istanbul Technical University Maritime Faculty in Turkey.

REFERENCES

BOLAT, P.; KAYISOGLU, G.; GUNES, E.; KIZILAY, F. E. & OZSOGUT, S., 2020. Weighting Key Factors for Port Congestion by AHP Method. *Journal of ETA Maritime Science*, vol. 8, no. 4, pp. 252 – 273. Available from: https://doi.org/10.5505/jems.2020.64426.

BOYES, H. & ISBELL, R., 2017. *Code of Practice: Cyber Security for Ships*. United Kingdom: Institution of Engineering and Technology. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642598/cyber-security-code-of-practice-for-ships.pdf.

CASEY, J. N., 2008. *Educational Curricula*. N.Y.: Nova Publishers.

CHENG, E. W. & LI, H., 2001. Analytic hierarchy process. *Measuring Business Excellence*, vol. *5,* no. 3, pp. 30–37. Available from: https://doi.org/10.1108/eum0000000005864.

HAREIDE, O. S.; JØSOK, Y.; LUND, M. S.; OSTNES, R. & HELKALA, K., 2018. Enhancing Navigator Competence by Demonstrating Maritime Cyber Security. *Journal of Navigation*, vol. *71, no.* 5, pp. 1025 – 1039. Available from: https://doi.org/10.1017/s0373463318000164.

HEERING, D.; MAENNEL, O. & VENABLES, A. N., 2021. Shortcomings in cybersecurity education for seafarers. *Developments in Maritime Technology and Engineering*, no. 1, pp. 49 – 61. Available from: https://doi.org/10.1201/9781003216582-6.

NIST, 2018. Framework for Improving Critical Infrastructure Cybersecurity. In: *Proceedings of the Annual ISA Analysis Division Symposium*, vol. 535, pp. 9–25.

SAATY, T. L., 1980. *The Analytic Hierarchy Process*.

SCANLAN, J.; HOPCRAFT, R.; COWBURN, R.; TROVÅG, J. M. & LÜTZHÖFT, M., 2022. Maritime Education for a Digital Industry. *NECESSE. Royal Norwegian Naval Academy. Monographic Series*, vol. 7, no. 1, pp. 24 – 34.

SHAPO, V. & LEVINSKYI, M., 2020. Means of Cyber Security Aspects Studying in Maritime Specialists Education. *Internet of Things, Infrastructures and Mobile Applications*, pp. 389 – 400. Available from: https://doi.org/10.1007/978-3-030-49932-7_38.

TAHERDOOST, H., 2018. Decision Making Using the Analytic Hierarchy Process (AHP); A Step by Step Approach. *International Journal of Economics and Management Systems*, no. 2, pp. 244 – 246.

✉ **Dr. Gizem Kayisoglu**
ORCID iD: 0000-0003-2730-9780
Istanbul Technical University
Istanbul, Turkey
E-mail: yukselg@itu.edu.tr

Dr. Pelin Bolat, Assoc. Prof.
ORCID iD: 0000-0003-4262-3612
Scopus Author ID: 55568241400
Istanbul Technical University
Istanbul, Turkey

Dr. Emre Duzenli
Istanbul Technical University
Istanbul, Turkey