TRANSNAV the International Journal on Marine Navigation and Safety of Sea Transportation
http://www.transnav.eu
Volume 16
Number 2
June 2022

DOI: 10.12716/1001.16.02.15

A Multiple Case Study of METI Cybersecurity Education and Training: A Basis for the Development of a Guiding Framework for Educational Approaches

J. Bacasdoon[1] & J. Bolmsten[2]
[1] *Maritime Academy of Asia and the Pacific, Mariveles Bataan, Philippines*
[2] *World Maritime University, Malmoe, Sweden*

ABSTRACT: Cyberattacks have become a serious global concern, effecting enormous losses to different sectors. In the shipping business, major companies report violations to their operations' integrity and security, and losing great amounts of money. While the International Maritime Organization (IMO), through the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) 1978, as amended, is yet to release a standard for the cybersecurity education and training of seafarers, some maritime education and training institutions (METIs) have acted proactively and included cybersecurity knowledge and skills in their curricular offerings. This study looked into the cybersecurity course offerings of four METIs that served as the case studies of the researchers. In particular, the following objectives were addressed: the cybersecurity knowledge and skills included in their curriculum; the importance of the cybersecurity knowledge and skills to seafarers; and the educational approaches of the METIs in delivering their topics on cybersecurity. The first and third objectives were answered using different sources of qualitative data, including document analysis, interview and direct observation. The quantitative approach, in the form of a survey questionnaire, was used to address the second objective. The METIs, though not the same in content, were found to have included cybersecurity knowledge and skills in their curriculum. These knowledge and skills were perceived to be very important by seafarers. Similar to the content of their courses, the METIs delivered their cybersecurity courses by employing varied educational approaches. To address the gap on the lack of cybersecurity course design and delivery minimum standards, a framework in the shape of a lantern is developed and proposed to guide maritime courses designers, in particular, and other course designers, in general.

1 INTRODUCTION

With the increasing dependence on technology-driven operational systems and equipment, security and operations are exposed to different risks. The ever-evolving technology applications and digital systems in an interconnected shipping industry present high vulnerability to cyber-attacks (Kala & Balakrishnan, 2019). Notably, the development of cybersecurity measures should be inextricably linked to technological advancements. However, the maritime domain is several years behind other computer-based industries (Karahalios, 2020) and has failed in prioritising cybersecurity (Caponi & Belmont, 2015). Some of the largest shipping companies were victims of cyber-attacks. In particular, Morgan (2020) highlighted the possible amount of damage of USD 6 trillion by the end of 2021 up to USD 10.5 trillion annually in 2025.

With such increasing concern on maritime cybersecurity, the International Maritime Organisation (IMO) adopted Resolution MSC.428(98) and posted guidelines that provide recommendations

to facilitate appropriate cyber risk management for vessel owners and operators. However, the International Convention on Standards of Training, Certification, and Watchkeeping for Seafarers (STCW) 1978 Convention, as amended, is struggling to keep pace with the technological changes taking place in the maritime industry (Heering et al., 2021), particularly that its current edition does not include anything about cybersecurity. While cybersecurity awareness and training are important to the maritime industry (Androjna et al., 2020), there is a dearth of evidence indicating the gaps and issues in cybersecurity education and training for seafarers. Some of the studies are the works of (Tam et al., 2021) and (Daum, 2019) providing preliminary recommendations for maritime cybersecurity training. Heering et al. (2021) argue that it is necessary to include cybersecurity awareness training into the MET programmes of all specialties.

While seafarers are critical to the success of the attacks because they are a significant vulnerability element for ships, they can also serve as a "human firewall" and protect the ship if they are trained well (Mraković & Vojinović, 2019). As seafarers play significant roles to maintain cybersecurity onboard ships, training and education is vital. This study reviews and examines the cyber security knowledge and skills needed for seafarers and examines the educational approaches to maritime cybersecurity.

Since cybersecurity is a global issue, it is therefore essential that the maritime industry raise cybersecurity awareness and impart skills that will enable the seafarers to avoid catastrophic mistakes while using the internet and other information technology devices and systems onboard the ship. However, apart from the IMO's cybersecurity guidelines, the specific knowledge and skills required of seafarers are not yet well defined.

In 2018, the International Association of Maritime Universities (IAMU)'s project "Addressing Cyber Security in Maritime Education and Training" (CYMET) (Ahvenjärvi, 2018) found out that none of the ten European maritime universities in their study offered courses in maritime cybersecurity. Currently, Maritime Education and Training Institutions (METI) have the freedom to choose which topics on cybersecurity to teach and educate their students and trainees. When it comes to course delivery, METIs employ their own approaches.

This research is a multiple case study of four METIs on the cybersecurity courses and their educational approaches. This article is based on the dissertation research of Bacasdoon (2021) at the World Maritime University (WMU).

The research methodology aimed to answer the following questions:
Question 1: What are the cybersecurity knowledge and skills taught by METIs?
Question 2: How do seafarers perceive the importance of cybersecurity knowledge and skills?
Question 3: How may the educational approaches employed by METIs in delivering their cybersecurity courses be described and optimised?

Section Two focuses on the educational approaches and its aspects and how these aspects formulated the analytical framework that was used in this study. Section Three includes the research methodology and methods used and an overview of the data collection and data analysis methods. The data findings, analyses, and discussions are presented in Section Four for cybersecurity knowledge and skills and Section Five for educational approaches. Section Six concludes the study, makes recommendations for METIs and other maritime stakeholders and identifies suggested research areas for future consideration.

2 THE CYBERSECURITY EDUCATIONAL FRAMEWORK

This section contains the operational and theoretical discussion of concepts included as variables of the study. These concepts are explained with the intention of showing how they relate with one another to develop the analytical framework, as illustrated at the end of this section. The discussion ventures into the different aspects of the educational approach developed in this study namely Cybersecurity knowledge and skills topics, Teaching/learning activities (TLA), Modality, Instructor-led and self-learning, Assessment, and Tools and equipment, and how they are related, and used for the formulation of the analytical framework. Although not included in the analytical framework, Target group and Course level, aim, and Intended Learning Outcome (ILO) are also presented to give context to the educational approaches. The analytical framework is then presented which will serve as the basis in the analysis of the empirical research in Section 5.

2.1 *Target group*

A target group of a course is the target learners whom the course is intended to be delivered. It is important to adapt the teaching methods to accommodate the target group of learners (Chicioreanu & Amza, 2018).

In the context of this study, the target group of a cybersecurity course are both present and future seafarers. These target groups can also be distinguished by level, rank or department. For the education and training of seafarers, some courses are specifically given depending on the department which is either deck, engine, galley or other departments found in passenger vessels. Seafarers, as the target group of learners, are also distinguished considering their level, which is either management, operational, or support level as stated in the STCW Convention 1978, as amended (IMO, 2017). On the other hand, target groups of future seafarers are usually distinguished based on their year level at the university.

2.2 *Course level, aim, and ILO*

(Light et al., 2009) distinguished between course aims, learning objectives and learning outcomes. Course aims originate from the perspective of the teacher, what he or she wants to achieve in the course. Learning objectives are under course aims; they describe what the students are expected to learn from

the course; learning outcomes are behavioral and specify what students need to actually demonstrate as a result of their learning experience. In this article, however, there is no distinction between the three. Course aims or outcomes are treated to be general statements while intended learning outcomes are broken down and more specific learning intentions based on the course outcomes.

In the design of course aims or outcomes, the programme outcomes, which are based on graduate attributes, should be referred to (Tang & Biggs, 2007). When this is done, the ILOs can be formulated based on the course outcomes. These course outcomes are broken down into ILOs by the instructors or the course developers.

An ILO describes what and how the student should learn (Tang & Biggs, 2007). Historically, developers and/or teachers used the term "objectives" to refer to these outcomes. Since the focus of the teaching-learning process is what the students do (Fry et al., 2008; Ramsden, 2003), it is better to formulate outcomes rather than objectives because outcomes are based on the students' perspective (Tang & Biggs, 2007).

Learning outcomes serve as a guide to teachers in deciding the TLA to facilitate and the assessments to be administered. Since learning outcomes are statements of course expectations to the students, they should be written from the students' perspective (Fry et al., 2008). Moreover, many course developers or teachers use Bloom's taxonomy as their guide in stating their ILOs. Tang and Biggs (2007), however, emphasize deep learning of students, meaning that outcomes to be formulated and translated in the TLA and assessments should focus on higher level of understanding for more important topics.

2.3 *Aspects of educational approach*

The research into educational approaches continues, and various theories of learning and their impact on these approaches have emerged. Theories include the relative merits of teacher-centered and student-centered perspectives of teaching and learning (Trigwell, 2006). They are referred to by some authors as instructed knowledge versus constructive knowledge (Hmelo-Silver et al., 2007; Scruggs & Mastropieri, 2007), explicit instruction versus minimally guided instruction (Kirschner et al., 2006), and traditional didactic instruction versus progressive methods (Adkisson & McCoy, 2006). The researcher took the factors of teacher and student and added the modality as another element of educational approach, as explored by Smith et al. (2006) and deLeon and Killian (2000), as well as the TLA, assessment by Biggs (2003), the use of tools and equipment (Murati & Ceka, 2017), and the cybersecurity knowledge and skills. They are presented as aspects of educational approach in this study which form part of the constructed analytical framework.

2.3.1 *Cybersecurity knowledge and skills topics*

In terms of cybersecurity knowledge and skills, this research relates to that of Bloom's Taxonomy which supports the classical Knowledge, Skills, Attitude (KSA) learning structure, including its broad sense of overlapping cognitive (knowledge), psychomotor (skills) and affective (attitude) domains.

The knowledge domain encompasses both theoretical knowledge received from formal education, training, or certification and practical knowledge developed through hands-on exercise and use of tools, operational methods, and work processes (Chi, 2006). The term "cybersecurity knowledge level" refers to an individual's theoretical understanding of cyber risks, weaknesses, attack patterns, and their impact on a host system (Ani et al., 2019). Additionally, supplementary cybersecurity knowledge can aid in detecting damaging cyber events and reduce the number of safe cyber activities that are incorrectly classified as malicious (Ben-Asher & Gonzalez, 2015).

A skill is the collection of abilities, knowledge, and experience that makes an individual able to perform well on a particular task (Boyatzis & Kolb, 1991; Carlton et al., 2015; Levy, 2005). Cybersecurity skills, in particular, refer to the technical capability and knowledge of a person to use his experience and/or tools to recognize and mitigate cyber-attacks (Ani et al., 2019; Carlton et al., 2015; Choi et al., 2013). Thus, cybersecurity skills can assist users in making sound judgments and taking actions that reduce or eliminate the malicious events. Individuals' need for cybersecurity skills is, on the other hand, not limited to one profession or field (Burley et al., 2014).

Cybersecurity covers a broad spectrum of domains, spanning both technical (e.g. information, systems, network, and Internet security) and non-technical (e.g. policy, governance, ethical, and human/society concerns) (Irons, 2019). Rashid et al. (2018) argue that the foundation of cybersecurity knowledge is disconnected, resulting in both students and educators having problems plotting meaningful paths across the subject. Recognizing appropriate content and coverage can be challenging for both institutions offering courses and employers recruiting graduates (Furnell, 2021). While Furnell (2021) claims that there is a maturation of cybersecurity as a profession due to the emergence of frameworks for curriculum development, the same could not be claimed specifically in the maritime profession. As society and industry become increasingly dependent on cybersecurity, efficiency in cybersecurity education both in terms of content and delivery become critical. Similarly, as an integral component of cybersecurity education, it is necessary to consider what has to be learned and how learning takes place (Irons, 2019). This is one of the gaps that this study intends to fill.

2.3.2 *Teaching/learning activities*

According to Tang and Biggs (2007), after deciding on the best TLA for particular ILOs and having considered available resources and the size of the class, the following criteria should be met by the said TLAs:

- The students should feel responsible of their learning through a learning climate that encourages them to move freely, explore and decide on their own;

– The students see the tasks as relevant and they are positive to succeed at it;
– The task is built on prior knowledge;
– The task requires the learner to be actively involved; and
– The task allows the learner to reflect as he/she proceeds in the process.

2.3.3 *Modality*

Mode of delivery, or modality, according to Bates (2015) lies in the technology-based learning progress, from 'pure' face-to-face instruction to fully online learning. Bates (2015) identified the modes of delivery in the following categories:
– Classroom teaching (no technology);
– Blended learning (technology used as classroom aids; flipped classroom; hybrid of face-to-face and online delivery); and
– Fully online learning.

In fully online modality, it can be sub-classified into synchronous (live) and asynchronous (recorded). Malik et al. (2017) distinguished the two in terms of structure and time, stating that synchronous learning is constrained by structure and time, whereas asynchronous learning occurs when learners can study at their own pace and in their own time.

The researchers modified the model of Bates (2015), and added the sub-classification of online learning to classify the modality in the context of this research. This modification is shown in Figure 1.

Figure 1. Classification of modality based on the continuum of technology-based teaching of Bates (2015).

2.3.4 *Instructor-led and self-learning*

Instructor-led is a traditional approach that is very dynamic due to the instructor's presence to address possible queries or concerns and to attend to students individually (Wehr, 1988). Many researchers used instructor-led approach in their studies and compared it to computer-based training (CBT) (Wehr, 1988) and peer-led approach (Ha & Lim, 2018), student-led (Dillon & VanDeGrift, 2021), and self-directed practice (Schlesinger et al., 2021). All of these studies have one thing in common - the presence of instructor in teaching. On the other hand, the absence of assistance from others in the process of acquiring and retaining knowledge by an individual is defined in this work as self-learning approach.

Good teachers usually have a repository of strategies and materials to use in different circumstances. With continual education and trainings on the technological advancements, they will be able to facilitate activities that equip the students with the necessary knowledge and skills to address issues in their future areas of work like cybersecurity issues in the maritime field (Burrell et al., 2015). The role of the instructor is also critical in using technology-based tools and equipment (Salah et al., 2015) and in conduction exercises using simulators (Fisher & Muirhead, 2005).

2.3.5 *Assessment*

Assessment involves the analysis of systematically collected information (Stassen et al., 2001) and serves as a feedback mechanism and an avenue to improve learning (Baik et al., 2017; Stassen et al., 2001). Moreover, Stassen et al. (2001) add that because of assessment, the learning process becomes more effective, teachers become better and students are provided with systematic feedback.

Assessments are of different kinds and forms depending on the purpose and the intended learning outcome. The assessment administered to measure the knowledge of students is not the same with the assessment given to measure their skills. In the same manner, an assessment given before the delivery of a course or topic is unique from an assessment given during its delivery. From here, it can be said that assessment is not a standalone or an independent activity from the other elements of instruction. It has to be aligned with these other elements and it has to be in different forms to fit the different purposes of instruction (Chudowsky et al., 2001).

Different types of assessments can be administered depending on the requirement of the learning outcomes. Again, the learning outcomes are central to this process of teaching and learning because it gives direction on how and what assessment should be carried out.

2.3.6 *Tools and equipment*

There are various tools and equipment that are used in teaching cybersecurity. These tools and equipment include traditional classrooms for lectures and physical laboratory, and simulation laboratories for hands-on exercises, which can be maximized depending on the requirement of the topic and the learning outcome.

As distance learning courses are becoming more popular, technology-based tools that will work virtually are also in demand. Some of these include cloud-based platforms, which can facilitate course assignments and provide the needed hands-on experience to students (Salah et al., 2015). According to Xu et al. (2014), cloud-based laboratories affect the students positively when teaching cybersecurity. Another tool that is widely used in conjunction with online learning is the learning management system (LMS). LMS has features like self-learning (Chao & Chen, 2009) and can also act as a repository (Davis et al., 2009) for course materials, videos, and assessments.

2.4 *Relationship among the educational aspects*

Several curriculum development models are presented in the literature. They include rational models like Tyler and Taba (Läänemets & Kalamees-Ruubel, 2013). Cyclical models are also formulated by

Wheeler, and Nicholls and Nicholls (Palupi, 2018). A dynamic and interactive model was also presented by Print (1993). These curriculum development models, in one way or another, mention the connections and relationships of target group, general aim and ILO of the course, organization of content, TLAs, modality, instructor, assessment, and tools and equipment, which are all used as aspects of educational approach in this research.

2.5 *The analytical framework*

This study asserts that the mentioned aspects - topic, TLA, assessment, modality, instructor, and tools and equipment, should be present and complete in the course design and delivery of all METIs. The connections of these aspects are presented in some of the existing curriculum development models, though not as explicit to some.

With the thesis stated above, the researchers conceptualized an analytical framework to identify and evaluate the educational approach and its contribution to the attainment of the general aims of each METI's cybersecurity courses. The educational approach framework is composed of six distinct but interrelated components that were used to analyze the cybersecurity courses in this case study. The researchers postulate that each component establishes relationships and interacts with one another in such a way that either supports or undermines the attainment of the training courses' general aims, primarily depending on the presence, type, and consistency in interactions.

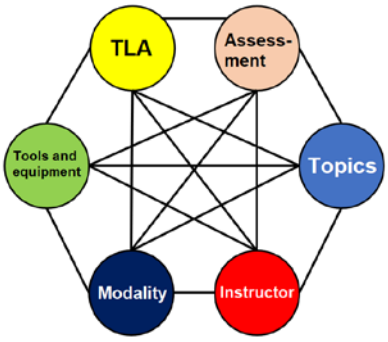

Figure 2. Analytical Framework of Strong Connection of the Aspects of Educational Approach.

To fully realize a training course's general aims, all the components present in a course, regardless if they are complete, should have positive relationships and interactions with all other components. One type of this educational approach is represented by a 'full lantern', where all six components are connected to each other with solid lines, as shown in Figure 2. Training objectives can likewise be achieved when each component establishes positive relationships with the other components and maintains this consistency across all possible interactions. However, an educational approach may or may not have all the identified components by design and still contribute to the attainment of the aims. This type of educational approach is described as an 'incomplete lantern', with each component connected by solid lines to as many other possible components, and one or more components completely disconnected from the rest. However, the choice of which component to omit is crucial in this regard. Table 1 summarizes the conditions for established relationships between each component. Unfulfilled conditions or not well-established relationships are represented by broken lines. Prior to establishing the relationships and forming the lantern, it should be noted that the starting point is the identification of target learners and the level of the course, and the formulation of general aim and learning outcomes.

Table 1. Pairing of Aspects of Educational Approach and the Conditions Establishing their Relationship.

Pair of aspects	Conditions for established relationship
Topics – TLA	If the topics can be delivered using the TLA
Topics – Modality	If the topics can be delivered using the modality
Topics – Instructor	If there is an instructor
Topics – Assessment	If an assessment is administered
Topics – Tools and equipment	If the topics can be delivered using the tools and equipment
TLA – Modality	If the TLA can be delivered using the modality
TLA – Instructor	If there is an instructor
TLA – Assessment	If an assessment is administered
TLA – Tools and equipment	If the TLA can be delivered using the tools and equipment
Modality – Instructor	If there is an instructor
Modality – Assessment	If an assessment can be administered through the modality
Modality – Tools and equipment	If tools and equipment can be used through the modality
Instructor – Assessment	If there is an instructor
Instructor – Tools and equipment	If there is an instructor
Assessment – Tools and equipment	If an assessment can be administered using the tools and equipment

2.6 *Section Summary*

Cybersecurity knowledge and skills, including its importance to seafarers, have been expounded to serve as the conceptual reference of the discussion of educational approach and its aspects in relation to course delivery. With the roles played by each aspect succinctly described, this section showed that all these aspects are interdependent of each other and that the absence or presence of each aspect affects the entire process delivering the course. With the use of research methods specified in Section 3, the interdependence is elaborated in Section 4 and Section 5.

The context in this study using these aspects is formed in this thought - that the effective use of TLAs, modality, instructor, assessment and tools and equipment to deliver the cybersecurity content will help in the attainment of the ILOs and the aim of the course in general to the target groups of METIs. Using these aspects of educational approach, the constructed analytical framework is used to structure the analysis and discussions in Section 5 to describe the educational approaches employed by METIs in delivering their cybersecurity courses.

3 RESEARCH METHODOLOGY AND METHODS

3.1 *Purpose and outline*

Studying METIs' educational approaches to cybersecurity education and training, as well as their course content and seafarers' perceptions of its importance, necessitates a real-world inquiry outside the laboratory (Robson & McCartan, 2016). Robson (2002) highlights the strength of mixed method approach which may yield both quantitative and qualitative data and explains both fixed and flexible research designs and how they can support each other. This research is a real-world inquiry that used a mixed method approach.

This section focuses on describing the research methodology and the specific methods used to conduct the research. It describes how the methods were employed to find answers to the research questions raised in Section 1. To recall, the present study worked on the following areas:

- Cybersecurity knowledge and skills taught by METIs;
- Perception of seafarers on the importance of cybersecurity knowledge and skills; and
- Educational approaches employed by METIs in teaching their cybersecurity courses.

3.2 *Methodological approach and rationale*

Bearman and Dawson (2013) argue that prior to selecting an appropriate research method, it is necessary to fully understand the philosophical conflict between two methodologies. However, Creswell and Creswell (2017) stated that relying solely on quantitative or qualitative research is viewed as insufficient and limiting. To resolve this, Flick (2018) stressed that the methodological triangulation approach assists in reinforcing one method with another and provides more grounded results. Therefore, this research utilized a combination of qualitative and quantitative methods, as derived from triangulation philosophy – an approach that also concurs with Johnson and Christensen (2019), who saw positive value in its application. Mixed-methods enabled the researchers to obtain seafarers' and METIs' perspectives on the cybersecurity knowledge and skills required of seafarers.

Data triangulation was used particularly in the qualitative approach in this research. It was conducted by utilizing multiple sources of evidence rather than a single source. According to Yin (2018), case studies that incorporated multiple sources of evidence received a higher rating for overall quality than those that relied solely on a single source of information. To apply, the qualitative method used in this study drew on a variety of sources, including semi-structured interviews, documentation, and direct observations, following a similar convergence, as illustrated in Figure 3.

Figure 3. Convergence of Multiple Sources of Evidence of Qualitative Method.

Qualitative method was used to obtain in-depth analysis and answer the research questions on cybersecurity knowledge and skills taught by METIs and their educational approaches in the delivery of their cybersecurity courses. On the other hand, a quantitative approach was used to answer the research question on the importance of cybersecurity knowledge and skills taught by METIs.

Figure 4 depicts the research approach and process of the study. Aside from answering research question 1 and research question 3, the data from the semi-structured interviews and documents were utilized to make the survey questionnaire to get the perception of seafarers about the importance of such cybersecurity knowledge and skills to answer research question 2. The use of NVivo aided qualitative data analysis, whereas Microsoft Excel aided quantitative data analysis.

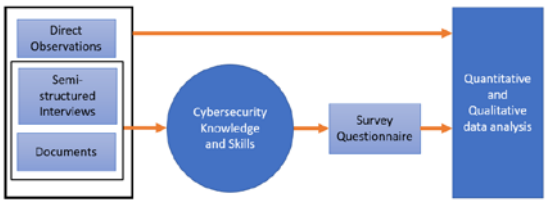

Figure 4. Research Approach and Process.

3.3 *Selection of participants*

The study made use of purposive sampling to determine the respondents of the study for both qualitative and quantitative research. Four METIs, which are regarded as premier providers of cybersecurity education and training to seafarers, were targeted cases. Additionally, this study surveyed seafarers as they are the end-users and key factors in maintaining cybersecurity onboard the ship. Determining their perception of how important cybersecurity knowledge and skills that are taught by METIs is significant in this study.

3.4 *Instrumentation and data collection*

3.4.1 *Semi-structured interview*

The researchers used interviews to answer research question 1 and research question 3. The respondents were selected based on the following criteria:

- Course developers
- Course instructors

– Persons in similar roles.

A semi-structured interview instrument was composed of three sections. The researchers intentionally chose the participants who are considered to give the required information on cybersecurity knowledge and skills taught by METIs. The questions in the interview guide targeted the cybersecurity knowledge and skills that they teach, and the educational approaches that they employed.

All interviews were transcribed and the generated cybersecurity knowledge and skills were used to create the online questionnaire for the survey.

3.4.2 *Documentation and direct observations*

The researchers gathered documents, which included curriculum documents, course syllabus and materials which aimed to answer research question 1 and research question 3. Furthermore, one of the researchers observed the delivery of classes (through recorded videos), visited the campuses and their equipment, and accessed their e-learning platforms. Direct observations aimed to answer research question 3.

3.4.3 *Self-administered questionnaire*

A self-administered survey questionnaire based on the semi-structured interviews and documents that aimed to find out how seafarers perceive the importance of cybersecurity knowledge and skills taught by METIs, was generated and distributed using Google Forms. Prior to distribution, the questionnaire was pilot tested to ten (10) World Maritime University (WMU) MSc in Maritime Affairs students, resulting in being fine-tuned. Additionally, the questionnaire was sent to 40 respondents for reliability testing, where its Cronbach's Alpha coefficient yielded excellent reliability for both cybersecurity knowledge (0.976) and skills (0.966).

After cleaning the data, there are 403 seafarers who are respondents in this study, as shown in Table 2. The majority of the respondents (62%) are below 31 years old. In terms of the department they work for, more than half of the respondents belong to the Deck Department (55%). In terms of training, less than half of the respondents (42%) have training experience in cybersecurity.

Table 2. Demographics

Age	n	%
Below 25	104	26
25-30	147	36
31-35	106	26
36-40	32	8
41-50	8	2
Above 50	6	1
Department		
Deck	221	55
Engine	178	44
Other	4	1
Training Experience		
NO	234	58
YES	169	42

Note: N = 403

3.5 *Data analyses*

3.5.1 *Qualitative data analysis*

The data gathered from the semi-structured interviews, documentations, and direct observations were analyzed using qualitative content analysis to generate insights into what cybersecurity knowledge and skills METIs teach and what educational approaches are employed in their courses. The researchers organized the data according to distinct themes. Typically, these themes corresponded to a single research question. For each theme, the researchers analyzed the interview and assigned codes to the responses. The researchers then attempted to fit the responses from the remaining interviews and documents into those codes. When the existing codes were found to be insufficient, a new one was added. For new codes, the researchers reviewed previous interviews to determine if any responses also fit this code. In the majority of cases, the codes were not mutually exclusive. As a result, an answer may be associated with one or more codes.

3.5.2 *Quantitative data analysis*

The quantitative data was analyzed using descriptive statistics that included the data for age, department and training experience, and the importance of cybersecurity knowledge and skills as perceived by seafarers.

3.6 *Section summary*

In this section, methods of quantitative and qualitative research were described and how the data of this study were collected and analyzed.

The following chapter presents the findings, analysis and discussion of cybersecurity knowledge and skills taught by METIs using a qualitative method. Additionally, the findings, analysis and discussions of the perception of importance of seafarers to such cybersecurity knowledge and skills are also presented using a quantitative approach. In section 5, the findings, analyses, and discussions using qualitative approach are presented to analyze the educational approaches used by METIs to deliver their cybersecurity courses.

4 CYBERSECURITY KNOWLEDGE AND SKILLS RESEARCH FINDINGS, ANALYSIS AND DISCUSSIONS

This section presents the cybersecurity knowledge and skills taught by METIs, which were identified as METI1, METI2, METI3, and METI4, from the qualitative data and their perceived importance by seafarers from the quantitative data, including their respective analyses.

The section is structured as follows:

– Cybersecurity knowledge and skills taught by METIs; and

– Seafarers' perception of importance to such cybersecurity knowledge and skills.

4.1 *Cybersecurity knowledge and skills taught by METIs*

Based on the document analyses and the interview with the four METIs, the two tables below reveal the cybersecurity knowledge and skills deemed necessary for seafarers and their perceived importance of the 403 seafarers.

Table 3 deals with the cybersecurity knowledge taught in the four METIs included as case studies in this research. As seen on the table, there were 29 cybersecurity knowledge included in the content of the courses being delivered by the METIs. It can also be noted from the table that some of the identified knowledge were common to the delivering institutions while some were tackled by one institution only. With an overall mean of 4.70, the cybersecurity knowledge taught by METIs were perceived to be very important by the seafarer respondents. Item number 12, which deals with the action during a cyber-attack had the highest mean of 4.80 with a descriptive equivalent of very important. On the other hand, digital forensics got the lowest mean of 4.42 with a descriptive equivalent of important.

In particular, only one out of the 29 knowledge items was common to all the four delivering institutions, itemNumber 22, which deals with the "cybersecurity rules, guidelines, standards, and legal frameworks developed for maritime sector." Five (5) items were part of the content of the deliveries of three institutions; eight (8) items were delivered by METI3 alone and seven (7) items were delivered by METI1 only.

Table 3. Cybersecurity Knowledge taught by selected METIs and their Importance as Perceived by Seafarers.

Cybersecurity Knowledge	Delivering Institution	Weighted Mean	Descriptive Equivalent
1. External cybersecurity threats to the ship	METI1, METI2, METI3	4.68	Very important
2. Internal cybersecurity threats posed by inappropriate use and poor cybersecurity practices	METI2, METI3	4.69	Very important
3. Consequences of a cybersecurity threat on onboard systems with direct and indirect communication links, including ship's IT and Operational Technology (devices, sensors, software and associated networking that monitor and control onboard systems)	METI3, METI4	4.72	Very important
4. How cyber risks can be reduced	METI1, METI2, METI3	4.75	Very important
5. How to respond to a cybersecurity breach or attack	METI1, METI3	4.73	Very important
6. The need for constant vigilance and reviews of the cyber risk management plan	METI3	4.66	Very important
7. Importance of each individual's role and how he/she can protect himself/herself and his/her organization against cyber security threats	METI3	4.78	Very important
8. Elements of Cybersecurity Management	METI2, METI3, METI4	4.61	Very important
9. Password and remote connection requests	METI1, METI4	4.73	Very important
10.Real-life cases of cyber incidents	METI1, METI2, METI3	4.74	Very important
11.Most common methods used by cyber attackers	METI1, METI3	4.68	Very important
12.What to do if you become a victim of a cyber-attack	METI3	4.80	Very important
13.What to do if your computer is infected by ransomware	METI1, METI3	4.78	Very important
14.Risks that can occur through overuse of smart phones, tablets, laptops and social media	METI3	4.71	Very important
15.How to achieve a healthy balance between work and leisure, offline and online	METI3	4.71	Very important
16.Best practices of cyber hygiene	METI1, METI3, METI4	4.66	Very important
17.How positive online behaviors can help to maintain concentration and focus while at work	METI3	4.68	Very important
18.Considerations to be made before posting on social media	METI3	4.73	Very important
19.Key steps to ensuring cybersecurity on board is maintained	METI3	4.72	Very important
20.Concept of security	METI1	4.72	Very important
21.Terminologies of cybersecurity	METI1, METI3	4.59	Very important
22.Cybersecurity rules, guidelines, standards, and legal frameworks developed for maritime sector	METI1, METI2, METI3, METI4	4.69	Very important
23.Cybersecurity ethics	METI1	4.65	Very important
24.Digital forensics	METI1	4.42	Important
25.Risks of connecting to wi-fi	METI1	4.67	Very important
26.Importance of secured messaging	METI1	4.71	Very important
27.Importance of backup files	METI1	4.76	Very important
28.Ship's vulnerability points to cyber risks	METI1, METI4	4.76	Very important
29.Capabilities and limitations of existing protection measures onboard	METI1	4.71	Very important
Overall		4.70	Very important

Scale:
4.50 – 5.00 – very important 3.50 – 4.49 – important 2.50 – 3.49 – moderately important
1.50 – 2.49 – less important 1.00 – 1.49 – not important

Table 4.Cybersecurity Skills Taught by selected METIs and their importance as perceived by seafarers.

Cybersecurity Skills	Delivering Institution	Weighted Mean	Descriptive Equivalent
1. Responding to cyber security incidents using the contingency plan.	METI3	4.63	Very important
2. Safely using devices that can be abused by cyber attackers such as smart phones, personal computers and USB sticks	METI1, METI3	4.76	Very important
3. Using VPN (Virtual Private Network)	METI1	4.46	Important
4. Using encrypted email services	METI1	4.51	Very important
5. Creating backup files	METI1	4.75	Very important
6. Cleaning the ECDIS infected with ransomware	METI1	4.67	Very important
7. Configuring firewall	METI1	4.61	Very important
8. Facilitating information sharing and knowledge exchange of best practices	METI4	4.64	Very important
9. Developing inventories of onboard systems with direct and indirect communication links	METI3	4.54	Very important
10.Determining the likelihood of cybersecurity vulnerabilities.	METI3	4.60	Very important
11.Reinstalling the operating system and software.	METI1	4.58	Very important
12.Restoring all the ports' connection to AIS, GPS and other sensors.	METI1	4.63	Very important
13.Reducing the potential impact of a vulnerability being exploited	METI1, METI3	4.62	Very important
14.Recovering from cyber-attacks.	METI1, METI3	4.63	Very important
15.Developing contingency plans to effectively respond to identified cyber risks.	METI3	4.61	Very important
16.Assessing the impact of the effectiveness of the response plan	METI3	4.64	Very important
Overall		4.70	Very important

Scale:
4.50 – 5.00 – very important 3.50 – 4.49 – important 2.50 – 3.49 – moderately important
1.50 – 2.49 – less important 1.00 – 1.49 – not important

Table 4 presents the cybersecurity skills taught in the same four METIs-cases and the weighted mean for each cybersecurity skill. As seen in the table, the content of METIs' cybersecurity courses included 16 cybersecurity skills. Similar to cybersecurity knowledge, some skills were common to the delivering institutions while some were tackled by one institution only.

Only two skill items were delivered by both METI1 and METI3; one cybersecurity skill was delivered by METI4 while no cybersecurity skill was delivered by METI2. Just like in cybersecurity knowledge, METI1 and METI3 had the most number of cybersecurity skill items in their courses, with METI1 delivering ten (10) cybersecurity skills and METI3 delivering eight (8).

Except for item 3, which is the skill in using VPN and with a mean of 4.46 and described as important, all the other skills were rated by seafarers as very important. Overall, cybersecurity skills taught by METIs were perceived to be very important by the respondents as indicated by the average mean of 4.62.

METI1 and METI3 taught the most number of cybersecurity knowledge and skills items in their courses. This is because METI1 offered the longest delivery, comprising a 6-European Credit Transfer and Accumulation [ECTS] credit course that was conducted for four hours weekly for the whole semester. In the case of METI3, its course was delivered through a CBT which had no time frame, thus, many topics could be included in the course. On the other hand, METI2 has a one-ECTS course while METI4 embedded its cybersecurity topics in its other courses; thus, their content was fewer.

METIs differed in the topics they were teaching. While there are topics that were common to METIs, some topics were delivered by one METI alone. This means that there is no standard as to what cybersecurity knowledge and skills should be taught to seafarers. This is because the STCW 1978 Convention which is supposed to set the minimum standard for seafarer education and training does not include specific requirements for seafarers' cybersecurity knowledge and skills. Due to the lack of legal framework, METIs exercised their freedom to choose what cybersecurity knowledge and skills to teach in their cybersecurity course.

Aside from STCW 1978 Convention not having prescribed the minimum standard for seafarer education and training in cybersecurity, the concept itself is so broad and may cover different technical and non-technical aspects (Irons, 2019) so the METIs could not have possibly come up with similar topics to include, not to mention the base knowledge of cybersecurity being fragmented (Rashid et al., 2018).

The data also resounds the claim of Heering et al. (2021) that IMO is not at the same pace with the advancements in technology in the maritime field. Further, the same authors pointed out the duration of putting in place the necessary changes in the convention. The long duration also affects the implementation of new requirements in maritime education and training.

Collaboration with stakeholders played a critical role in the identification of knowledge and skills to be included in the course contents offered by METIs. These institutions worked with those who have conducted their own needs analysis of the cybersecurity knowledge and skills that seafarers need to identify the topics that they taught in their courses. Moreover, some of the course documents and materials such as The Guidelines on Cyber Security Onboard Ships, ISO/IEC 27001 Information Security Management and the NIST Framework, which all mentioned about necessary cybersecurity knowledge and skills were also referred to by METIs in finalizing the content of their courses. With these collaborations,

the METIs were able to deliver what really mattered in the workplace, which is on board vessels.

5 EDUCATIONAL APPROACHES RESEARCH FINDINGS, ANALYSIS AND DISCUSSIONS

This section presents the converged data gathered from the cases through semi-structured interviews, documents, and direct observations. Cases were characterized as METI1, METI2, METI3 and METI4. All quotations from the interviews are reproduced verbatim. The discussions are presented following the analysis in this section. Specifically, the analysis and discussion of the educational approaches of METIs are structured according to the analytical framework that was positioned based on the literature review in Section 2. In general, this section is presented in the following structure:

- Educational approach and its aspects
- The educational approaches of the cases using the analytical framework.

5.1 *Educational approach*

5.1.1 *Course level, target group, general aim, and ILO*

The data showed that the target group of all METIs are students except for METI3 who caters to seafarers. However, METIs also differ in which students (level, and course) they deliver their cybersecurity courses.

METI1: I (course developer) want this course to be very practical. The concentration is how we can increase cyber awareness among the seafarers before they join the vessel and also onboard the ship. The course is given to second year deck cadets.

METI2: A small course was developed for our deck and engine students. They are not actually students who will become true specialists in automation or in IT. That's why this maritime cybersecurity we are giving is more or less awareness training, not developing of systems to protect from being affected by cybersecurity attacks.

METI3: Pretty much all of our content in our library is aimed at serving seafarers are all disciplines onboard. And because cybersecurity is as much relevant to the deck department as it is to catering, as it is to engineering, we would call cybersecurity like a generic title, because it applies to all types of seafarers in all departments onboard the ship.

METI4: At present, we do teach cybersecurity in a sort of a very introductory level, within programs of cadets. Currently, cybersecurity topics are embedded in other courses.

From the data, it can be deduced that both the target group and the course level influenced how METIs formulated the general aim of their cybersecurity course. METI1 intended to offer a practical and skill-based course while METI2 and METI4 offer an introductory level course intending to raise cybersecurity awareness while METI3 aims to provide a generic course. Consequently, these general aims were defined and subdivided into smaller ILOs only by METI1 and METI3. METI1 also used Bloom's Taxonomy in defining its aims and ILOs as well as METI3. METI2 and METI4, however, did not define their ILOs and generated their topics after determining their general aim of their cybersecurity courses. This is shown in Figure 5.

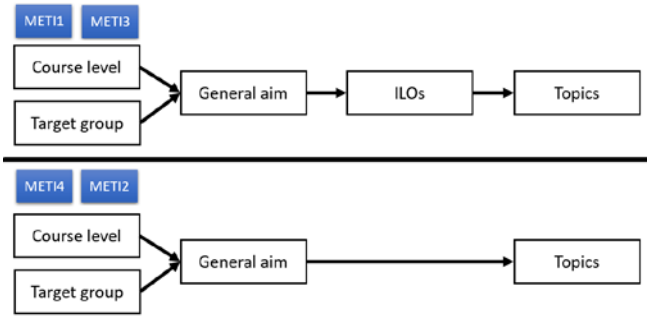

Figure 5. Process of how METIs came up with their Cybersecurity Course.

5.2 *Discussion of educational approaches of METIs*

The data in Table 5 shows the different aspects and/or components considered by METIs in the development and delivery of their cybersecurity course. As noted, all METIs take into consideration the following: course level, target group and the general aim of the course. On the other hand, they are not the same in giving importance to the following in designing and delivering their cybersecurity course as indicated by the absence of a particular aspect, or one or two sub-categories under each aspect: ILO, topics, TLAs, modality, instructor, tools and equipment, and assessment.

Using the analytical framework presented in the literature review, the following are the analyses of the educational approaches employed by METIs.

5.2.1 *Case 1: METI1*

The educational approach of METI1 formed a 'full lantern' with solid lines, as shown in Figure 6.

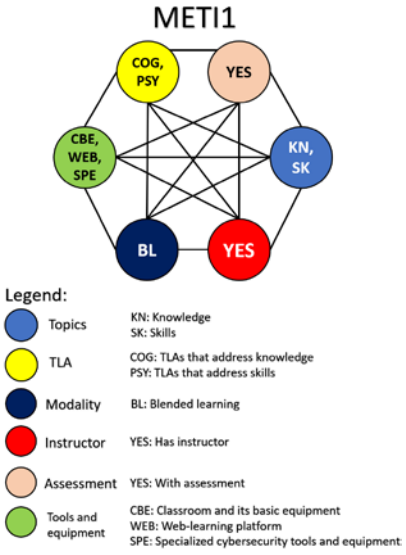

Figure 6. Visual Representation of the Educational Approach of METI1.

Table 5. Summary of Educational Approaches Employed by METIs.

	METI1	METI2	METI3	METI4
Content	KN, SK	KN	KN, SK	KN, SK
TLA	COG (Lecture, case studies, group discussion and presentation), PSY Demonstration, simulator exercise, field visit)	COG (Plain reading and browsing of the course materials uploaded in its web-learning platform)	COG (Lecture by an "audio lecturer" in its web-learning platform)	COG (Lecture)
Modality	BL	OA	OA	BL
Instructor	YES	NO	NO	YES
Assessment	YES	YES	YES	NO
Tools and equipment	CBE, WEB, SPE	WEB	WEB	CBE

Codes:
Content: KN – knowledge, SK – skills
TLA: COG – TLAs that address knowledge, PSY – TLAs that address skills
Modality: BL – blended learning, OA – fully online (asynchronous)
Instructor: YES – has instructor, NO – self-learning
Assessment: YES – with assessment, NO – without assessment
Tools and equipment: CBE – classroom and its basic equipment, including computer
WEB – web-learning platform (learning management system)
SPE – specialized cybersecurity tools and equipment (ECDIS simulator, cyber laboratory, wi-fi router, USB port blocker lock, Security USB Data Blocker Smart Charger, Yubikey)

METI1 delivered topics on both cybersecurity knowledge and skills using various TLAs that also both address the knowledge and skills that they teach. This is emphasized by Biggs (2003) about choosing the suitable TLAs to teach the subject to attain the objective of the course. The variety of TLAs they used were also possible to deliver using their choice of modality, which was a blended learning approach. Blended learning broadens students' horizons and assists them in acquiring the skills necessary for success in the 21st century (Tadlaoui & Chekou, 2021). Moreover, the presence of their instructors enabled them to conduct face-to-face and online synchronous classes, which were necessary in the delivery of most of their topics, particularly skill-based topics. In delivering their skill-based topics, they also used their specialized cybersecurity tools and equipment, including their ECDIS simulator in their cybersecurity laboratory. This necessitated them to employ instructors to properly and effectively demonstrate the use of their tools and equipment, and carry out their TLAs. The role of the instructor is critical especially in conducting simulation exercises (Fisher & Muirhead, 2005). The instructor not only demonstrates but also guides the students in doing an activity or an exercise safely, properly, and effectively. METI1 also administered assessments which is very important in determining whether their target group acquired the knowledge and skills that they delivered or not, as expressed in their course or learning outcomes.

Within the limits of this discussion, the educational approach that METI1, with the strength of the connection of each aspect, has contributed to the attainment of the outcomes and aims of their cybersecurity course.

5.2.2 *Case 2: METI2*

The educational approach of METI2 formed an 'incomplete lantern with solid lines', as shown in Figure 7.

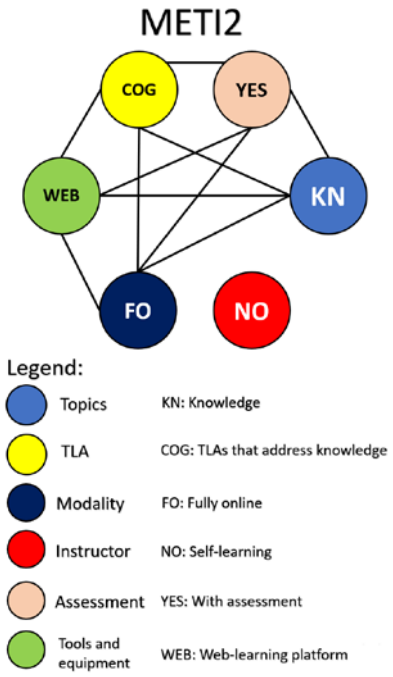

Figure 7. Visual Representation of the Educational Approach of METI2.

METI2 delivered topics on cybersecurity knowledge only and they also used TLAs that address the knowledge domain, which can also be delivered using their choice of modality which is fully online, without instructor. Their cybersecurity course was a self-learning course that even without an instructor, they were still able to deliver their course. One key

factor is their choice of tools and equipment which was a web-learning platform - an LMS, wherein self-learning is one of the key features (Chao & Chen, 2009). METI2 utilized other features of LMS such as it being a repository (Davis et al., 2009) and stored their learning resources including their assessments. LMS is very effective in delivering knowledge-based topics and allows for the delivery of TLAs that address knowledge.

The 'complete lantern' did not emerge as the educational approach of METI2 but that is because of the choice of modality which is fully online and the topics included in the course which is knowledge-based. Regardless of the choice of modality, it still presented 'harmony' among the aspects. This educational approach fits their intention of delivering a cybersecurity course that is knowledge-based in a basic level of raising cybersecurity awareness of its target group of learners.

5.2.3 *Case 3: METI3*

The educational approach of METI3 formed an 'incomplete lantern with various broken lines', as shown in Figure 8.

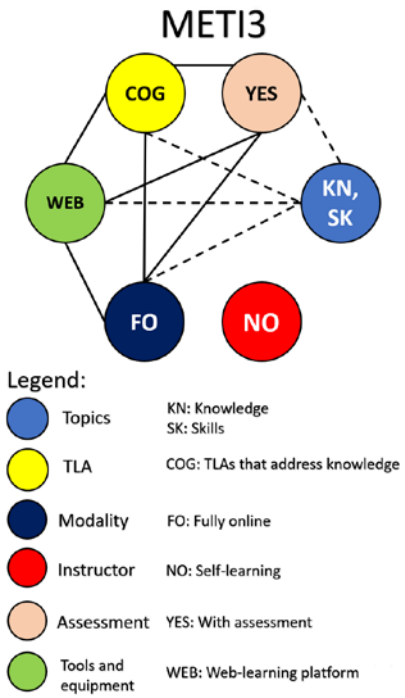

Figure 8. Visual Representation of the Educational Approach of METI3.

The topics that METI3 delivered, particularly the cybersecurity skills, were not supported by the other aspects of the educational approach they employed, which resulted in weak connections represented by broken lines. First, their TLAs only addressed knowledge (COG) but they did not use TLAs to address the topics of skills, which are included in their topics. Second, their modality which was fully online could not also support the delivery of cybersecurity skills because of the absence of an instructor. An instructor can effectively assist students in developing their cybersecurity skills (Burrell et al., 2015). The technology today like the cloud-based laboratory (Salah et al., 2015), which is found to have a positive impact on student learning (Xu et al., 2014), can be used to teach cybersecurity skills. However, the literature still emphasizes the role of instructor to effectively deliver the course using these technology-based tools and equipment (Salah et al., 2015). Nevertheless, METI3 did not show evidence that their tools and equipment have supported the delivery of their cybersecurity skills. Although they had assessments, they only addressed their cybersecurity knowledge but not their cybersecurity skills topics.

METI3's case is a good example that if cybersecurity skills are included in the topics of the course, the TLAs, modality, and the choice of tools and equipment should be reconsidered. METI3 might not have chosen the appropriate modality as it will be very difficult to successfully or even adequately deliver the cybersecurity course that is heavily skills-oriented with the chosen modality of fully online. Moreover, the effective delivery of TLAs that address skills with the tools and equipment that METI3 has requires the involvement of instructors. Furthermore, the chosen tools and equipment should effectively facilitate the development of skills and it should be utilized by METI. The potential of a LMS to support the wide array of teaching and learning methods, including the topics is huge. However, it should be utilized to maximize its features that could develop the TLAs that address cybersecurity skills.

Within the limits of this discussion, it is challenging to establish that the 'broken lantern' educational approach that METI3 employed contributed to the attainment of the objective of their cybersecurity course.

5.2.4 *Case 4: METI4*

The educational approach of METI4 formed an 'incomplete lantern with a broken line', as shown in Figure 9.

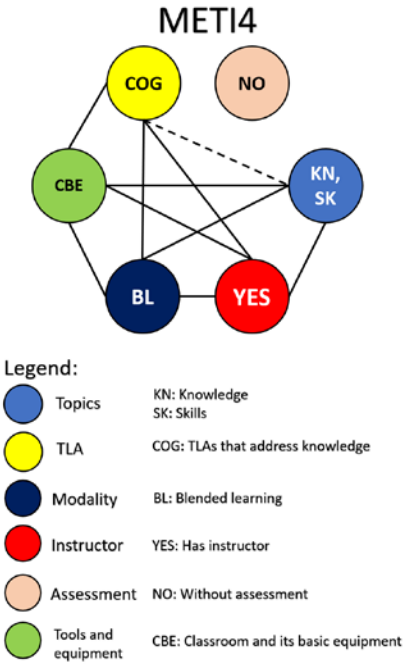

Figure 9. Visual Representation of the Educational Approach of METI4.

The topics delivered by METI4 both included cybersecurity knowledge and skills. However, its selection of TLAs did not address the topics on cybersecurity skills. The presence of instructor and the choice of blended learning approach as modality supported its other aspects of educational approach, but its lack of assessment did not support the attainment of the objectives of its cybersecurity course.

For the sake of discussion, if cybersecurity skills are removed in the topics of METI4, it would have formed an 'incomplete yet solid lantern' that might be a better educational approach to their course. However, not conducting the assessment is also the big demerit of the approach. As mentioned in literature, the assessment serves as a feedback mechanism and if this is removed from the process, there is no way the institution or the teacher is informed whether the goals or the intended learning outcomes are attained. Moreover, there is also no information on how the delivery is being done and how the instructor is doing if assessment is not conducted.

5.3 *Section summary*

This section presented that the METIs differed in the educational approaches they employed in the development and delivery of their cybersecurity course. Moreover, using the framework developed by the researchers, this paper also highlighted how the METIs regarded the relevance of the different aspects of educational approaches in their cybersecurity course.

6 CONCLUSION AND RECOMMENDATIONS

Any cybersecurity course, with all its aspects, is unique to each delivering METI. Different factors come into play, including the target group and the aim of the course, that affect its design and delivery process. With this stated, a minimum standard can still be set to serve as a framework of concerned institutions, especially for those with the same target group and aim.

This research has explored the knowledge and skills included in the cybersecurity courses offered by four METIs. Some topics came out to be common to the METIs while most were unique to a specific METI. With this, one can say that METIs do not have a uniform course content, as far as cybersecurity knowledge and skills are concerned. However, different METIs may differ in course content depending on their aims and objectives, as well as the target group of its cybersecurity course for as long as its educational approach helps in the attainment of such aims and objectives.

In order to make sure that the educational approach covers the necessary aspects in achieving the course aims and objectives, strong connections should be established between and among the different aspects of the educational approach employed. This is the main reason why the framework developed in this study fits into the whole picture of how cybersecurity education and training is given to seafarers, as presented in Figure 10. This framework will be a general guide to make the delivery of cybersecurity courses METIs harmonized and systematized in order to achieve their course's aims and objectives.

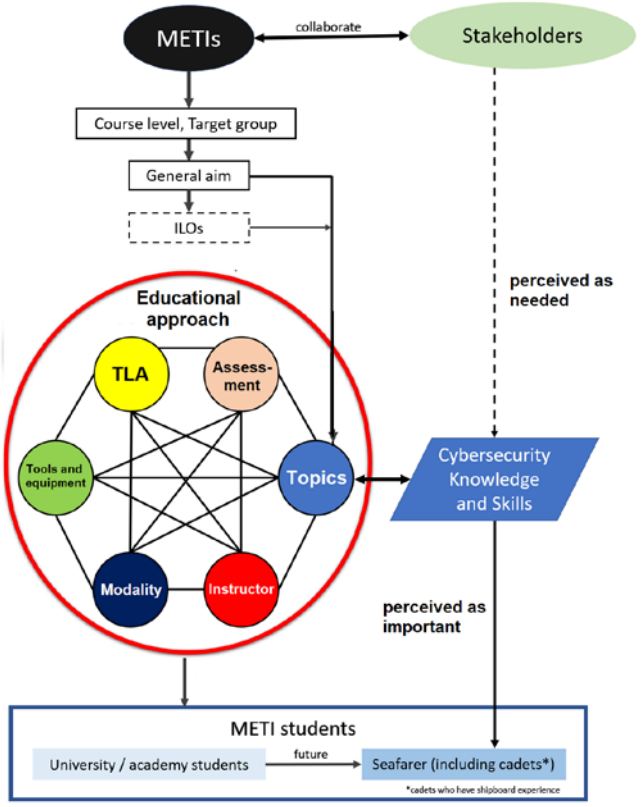

Figure 10. Overview of how the framework fits into cybersecurity education and training for seafarers.

With the help of collaboration with other stakeholders, METIs can identify their course level, target group, general aim, ILOs and topics of the course. The framework will then be used in order to determine the harmony of the aspects of their educational approaches. A harmonized educational approach will contribute to the attainment of the aims and objectives of their cybersecurity courses in order for their target group of learners, which are seafarers, to acquire the cybersecurity knowledge and skills that they need to possess. The framework, as highlighted above, presents the six aspects of educational approach – topics, TLA, modality, instructor, assessment, and tools and equipment. Whether they are complete or not, they should demonstrate a strong relationship among each other and should lead to the attainment of the course aim and objectives.

Nevertheless, all the identified knowledge and skills were deemed very relevant to the maritime profession by active seafarers.

6.1 *Recommendations*

This study recommends to the IMO to revisit the STCW Convention 1978, as amended, and make significant amendments that will enable seafarers to adequately perform their functions in an increasingly

digitalized environment. Moreover, it recommends that Administrations incorporate maritime cybersecurity education and training in their competence framework for seafarers in the absence of the standards prescribed by the STCW Convention 1978 in this regard. For METIs, the following are recommended:

- Existing METIs that deliver cybersecurity courses can make use of the 'lantern' framework and check their cybersecurity courses. The result would suggest for either retention or readjustment to determine the appropriate educational approach for their courses considering their objective and target group. METIs launching their cybersecurity course can also use the framework to consider the content, TLAs, modality, assessment, and selection of tools and equipment. Although it may not fill in all the gaps in cybersecurity education and training for seafarers, it may be helpful in standardizing the process of course design, development and delivery.
- Collaborate with their Administrations in incorporating maritime cybersecurity into the latter ' s competence framework (bottom-up approach).
- Design maritime cybersecurity education and training based on empirical data that reflects the specific knowledge and skills needed by seafarers based on their functions onboard the ship, and the best practices of educational approaches to teaching and learning cybersecurity.

6.2 *Limitations and future research*

- This research specifically focused on cybersecurity knowledge and skills for seafarers. Future researchers will benefit from a 'competencies' approach that also addresses the attitude component (affective domain) of cybersecurity education and training for seafarers.
- Future researchers can include other components of educational approach like evaluation for its improvement. As the researchers were limited to gathering enough and more detailed and substantial data to establish constructive alignment in the cybersecurity courses of the cases, future studies can consider integrating whether constructive alignment is established by looking at the specific contents of the ILOs, TLAs, and assessment. In the case of this study, not all ILOs were established by all cases, and the content of the assessment could not be provided due to its commercial value.
- Future researchers can either add more respondents from departments other than deck or engine or conduct a study that focuses on these departments and determine their specific needs. This will help in designing and delivering a cybersecurity course that is intended for their target group.
- Additional statistical tools, like factor analysis, can be performed to determine the order of importance of cybersecurity knowledge and skills for seafarers taught by METIs.
- Collaboration among the maritime stakeholders and its importance to maritime cybersecurity education and training was identified as a potential for future development of this study. This paper has provided a framework composed of aspects of educational approaches, which could be developed and enhanced with the help of METIs collaborating with other stakeholders. This study has opened up for such research to be able to optimize the development and delivery of cybersecurity education and training to seafarers.

REFERENCES

Adkisson, C., & McCoy, L. P. (2006). A study of teachers' perceptions of high school mathematics instructional methods. Studies in teaching, 1-6.

Ahvenjärvi, S. (2018). Addressing cyber security in training of the mariner of the future - the CYMET project. In International Symposium on Integrated Ship's Information Systems & Marine Traffic Engineering Conference.

Androjna, A., Brcko, T., Pavic, I., & Greidanus, H. (2020). Assessing Cyber Challenges of Maritime Navigation. Journal of Marine Science and Engineering, 8(10), 776. https://www.mdpi.com/2077-1312/8/10/776

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: evaluating the cybersecurity capacity of the industrial workforce. Journal of Systems and Information Technology, 21(1), 2-35. https://doi.org/10.1108/JSIT-02-2018-0028

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. (1680.). World Maritime University Dissertations. https://commons.wmu.se/all_dissertations/1680

Baik, C., Larcombe, W., Brooker, A., Wyn, J., Allen, L., Brett, M., Field, R., & James, R. (2017). Enhancing Student Mental Wellbeing: A Handbook for Academic Educators

Bates, A. W. (2015). Teaching in a digital age: Guidelines for designing teaching and learning. BCampus.

Bearman, M., & Dawson, P. (2013). Qualitative synthesis and systematic review in health professions education. Medical Education, 47(3), 252-260. https://doi.org/https://doi.org/10.1111/medu.12092

Ben-Asher, N., & Gonzalez, C. (2015, 2015/07/01/). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, 51-61. https://doi.org/https://doi.org/10.1016/j.chb.2015.01.039

Biggs, J. (2003). Aligning teachning for constructing learning. Higher Education Academy, 1(4), 1-4.

Boyatzis, R. E., & Kolb, D. A. (1991, 1991/01/01). Assessing Individuality in Learning: the learning skills profile. Educational Psychology, 11(3-4), 279-295. https://doi.org/10.1080/0144341910110305

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Would cybersecurity professionalization help address the cybersecurity crisis? Commun. ACM, 57(2), 24–27. https://doi.org/10.1145/2556936

Burrell, D. N., Finch, A., Simmons, J., & Burton, S. L. (2015). The Innovation and Promise of STEM-Oriented Cybersecurity Charter Schools in Urban Minority Communities in the United States as a Tool to Create a Critical Business Workforce. In New Threats and Countermeasures in Digital Crime and Cyber Terrorism (pp. 271-285). IGI Global.

Caponi, S. L., & Belmont, K. B. (2015). Maritime cybersecurity: a growing threat goes unanswered. Intellectual Property & Technology Law Journal, 27(1), 16.

Carlton, M., Levy, Y., Ramim, M., & Terrell, S. (2015). Development of the MyCyberSkills™ iPad app: A scenarios-based, hands-on measure of non-IT professionals' cybersecurity skills. Proceedings of the

Pre-International Conference of Information Systems (ICIS) SIGSEC-Workshop on Information Security and Privacy (WISP) 2015.
Chao, R.-J., & Chen, Y.-H. (2009, 2009/09/01/). Evaluation of the criteria and effectiveness of distance e-learning with consistent fuzzy preference relations. Expert Systems with Applications, 36(7), 10657-10662. https://doi.org/https://doi.org/10.1016/j.eswa.2009.02.047
Chi, M. T. (2006). Two approaches to the study of experts' characteristics. The Cambridge handbook of expertise and expert performance, 21-30.
Chicioreanu, T. D., & Amza, C. G. (2018). Adapting your teaching to accommodate the Net Generation/Z-Generation of learners. The International Scientific Conference eLearning and Software for Education.
Choi, M., Levy, Y., & Hovav, A. (2013). The role of user computer self-efficacy, cybersecurity countermeasures awareness, and cybersecurity skills influence on computer misuse. Proceedings of the Pre-International Conference of Information Systems (ICIS) SIGSEC–Workshop on Information Security and Privacy (WISP).
Chudowsky, N., Glaser, R., & Pellegrino, J. W. (2001). Knowing what students know: The science and design of educational assessment. National Academy Press.
Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.
Daum, O. (2019). Cyber security in the maritime sector. J. Mar. L. & Com., 50, 1.
Davis, B., Carmean, C., & Wagner, E. D. (2009). The evolution of the LMS: From management to learning. Santa Rosa, CA: e-Learning Guild.
deLeon, L., & Killian, J. (2000, 2000/01/01). Comparing Modes of Delivery: Classroom and On-Line (and Other) Learning. Journal of Public Affairs Education, 6(1), 5-18. https://doi.org/10.1080/15236803.2000.12022092
Dillon, H., & VanDeGrift, T. (2021, 2021/07/26). Creating an Inclusive Engineering Student Culture Through Diverse Teams: Instructor-led and Student-led Approaches Virtual Conference. https://peer.asee.org/36871
Fisher, D., & Muirhead, P. (2005). Practical teaching skills for maritime instructors. WMU publications.
Flick, U. (2018). Doing Triangulation and Mixed Methods. In. SAGE Publications Ltd. https://doi.org/10.4135/9781529716634
Fry, H., Ketteridge, S., & Marshall, S. (2008). A handbook for teaching and learning in higher education: Enhancing academic practice. Routledge.
Furnell, S. (2021, 2021/01/01/). The cybersecurity workforce and skills. Computers & Security, 100, 102080. https://doi.org/https://doi.org/10.1016/j.cose.2020.102080
Ha, E.-H., & Lim, E. J. (2018, 2018/05/01/). Peer-Led Written Debriefing Versus Instructor-Led Oral Debriefing: Using Multimode Simulation. Clinical Simulation in Nursing, 18, 38-46. https://doi.org/https://doi.org/10.1016/j.ecns.2018.02.002
Heering, D., Maennel, O., & Venables, A. (2021). Shortcomings in cybersecurity education for seafarers. In Developments in Maritime Technology and Engineering (pp. 49-61). CRC Press.
Hmelo-Silver, C. E., Duncan, R. G., & Chinn, C. A. (2007, 2007/04/26). Scaffolding and Achievement in Problem-Based and Inquiry Learning: A Response to Kirschner, Sweller, and. Educational Psychologist, 42(2), 99-107. https://doi.org/10.1080/00461520701263368
STCW Inc. 2010 Manila Amendments, (2017).
Irons, A. (2019). Delivering cybersecurity education effectively. In Cybersecurity Education for Awareness and Compliance (pp. 135-157). IGI Global.
Johnson, R. B., & Christensen, L. (2019). Educational research: Quantitative, qualitative, and mixed approaches. Sage publications.
Kala, N., & Balakrishnan, M. (2019). Cyber Preparedness in Maritime Industry. Int. J. Sci. Technol. Adv, 5, 19-28.
Karahalios, H. (2020, 2020/12/01). Appraisal of a Ship's Cybersecurity efficiency: the case of piracy. Journal of Transportation Security, 13(3), 179-201. https://doi.org/10.1007/s12198-020-00223-1
Kirschner, P., Sweller, J., & Clark, R. E. (2006). Why unguided learning does not work: An analysis of the failure of discovery learning, problem-based learning, experiential learning and inquiry-based learning. Educational Psychologist, 41(2), 75-86.
Läänemets, U., & Kalamees-Ruubel, K. (2013). The taba-tyler rationales. Journal of the American Association for the Advancement of Curriculum Studies (JAAACS), 9(2).
Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. International Journal of Information and Communication Technology Education (IJICTE), 1(3), 1-20.
Light, G., Calkins, S., & Cox, R. (2009). Learning and teaching in higher education: The reflective professional. Sage.
Malik, M., Fatima, G., & Sarwar, A. (2017). E-Learning: Students' Perspectives about Asynchronous and Synchronous Resources at Higher Education Level. Bulletin of Education and Research, 39(2), 183-195.
Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. Cybercrime Magazine, 13(11).
Mraković, I., & Vojinović, R. (2019). Maritime cyber security analysis–how to reduce threats? Transactions on maritime science, 8(01), 132-139.
Murati, R., & Ceka, A. (2017). The use of technology in educational teaching. Journal of Education and Practice, 8(6), 197-199.
Palupi, D. (2018). What Type of Curriculum Development Models Do We Follow? An Indonesia's 2013 Curriculum Case. Indonesian Journal of Curriculum and Educational Technology Studies, 6(2), 98-105.
Print, M. (1993). Curriculum development and design / Murray Print. Allen & Unwin.
Ramsden, P. (2003). Learning to teach in higher education. Routledge.
Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., & Peersman, C. (2018). Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy, 16(3), 96-102. https://doi.org/10.1109/MSP.2018.2701150
Robson, C. (2002). Real world research: A resource for social scientists and practitioner-researchers. Wiley-Blackwell.
Robson, C., & McCartan, K. (2016). Real world research : a resource for users of social research methods in applied settings : fourth edition. John Wiley & Sons.
Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching Cybersecurity Using the Cloud. IEEE Transactions on Learning Technologies, 8(4), 383-392. https://doi.org/10.1109/TLT.2015.2424692
Schlesinger, S. L., Heuwieser, W., & Schüller, L.-K. (2021). Comparison of Self-Directed and Instructor-Led Practice Sessions for Teaching Clinical Skills in Food Animal Reproductive Medicine. Journal of Veterinary Medical Education, 48(3), 310-318.
Scruggs, T. E., & Mastropieri, M. A. (2007, 2007/05/15). Science Learning in Special Education: The Case for Constructed Versus Instructed Learning. Exceptionality, 15(2), 57-74. https://doi.org/10.1080/09362830701294144
Smith, A., Ling, P., & Hill, D. (2006). The adoption of multiple modes of delivery in Australian universities. Journal of University Teaching & Learning Practice, 3(2), 4-19.
Stassen, M., Doherty, K., & Poe, M. (2001). Course-based review and assessment: Methods for understanding student learning www.umass.edu/oapa/sites/default/files/pdf/handbooks/course_based_assessment_handbook.pdf
Tadlaoui, M. A., & Chekou, M. (2021). A blended learning approach for teaching python programming language: towards a post pandemic pedagogy. International Journal of Advanced Computer Research, 11(52), 13.

Tam, K., Moara-Nkwe, K., & Jones, K. D. (2021). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. Maritime Technology and Research, 3(1), 16-30.
Tang, C., & Biggs, J. (2007). Teaching for quality learning at university: what the student does. Society for Research into Higher Education & Open University Press.
Trigwell, K. (2006). An analysis of the relations between learning and teaching approaches. Lifelong learning: Concepts and contexts, 108-116.
Wehr, J. (1988, 1988/06//). Instructor-led or computer-based: which will work best for you? Training & Development Journal, 42(6), 18+. https://link.gale.com/apps/doc/A6919245/AONE?u=anon~7a8d862b&sid=googleScholar&xid=a4d3fff8
Xu, L., Huang, D., & Tsai, W. T. (2014). Cloud-Based Virtual Laboratory for Network Security Education. IEEE Transactions on Education, 57(3), 145-150. https://doi.org/10.1109/TE.2013.2282285
Yin, R. K. (2018). Case study research and applications. Sage.