10-31-2021

A multiple case study of METI cybersecurity education and training: a basis for the development of a guiding framework for educational approaches

Jeric Bacasdoon

WORLD MARITIME UNIVERSITY

Malmö, Sweden

A MULTIPLE CASE STUDY OF METI CYBERSECURITY EDUCATION AND TRAINING:

A basis for the development of a guiding framework for educational approaches

JERIC BACASDOON
Philippines

A dissertation submitted to the World Maritime University in partial fulfilment of the requirements for the award of the degree of

MASTER OF SCIENCE
in
MARITIME AFFAIRS

(MARITIME EDUCATION AND TRAINING)

2021

Declaration

I certify that all the material in this dissertation that is not my own work has been identified, and that no material is included for which a degree has previously been conferred on me.

The contents of this dissertation reflect my own personal views, and are not necessarily endorsed by the University.

(Signature):
....

(Date): **21 September 2021**

Supervised by: Professor **Johan Bolmsten**

Supervisor's affiliation**: World Maritime University**

Acknowledgements

My heart is overflowing with gratitude to everyone who guided, supported, encouraged and empowered me in this journey.

Above everyone and everything, thank you Jesus, my Lord and Savior, for breaking me. And in my brokenness, you came to rescue me. You demonstrated your mighty power and gave me the grace to finish this study. Thank you for using this journey and letting me experience You like I have never before. Indeed, with You, all things are possible. All the glory, honor and praises belong to You!

> ‘*Because your steadfast love is better than life, my lips will praise you. So I will bless you as long as I live; in your name I will lift up my hands (Psalm 63:3-4, English Standard Version)*

To my family, my prayer warriors. Thank you to my parents, Antonino and Clarita, for loving me unconditionally; and to my siblings and in-laws Shayne, Ace, Arjay, Vince, Indeok, Vanessa, and Krista for standing with me in prayer. My nephews and nieces – Minwoo, Minji, Star, Addy, and Ice, you are my stress relievers.

To Dr. Conrado Oca, Chairman of the Associated Marine Officers’ and Seamen’s Union of the Philippines [AMOSUP]. Thank you for giving me the opportunity to study at the World Maritime University.

My heartfelt gratitude to Vice Admiral Eduardo Ma R Santos, AFP (Ret), President of the Maritime Academy of Asia and the Pacific [MAAP]. Thank you for your never-ending support and for always believing in me.

My deepest appreciation to my supervisor, Professor Johan Bolmsten, for connecting me to the METIs of my study, but more importantly, for seeing the potential in me and for not letting me settle for less; for pushing me to my limits; and for encouraging me throughout this study. Thank you, Professor! You are the best.

To my mentors and friends, Caroline and Nikki. Thank you for supporting me and for not letting go of me throughout this journey. You are a huge part of my success. You will forever be cherished.

My sincerest thanks to the American Bureau of Shipping for choosing me as one of the recipients of their research grant.

To the rest of MET faculty led by the head of specialization, Professor Michael Manuel, and Professor Inga Bartuseviciene, Professor Momoko Kitada, and Professor Anne Pazaver. Thank you for your assistance and support.

Special thanks to Dan Heering, Steven Gosling, Alex Barlow, Sauli Ahvenjärvi, and Gabriel Raicu.

To my Hillsong Malmö family, I found my spiritual family in Sweden in you. Thank you for being my home away from home.

And to my MET family, my support system – Moi, Cynthia, Dana, Peter, Hnin, Ayu, Pearl, Deron, Jackson, Joe and DJ; my WMU Christian Fellowship family, especially to Chris Nii Lantei and Tracy, my prayer partners, and to all my S21 friends, thank you for all your genuine support during the past 14 months.

Abstract

Title of Dissertation:	**A MULTIPLE CASE STUDY OF METI CYBERSECURITY EDUCATION AND TRAINING:** A basis for the development of a guiding framework for educational approaches
Degree:	Master of Science

Cyberattacks have become a serious global concern, effecting enormous losses to different sectors. In the shipping business, huge shipping companies reported losing great amounts of money and having had to address their operations' integrity and security. While the International Maritime Organization (IMO), through the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers (STCW) 1978, 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 researcher. In particular, the following objectives were addressed: cybersecurity knowledge and skills included in their curriculum; importance of the cybersecurity knowledge and skills to seafarers; differences in the perceptions of seafarers; educational approaches of the METIs in delivering their topics on cybersecurity; and the role of collaboration in their course design and delivery. The first, fourth and fifth objectives were answered using different sources of qualitative data, including document analysis, interview and direct observation. Quantitative approach, in a form of a survey questionnaire, was used to address the second and third objectives. 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 and that except for training experience, they did not significantly differ in their perception. Similar to the content of their courses, the METIs delivered their cybersecurity courses by employing varied educational approaches. Nevertheless, they all valued the contribution of collaboration in their course design and delivery. To address the gap on the lack of cybersecurity course design and delivery minimum standards, a framework in the shape of a lantern was developed and proposed to guide maritime courses designers, in particular, and other course designers, in general.

KEYWORDS: Cybersecurity education and training, educational approaches, lantern framework, collaboration, METI cybersecurity, cybersecurity framework

Table of Contents

Declaration i

Acknowledgements ii

Abstract iv

Table of Contents vi

List of Tables viii

List of Figures viii

List of Abbreviations ix

1. Introduction 1

1.1 Background and context 1

1.2 Problem statement 3

1.3 Research aims and objectives 5

1.4 Research questions 5

1.5 Research methodology and methods 6

1.6 Structure of the dissertation 6

2. Literature review 8

2.1 Cybersecurity knowledge and skills 8

2.2 Cybersecurity education and training for seafarers 9

2.3 Educational approaches 10

2.3.1 Target group 11

2.3.2 Course level, aim, and ILO 11

2.3.3 Cybersecurity topics 12

2.3.4 Teaching/learning activities 12

2.3.5 Modality 13

2.3.6 Instructor-led and self-learning 14

2.3.7 Assessment 14

2.3.8 Tools and equipment 15

2.4 Relationship among the educational aspects 16

2.5 Collaboration 16

2.6 Chapter Summary 17

3. Research methodology and methods 19

3.1 Purpose and outline 19

3.2 Methodological approach and rationale 19

3.3 Selection of participants 22

3.3.1 METIs 22

3.3.2 Seafarers 22

3.4 Instrumentation and data collection 22

3.4.1 Semi-structured interview 22

3.4.2 Documentation and direct observations 23

3.4.3 Self-administered questionnaire 23

3.5 Data analyses **24**
3.5.1 Qualitative data analysis 24
3.5.2 Quantitative data analysis 25
3.6 Ethical issues **25**
3.7 Chapter summary **25**

4. Cybersecurity knowledge and skills research findings, analysis and discussions **27**
4.1 Cybersecurity knowledge and skills taught by METIs **27**
4.2 Importance of cybersecurity knowledge and skills **32**
4.2.1 Importance of cybersecurity knowledge 32
4.2.2 Differences on the responses of the seafarer-respondents 36
4.3 Chapter summary **39**

5. Educational approaches and collaboration research findings, analysis and discussions **40**
5.1 Educational approach **40**
5.1.1 Course level, target group, general aim, and ILO 40
5.1.2 Aspects of educational approach 42
5.2 Discussion of educational approaches of METIs **49**
5.2.1 Case 1: METI1 52
5.2.2 Case 2: METI2 54
5.2.3 Case 3: METI3 56
5.2.4 Case 4: METI4 58
5.2.5 Convergence of cases 59
5.3 Collaboration **60**
5.3.1 Collaboration guides the delivery of the course (METI1) 63
5.3.2 Collaboration helps in the development of quality reference materials (METI2) 63
5.3.3 Collaboration enriches the content of the course (METI3 and METI4) 64
5.4 Chapter summary **65**

6. Conclusion and recommendations **66**
6.1 Research conclusion **66**
6.2 Recommendations **68**
6.2.1 International Maritime Organization 68
6.2.2 Administrations 69
6.2.3 METIs 69
6.3 Limitations and future research **69**

References **71**

Appendices **76**
Appendix A: Interview Instrument **76**
Appendix B: Survey Questionnaire **77**
Appendix C: Reliability test **82**
Appendix D: Normality Test **83**

List of Tables

Table 1 Demographics. 24
Table 2 Cybersecurity Knowledge Taught by Selected METIs. 28
Table 3 Cybersecurity Skills Taught by Selected METIs. 29
Table 4 Importance of Cybersecurity knoweldge as perceived by seafarers. 32
Table 5 Importance of Cybersecurity skills as perceived by seafarers. 34
Table 6 Hypothesis Test Summary by Age (Kruskal-Wallis Test). 36
Table 7 Hypothesis Test Summary by Department (Kruskal-Wallis Test). 37
Table 8 Hypothesis Test Summary by Training (Mann-Whitney U Test). 38
Table 9 Cybersecurity Topics that METIs Teach. 42
Table 10 TLAs used by METIs in Delivering Their Cybersecurity Course 42
Table 11 Instructors Employed by METIs. 44
Table 12 Tools and Equipment Used by METIs. 44
Table 13 Assessments Used by METIs. 46
Table 14 Summary of Educational Approaches Employed by METIs. 47
Table 15 Pairing of Aspects of Educational Approach and the Conditions Establishing Their Relationship. 51

List of Figures

Figure 1. Classification of modality based on the continuum of technology-based teaching of Bates (2015). .... **Error! Bookmark not defined.**
Figure 2. Convergence of Multiple Sources of Evidence of Qualitative Method. 20
Figure 3. Research Approach and Process. 21
Figure 4. Process of how METIs came up with their Cybersecurity Course. 41
Figure 5. Modes of Delivery of METIs based from the Continuum of Technology-based Learning of Bates (2015). 43
Figure 6. Other Tools and Equipment used by METI1. 45
Figure 7. ECDIS Simulator in the Cyber Laboratory of METI1. 46
Figure 8. Summary of the Aspects of Educational Approach Employed by METIs in Delivering their Cybersecurity Course. 48
Figure 9. Analytical Framework of Strong Connection of the Aspects of Educational Approach. 50
Figure 10. Visual Representation of the Educational Approach of METI1. 52
Figure 11. Visual Representation of the Educational Approach of METI2. 54
Figure 12. Visual Representation of the Educational Approach of METI3. 56
Figure 13. Visual Representation of the Educational Approach of METI4. 58
Figure 14. Collaboration of METIs with Other Entities. 62
Figure 15. Overview of how the framework fits into cybersecurity education and training for seafarers. 67

List of Abbreviations

AIS	Automatic Identification System
BIMCO	Baltic and International Maritime Council
CBT	computer-based training
CYMET	Addressing Cyber Security in Maritime Education and Training
DOC	Document of Compliance
ECDIS	Electronic Chart Display and Information System
ECTS	European Credit Transfer and Accumulation
EU	European Union
GPS	Global Positioning System
IAMU	International Association of Maritime Universities
ICS	International Chamber of Shipping
IEC	International Electrotechnical Commission
ILO	Intended learning outcome
IMO	International Maritime Organization
INTERCARGO	International Association of Dry Cargo Shipowners
ISM Code	International Safety Management Code
ISO	International Organization for Standardization
ISPS	International Ship and Port Facility Security Code
IT	Information technology
IUMI	International Union of Marine Insurance
LMS	Learning Management System
MET	Maritime Education and Training
METI	Maritime Education and Training Institution
NICE	National Institute for Cybersecurity Education
NIST	National Institute of Standards and Technology
OCIMF	Oil Companies International Marine Forum
OT	Operational technology
STCW Code	Seafarers Training, Certification, and Watchkeeping Code
STCW Convention	The International Convention on Standards of Training,

	Certification, and Watchkeeping for Seafarers, 1978, as amended
SYBASS	Superyacht Builders Association
TLA	Teaching/learning activities
UNCTAD	United Nations Conference on Trade and Development
VPN	Virtual Private Network
WMU	World Maritime University
WSC	World Shipping Council

1. Introduction

1.1 Background and context

Today, shipping is an integral aspect of the global economy, transporting about 80% of global trade by volume. Every country has become interdependent on trades that are mainly carried out at sea. This global trade involved approximately 98,140 ships (UNCTAD, 2020), and 1.8 million seafarers (BIMCO & ICS, 2021) participate actively in this worldwide trade. In an era of digitalization led by the fourth industrial revolution or Industry 4.0, such ships and the maritime industry, in general, are influenced by technological innovations. Numerous technological applications have evolved into a critical component of shipping, delivering real-time information and facilitating effective communication on a global scale.

Technological advancements bring both benefits and challenges for the shipping industry. Numerous emerging technologies in the maritime industry have led to the improvement of safety and efficiency onboard. Consequently, the maritime sector has seen enormous growth and investment over the last five years, transforming transportation and creating various commercial opportunities (see Ledger Insights, 2021; Inmarsat, 2020; DNV, 2019; Rolls-Royce, 2018). In terms of vessel operations, technology can assist in maintaining safe navigation, reducing manning, as well as securing and effecting vessel operations.

However, 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 (NEP&I, 2017; Saul, 2017). At the turn of the twenty-first century and with the popular use of the internet and computer networks, which led to the increased use of cyberspace as a business platform, the risk of cyber-attacks greatly increased. Cyber-attack refers to any attempt to gain unauthorized access to computer systems, and exploit them to disturb computers and compromise the confidentiality, integrity and availability of data (Bendovschi, 2015). Cybercriminals or terrorists access and control a target's system causing damage. Some of the largest shipping companies were victims of cyber-attacks. In 2017, Maersk lost $200-300 million; in 2018, COSCO's Port of Long Beach terminal and internet connection in some of its sites in America were affected (*The Maritime Executive,* 2018) and; in 2020, both Mediterranean Shipping Company and CMA CGM reported being victims of cybercrimes (Cimpanu, 2020). The unauthorized access to sensitive systems and usage of maritime transportation for illegal purposes put the safety and security of shipping operations at risk (DiRenzo, 2017). 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. The impact to the entire maritime industry will be great, necessitating a global action.

With such increasing concern on maritime cybersecurity, the International Maritime Organization [IMO] adopted Resolution MSC.428(98) that "encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the International Safety Management [ISM] Code) no later than the first annual verification of the company's Document of Compliance [DOC] after 1 January 2021." IMO subsequently posted guidelines that provide recommendations to facilitate appropriate cyber risk management for vessel owners and operators. These include The Guidelines on Cyber Security Onboard Ships[1], ISO/IEC 27001 Information Security Management[2] and the NIST Framework[3].

Notably, the development of cybersecurity measures should be inextricably linked to technological advancements. However, the maritime domain is several years behind

[1] The Guidelines on Cyber Security Onboard Ships is produced and supported by Baltic and International Maritime Council [BIMCO], Chamber of Shipping of America, Digital Containership Association, International Association of Dry Cargo Shipowners [INTERCARGO], InterManager, International Association of Independent Tanker Owners [INTERTANKO], International Chamber of Shipping [ICS], International Union of Marine Insurance [IUMI], Oil Companies International Marine Forum [OCIMF], Superyacht Builders Association [SYBASS] and World Shipping Council [WSC].

[2] ISO/IEC 27001 Information Security Management is published jointly by the International Organization for Standardization [ISO] and the International Electrotechnical Commission [IEC]

[3] NIST Framework is United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity.

other computer-based industries such as aviation (Alsulami & Zein-Sabatto, 2021) and healthcare (see Fosch-Villaronga & Mahler, 2021; Iwendi et al., 2021), and has failed in prioritizing cybersecurity (Caponi & Belmont, 2015).

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). Moreover, its current edition does not include anything about cybersecurity. Furthermore, the IMO is behind in its review of the STCW to keep the Convention up to date with emerging technologies, as stated in Resolution 15 of the Convention.

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 (Bhasin, 2007). Hence, adding cybersecurity knowledge and skills to the safety culture on board is critical. Alop (2019) emphasized that, in the context of smart shipping innovation, investing in education and new skills is equally necessary, if not more so, than the technology itself. As seafarers play significant roles to maintain cybersecurity onboard ships, training and education is vital. For that reason, this dissertation reviews and examines the cyber security skills and competences needed for seafarers. Furthermore, it examines the educational approaches to maritime cybersecurity and the significance of collaboration of maritime stakeholders.

1.2 Problem statement

As the maritime industry, including seafarers as individuals, expands its use of new and advanced technologies, cybercriminals are also working hard to identify and exploit the weakest links. Despite the media reports of cyberattacks in shipping, the concerned stakeholders seem to lack understanding about the impact of these incidents on the systems of navigation (Hareide et al., 2018).

One of the areas that criminals focus on is mistakes made by uneducated and poorly skilled computer users (Cain et al., 2018). It is evident that the employees are weak links that make the organization vulnerable to security threats (Canfield et al., 2016). In particular, organizations with a workforce that is not trained in cybersecurity and other related threats are likely to face challenges when it comes to data security and the integrity of their systems.

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. Hence, education and training are fundamental (Heering et al., 2021) in the successful mitigation of cyberthreats. The IMO, shipping companies, and other maritime stakeholders, should be at the frontlines to develop seafarers as a workforce that can circumvent threats from cyberspace.

However, apart from the IMO's cybersecurity guidelines, the specific skills and competences required of seafarers are not yet well defined. Additionally, such skills and competences should be classified according to their levels - either Management level, Operational Level or Support Level, as per the Seafarers Training, Certification, and Watchkeeping [STCW] Code Table of Competences.

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. However, teaching cybersecurity to seafarers efficiently and effectively cannot be neglected. Appropriate instructional approaches and training methods, the competence of the instructor teaching specific topics, and the right equipment suitable for the delivery of the course have to be considered.

Wang et al. (2020) noted that collaborations and partnerships in the industry for a successful information technology education is important. In the case of maritime cybersecurity, it is fundamental to bring together the stakeholders, though challenging, to ensure that the course to be delivered will address and meet the industry requirements. The combination of dynamic content and the task of monitoring course activities make teaching cybersecurity challenging. It is therefore necessary to find out the significance of stakeholder collaboration in the areas of course content and delivery for the development and improvement of the course.

1.3 Research aims and objectives

The aim of the study is to examine the cybersecurity courses of METIs and obtain the perception of seafarers to the cybersecurity knowledge and skills that METIs teach. In order to achieve this, five research objectives are proposed as follows:

- To determine the cybersecurity knowledge and skills taught by METIs;
- To determine the importance of such cybersecurity knowledge and skills as perceived by seafarers;
- To determine if the perceived importance of seafarers to cybersecurity knowledge and skills has a significant difference in terms of their age, department, and training experience;
- To discuss what educational approaches were employed by METIs in delivering their cybersecurity course; and
- To describe the role of collaboration in cybersecurity education and training for seafarers.

1.4 Research questions

The research methodology aimed to answer the following:

Research Question 1: What are the cybersecurity knowledge and skills taught by METIs?

Research Question 2: How do seafarers perceive the importance of cybersecurity knowledge and skills?

Research Question 3: Is there a significant difference in the perception of seafarers when grouped according to:

a. Age;
b. Department; and
c. Training experience?

Research Question 4: How may the educational approaches employed by METIs in delivering their cybersecurity courses be described?

Research Question 5: What is the role of collaboration among the maritime stakeholders in the development and delivery of cybersecurity education and training to seafarers?

1.5 Research methodology and methods

This study employed the principles of two distinct types of triangulation: methodological triangulation and data triangulation (Patton, 2015). Further, it utilized a combination of qualitative and quantitative methods.

The qualitative approach drew on a variety of sources of evidence to examine how cybersecurity education and training for seafarers are delivered and to describe the critical role of collaboration among the stakeholders in the development and delivery of cybersecurity education and training to seafarers. This included semi-structured interviews, documents, and direct observations. These data were gathered from four METIs who served as cases for the study. Additionally, data from the aforementioned sources were used to develop a questionnaire for the quantitative method.

In the quantitative approach, the views of 403 seafarers were surveyed to understand the perception of seafarers about the importance of cybersecurity knowledge and skills taught by METIs.

The approval of the WMU Research Ethics Committee was obtained before the collection of data.

A detailed presentation of the methodological approach and specific methods is contained in the third chapter of this research.

1.6 Structure of the dissertation

The literature review in Chapter Two focuses on the background of cybersecurity; educational approaches and its aspects; and the collaboration of maritime stakeholders. Chapter 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 Chapter Four for cybersecurity knowledge and skills and Chapter Five for educational approaches and collaboration. Chapter Six concludes the study, makes recommendations for METIs and other maritime stakeholders and identifies suggested research areas for future consideration.

2. Literature review

This chapter 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 form a framework that is to be developed and illustrated in the succeeding chapters. The discussion takes off from cybersecurity, and ventures into educational approaches employed in designing and delivering a course, including the collaborations of maritime stakeholders that are already in place.

2.1 Cybersecurity knowledge and skills

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., 2018). 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 & Gonzales, 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., 2018; 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 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) argues 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.

2.2 Cybersecurity education and training for seafarers

While research on cybersecurity and maritime safety and security is becoming popular, 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. (2020) 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.

Considering the current state of technical progress in the shipping sector, training seafarers should include appropriate cybersecurity knowledge and skills. However, the current edition of the STCW Convention by the IMO (2017), which is the international minimum standard for seafarer training, does not include specific requirements for seafarers' cybersecurity knowledge and skills. The STCW Code mentions the duties of seafarers as stated in the International Ship and Port Facility Security [ISPS] Code, which aims at addressing all aspects of security. However, it fails to address cyber threats. Heering et al. (2021) claim that the IMO is falling behind the pace of technological advancements in the maritime industry. Due to the international decision-making mechanisms in place today, amendments to the STCW Convention can take an extended period of time to approve and implement into the curriculum. As a result, METI’s curricula may not contain a cybersecurity course. This is echoed in International Association of Maritime Universities [IAMU]’s project “Addressing Cyber Security in Maritime Education and Training” [CYMET] (Ahvenjärvi, et al., 2019) where none of the ten European maritime universities in their study offered courses in maritime cybersecurity. Simultaneously, seafarers' skills require immediate upgrading and ongoing updating, as cyber threats continue to evolve in terms of form, direction, and aim.

METIs and other organizations spearheaded initiatives to address the concerns of maritime cybersecurity education and training. CYMET project resulted in the development of a training package on maritime cybersecurity issues for the use of IAMU member universities (Ahvenjärvi, et al., 2019). The European Union [EU] funded project SkillSea has been initiated to ensure that maritime professionals acquire necessary digital, green and soft management skills at par with the changes in the maritime labor market. In their latest report on current skills needed, the consortium addresses the main challenges the maritime shipping sector must face in nearest future (Zec et al., 2020).

2.3 Educational approaches

The research into educational approaches continues, and debates over various theories of learning and their impact on these approaches have emerged. The debates focused on 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 (Scruggs & Mastropieri, 2007; Hmelo-Silver et al., 2007), explicitly 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 & Killian (2000), as well as the intended level outcomes [ILO], Teaching/learning activities [TLA], assessment by Biggs (2003) and the use of tools and equipment (Muraki & Ceka, 2017). They are presented as aspects of educational approach in this study.

2.3.1 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 groups of 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 target group of learners, are also distinguished considering their level which is either management, operational, or support level as stated in the STCW Convention (IMO, 2017). On the other hand, target groups of future seafarers are usually distinguished based on their year level at the university.

2.3.2 Course level, aim, and ILO

Light et al. (2009) distinguished between course aim, learning objectives and learning outcomes. Course aim originates 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 paper, 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 (Biggs & Tang, 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 (Biggs & Tang, 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., 2004; Ramsden, 2003), it is better to formulate outcomes rather than objectives because outcomes are based on the students’ perspective (Biggs & Tang, 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., 2004). Moreover, many course developers or teachers use Bloom’s taxonomy as their guide in stating their ILOs. Biggs and Tang (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.

2.3.3 Cybersecurity topics

This section deals with the content of the course. Content, in the case of this study, deals with cybersecurity topics which are categorized as knowledge and skills as presented in section 2.1.

2.3.4 Teaching/learning activities

According to Biggs and Tang (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.

2.3.5 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 and Fatima (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 researcher 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.

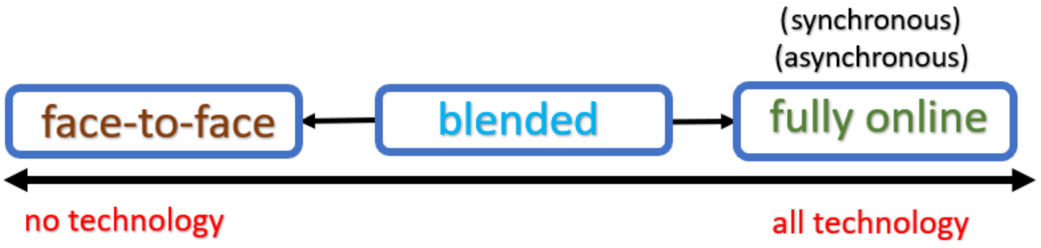


Figure 1. Classification of modality based on the continuum of technology-based teaching of Bates (2015).

Implications for practice or policy according to (Nieuwoudt, 2020):

- Different choices on online learning, including participation and attendance, may increase the academic success of students.
- Different online activities should be prepared and facilitated in order for the students to have several chances of interacting and participating during synchronous or asynchronous sessions.
- Synchronous virtual classes should be recorded and made available to students.

2.3.6 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, 2019).

2.3.7 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 & Larcombe, 2016; 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 (Pellegrino et al., 2001).

The most popular types of assessment are formative and summative assessments. Formative assessments are administered for the purpose of having feedback on how the students (in terms of their learning performance) and the teachers (in terms of their teaching performance) are doing during the delivery of the topic or the course. The feedback that students and teachers receive should improve their learning and teaching practices, respectively. Summative assessments, on the other hand, are given at the end of a unit or course to gauge how well the students have learned what they were expected to learn (Biggs & Tang, 2007). There is another type of assessment, the diagnostic assessment, which intends to determine what and how much the students know before a course is delivered (Tookoian, 2018). This is administered so that the teacher would know where to start and what to include in the course topics.

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.

2.3.8 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 (Topham et al., 2016), 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. (2013), cloud-based laboratory affects 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 Manuel (2021), as adapted from 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 Collaboration

Various cybersecurity guidelines and frameworks are products of collaboration of different entities. The development of the National Institute for Cybersecurity Education [NICE] Cybersecurity Workforce Framework of the U.S. Department of Commerce for cybersecurity workforce training and education is a product of many years of collaboration between industry, government and academia (Newshouse et al., 2017). They emphasized that collaboration between public and private entities, such as the NICE program, enables these institutions to identify necessary knowledge and abilities.

SecTech project is a collaborative effort in cybersecurity education that provides the foundations of a collaborative program in education. It includes clarifying content, describing the structure of the module and its delivery, and the appropriating tool support to enable collaboration and content reuse (Tokola et al., 2019).

CYMET project provides opportunities for joint production of web-learning materials. It is a collaborative work of three METIs who are members of IAMU where the international maritime education community could benefit from collaboration in the area of training material development (Ahvenjärvi, et al., 2019). By utilizing the best available expertise within its member universities, IAMU could promote the quality of cybersecurity in Maritime Education and Training [MET] globally.

SkillSea is a multilateral project, composed of 27 partners from 16 European countries, promotes cooperation between various players in the industry and the academic world, universities and government agencies (Oksavik et al., 2020). It also acknowledges that some skills, including cybersecurity, are not included in the training courses offered at present, thus, collaboration between the business community and research-based universities is encouraged.

It is the aim of this research to find out the roles of collaboration in cybersecurity education and training for seafarers.

2.6 Chapter 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 chapter 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 Chapter 3, the interdependence is elaborated in Chapter 4 and Chapter 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 researcher created an analytical framework which is used to structure the analysis and discussions in Chapter 5 to describe the educational approaches employed by METIs in delivering their cybersecurity courses.

3. Research methodology and methods

3.1 Purpose and outline

This chapter focuses on discussing the approach 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 Chapter 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;
- Educational approaches employed by METIs in teaching their cybersecurity courses; and
- Role of collaboration among maritime stakeholders in cybersecurity education and training for seafarers.

3.2 Methodological approach and rationale

Qualitative research methods are focused and require in-depth analysis of details of a particular area of study. The information yielded by the analysis helps the researcher to understand the areas of his or her study. The same information may also serve as a basis in formulating new themes to study (Suri & Clarke, 2009). However, because qualitative research does not make use of statistics, many researchers argue that its data may not be objective and it may not result in the same interpretation and/or analysis from different readers (Bearman & Dawson, 2013). Meanwhile, quantitative research is systematic and believed to be objective, so it is therefore vital in the dissemination of research methodology. However, its being systematic is also its restriction because it may disregard other areas covered by the qualitative method. It treats all knowledge as quantifiable which is not entirely true (Suri & Clarke, 2009). In fact, Colliver (2008) demonstrated that quantitative research can be biased.

Bearman and Dawson (2013) argued that prior to selecting an appropriate research method, it is necessary to fully understand the philosophical conflict between two methodologies. However, Creswell and Creswell (2018) 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 researcher to obtain seafarers' and METIs' perspectives on the cybersecurity knowledge and skills required of seafarers, and the role of collaboration among stakeholders in the development and delivery of a cybersecurity training or course.

Another type of 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. Using multiple sources of evidence enables the development of converging lines of inquiry; consequently, any finding or conclusion drawn from multiple sources of evidence is more likely to be persuasive and accurate (Yin, 2018). 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 2.

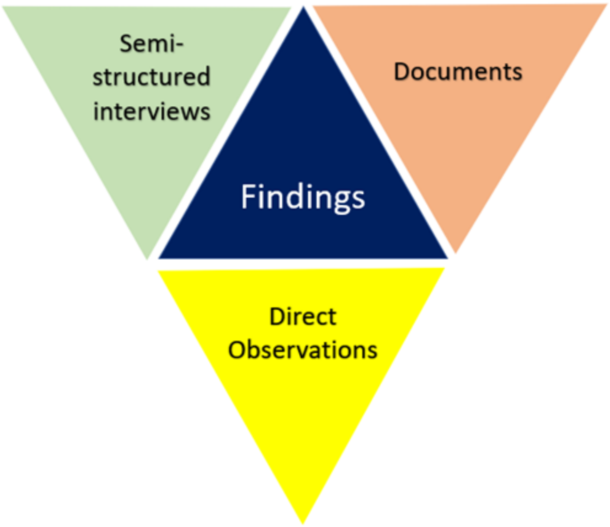


Figure 2. Convergence of Multiple Sources of Evidence of Qualitative Method.

The research methods used should maximize the likelihood of obtaining useful answers to the research questions (Johnson & Onwuegbuzie, 2004). Qualitative method was used to obtain in-depth analysis and answer the research questions on cybersecurity knowledge and skills taught by METIs, their educational approaches in the delivery of their cybersecurity courses and the role of collaboration in cybersecurity education and training for seafarers. On the other hand, a quantitative approach was used to acquire an objective answer to the research question on the importance of cybersecurity knowledge and skills taught by METIs.

Figure 3 depicts the research approach and process of the present study. Aside from answering research question 1, research question 4 and research question 5, 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 questions 2 and research question 3. The use of NVivo aided qualitative data analysis, whereas Microsoft Excel aided quantitative data analysis.

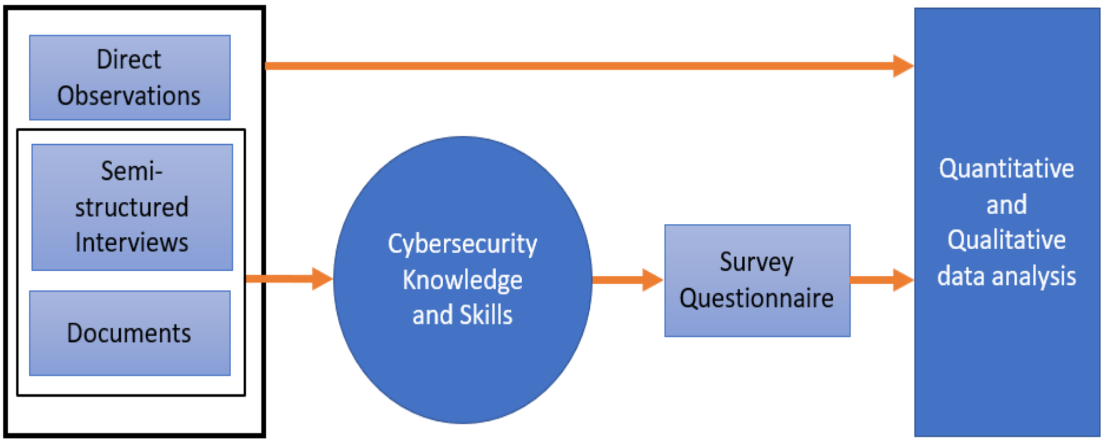

Direct Observations
Semi-structured Interviews
Documents
Cybersecurity Knowledge and Skills
Survey Questionnaire
Quantitative and Qualitative data analysis

Figure 3. Research Approach and Process.

3.3 Selection of participants

The researcher made use of purposive sampling to determine the respondents of the study. This is applicable when the researcher wants to include comprehensive data from a particular person or group of persons (Etikan et al., 2016; Patton, 2005).

3.3.1 METIs

In this research, four METIs that offer cybersecurity education and training were targeted cases. These institutions are regarded as premier providers of cybersecurity education and training to seafarers.

3.3.2 Seafarers

Additionally, this study surveyed seafarers, who are end-users of Information Technology [IT] and operational technology [OT] systems, as they are 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 researcher used interviews to answer research question 1, research question 4, and research question 5. 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 (see Appendix A). The researcher 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, the educational approaches that they employed, and the role of collaboration in cybersecurity education and training for seafarers.

All interviews were transcribed and imported into NVivo software for qualitative analysis. The generated cybersecurity knowledge and skills were used to create the online questionnaire for the survey.

3.4.2 Documentation and direct observations

The researcher gathered documents, which included curriculum documents, course syllabus and materials which aimed to answer research question 1, research question 4, and research question 5. The researcher 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 4, and research question 5.

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. The questions were stated in the most practical way so as to be understood by the respondents. The survey had four sections: one aimed to find out the respondents' demography. The next section asked for the respondent's training experience. The third section dealt with cybersecurity knowledge, while the fourth focused on cybersecurity skills. Then, a 5-point rating scale was used to assess respondents' perceptions of the importance of cybersecurity knowledge and skills required. Prior to distribution to target respondents, the researcher pilot tested the questionnaire to his colleagues from the World Maritime University [WMU]'s MSc in Maritime Affairs program. For instrument validation, ten (10) responses were gathered, which resulted in the questionnaire being fine-tuned (see Appendix B). Additionally, since Likert scale was used, the questionnaire was sent to 40 respondents for reliability testing. The Cronbach's Alpha coefficient yielded an excellent reliability (see Appendix C).

The advantage of questionnaire-based surveys is that they enable the efficient collection of specific data from a large sample (Creswell, 2014), as well as the analysis and modelling of the resulting correlational relationships while minimizing negative human interactions – a method that ensures the highest possible data quality and validity (McCusker & Gunaydin, 2015). The researcher used this research method and targeted seafarers from all ranks onboard the ship, in preparation for comparing the data from the cases. Questionnaire responses were imported to Microsoft Excel software for analysis.

After cleaning the data, there are 403 seafarers who are respondents in this study, as shown in Table 1. 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 1.
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 with the aid of NVivo

12 Plus software to generate insights into what cybersecurity knowledge and skills METIs teach, what educational approaches are employed in their courses and what the role of collaboration in cybersecurity education and training is. The researcher organized the data according to distinct themes. Typically, these themes corresponded to a single research question. For each theme, the researcher analyzed the interview and assigned codes to the responses. The researcher 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 researcher 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 Microsoft Excel, where both descriptive and inferential statistics were used. Descriptive statistics included the data for age, department and training experience. On the other hand, principles of inferential statistics were used to determine the perceived importance to seafarers of cybersecurity knowledge and skills taught by METIs, and the significant difference of perceived importance in terms of their age, department and training experience.

3.6 Ethical issues

This research adhered to the WMU Research Ethics Committee's rules and guidelines regarding human participation in data collection. The researcher collected data with a strong emphasis on respondent safety - adhering to established research ethics principles such as not harming the participants, obtaining informed participant’s consent, considering the privacy of participants, and being honest at all times. The collected data was treated with strict confidentiality and anonymity, and was securely stored using password protection before being securely deleted at the conclusion of the study.

3.7 Chapter summary

In this chapter, 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 chapter 5, the findings, analyses, and discussions using qualitative approach are presented to analyze the educational approaches used by METIs to deliver their cybersecurity courses, and also the role of collaboration in cybersecurity education and training to seafarers.

4. Cybersecurity knowledge and skills research findings, analysis and discussions

This chapter includes the qualitative data obtained from documents, and semi-structured interviews from four METIs, which were identified as METI1, METI2, METI3, and METI4, and their analysis to find out the cybersecurity knowledge and skills taught by METIs. As mentioned in the previous chapter, such knowledge and skills were used to generate a survey questionnaire, forming the quantitative data, to obtain the perception of seafarers of their importance.

This chapter is structured as follows:

- Cybersecurity knowledge and skills taught by METIs;
- Seafarers' perception of importance to such cybersecurity knowledge and skills; and
- The differences in the responses of seafarers.

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 would-be and active seafarers.

Table 2 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.

Table 2.
Cybersecurity Knowledge Taught by Selected METIs.

Cybersecurity Knowledge	Delivering Institution
1. External cybersecurity threats to the ship	METI1, METI2, METI3
2. Internal cybersecurity threats posed by inappropriate use and poor cybersecurity practices	METI2, METI3
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. How cyber risks can be reduced	METI1, METI2, METI3
5. How to respond to a cybersecurity breach or attack	METI1, METI3
6. The need for constant vigilance and reviews of the cyber risk management plan	METI3
7. Importance of each individual's role and how he/she can protect himself/herself and his/her organization against cyber security threats	METI3
8. Elements of Cybersecurity Management	METI2, METI3, METI4
9. Password and remote connection requests	METI1, METI4
10. Real-life cases of cyber incidents	METI1, METI2, METI3
11. Most common methods used by cyber attackers	METI1, METI3
12. What to do if you become a victim of a cyber-attack	METI3
13. What to do if your computer is infected by ransomware	METI1, METI3
14. Risks that can occur through overuse of smart phones, tablets, laptops and social media	METI3
15. How to achieve a healthy balance between	METI3

work and leisure, offline and online	
16. Best practices of cyber hygiene	METI1, METI3, METI4
17. How positive online behaviors can help to maintain concentration and focus while at work	METI3
18. Considerations to be made before posting on social media	METI3
19. Key steps to ensuring cybersecurity on board is maintained	METI3
20. Concept of security	METI1
21. Terminologies of cybersecurity	METI1, METI3
22. Cybersecurity rules, guidelines, standards, and legal frameworks developed for maritime sector	METI1, METI2, METI3, METI4
23. Cybersecurity ethics	METI1
24. Digital forensics	METI1
25. Risks of connecting to wi-fi	METI1
26. Importance of secured messaging	METI1
27. Importance of backup files	METI1
28. Ship's vulnerability points to cyber risks	METI1, METI4
29. Capabilities and limitations of existing protection measures onboard	METI1

In particular, only one out of the 29 knowledge items was common to all the four delivering institutions, item number 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 Skills Taught by Selected METIs.

Cybersecurity Skills	Delivering Institution
1. Responding to cyber security incidents using the	METI3

	contingency plan.	
2.	Safely using devices that can be abused by cyber attackers such as smart phones, personal computers and USB sticks	METI1, METI3
3.	Using VPN (Virtual Private Network)	METI1
4.	Using encrypted email services	METI1
5.	Creating backup files	METI1
6.	Cleaning the ECDIS infected with ransomware	METI1
7.	Configuring firewall	METI1
8.	Facilitating information sharing and knowledge exchange of best practices	METI4
9.	Developing inventories of onboard systems with direct and indirect communication links	METI3
10.	Determining the likelihood of cybersecurity vulnerabilities.	METI3
11.	Reinstalling the operating system and software.	METI1
12.	Restoring all the ports' connection to AIS, GPS and other sensors.	METI1
13.	Reducing the potential impact of a vulnerability being exploited	METI1, METI3
14.	Recovering from cyber-attacks.	METI1, METI3
15.	Developing contingency plans to effectively respond to identified cyber risks.	METI3
16.	Assessing the impact of the effectiveness of the response plan	METI3

Table 3 presents the cybersecurity skills taught in the same four METIs-cases. 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).

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 was 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 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 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.

4.2 Importance of cybersecurity knowledge and skills

This section generally presents the data of the perception of 403 seafarers on the importance of cybersecurity knowledge and skills to them and in their work. Some of them are overarching the others but the researcher decided to retain them including their more specific knowledge or skill/s.

4.2.1 Importance of cybersecurity knowledge

The table below presents the summary of the perception of the seafarer-participants on the importance of cybersecurity knowledge to them and in their work. With an overall mean of 4.70, the cybersecurity knowledge taught by METIs were perceived to be *very important* by the respondents.

Table 4.
Importance of Cybersecurity Knowledge as Perceived by Seafarers.

Cybersecurity Knowledge	**Weighted Mean**	**Descriptive Equivalent**
1. External cybersecurity threats to the ship	4.68	Very important
2. Internal cybersecurity threats posed by inappropriate use and poor cybersecurity practices	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)	4.72	Very important
4. How cyber risks can be reduced	4.75	Very important
5. How to respond to a cybersecurity breach or attack	4.73	Very important
6. The need for constant vigilance and reviews of the cyber risk management plan	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	4.78	Very important
8. Elements of Cybersecurity Management	4.61	Very

		important
9. Password and remote connection requests	4.73	Very important
10. Real-life cases of cyber incidents	4.74	Very important
11. Most common methods used by cyber attackers	4.68	Very important
12. What to do if you become a victim of a cyber-attack	4.80	Very important
13. What to do if your computer is infected by ransomware	4.78	Very important
14. Risks that can occur through overuse of smart phones, tablets, laptops and social media	4.71	Very important
15. How to achieve a healthy balance between work and leisure, offline and online	4.71	Very important
16. Best practices of cyber hygiene	4.66	Very important
17. How positive online behaviors can help to maintain concentration and focus while at work	4.68	Very important
18. Considerations to be made before posting on social media	4.73	Very important
19. Key steps to ensuring cybersecurity on board is maintained	4.72	Very important
20. Concept of security	4.72	Very important
21. Terminologies of cybersecurity	4.59	Very important
22. Cybersecurity rules, guidelines, standards, and legal frameworks developed for maritime sector	4.69	Very important
23. Cybersecurity ethics	4.65	Very important
24. Digital forensics	4.42	Important
25. Risks of connecting to wi-fi	4.67	Very important
26. Importance of secured messaging	4.71	Very important
27. Importance of backup files	4.76	Very important
28. Ship's vulnerability points to cyber risks	4.76	Very important
29. Capabilities and limitations of existing protection measures onboard	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

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*.

Table 5.
Importance of Cybersecurity Skills as Perceived by Seafarers.

Cybersecurity Skill	**Weighted Mean**	**Descriptive Equivalent**
1. Responding to cyber security incidents using the contingency plan.	4.63	Very important
2. Safely using devices that can be abused by cyber attackers such as smart phones, personal computers and USB sticks	4.76	Very important
3. Using VPN (Virtual Private Network)	4.46	Important
4. Using encrypted email services	4.51	Very important
5. Creating back up files	4.75	Very important
6. Cleaning the Electronic Chard Display and Information System [ECDIS] infected with ransomware	4.67	Very important
7. Configuring firewall	4.61	Very important
8. Facilitating information sharing and knowledge exchange of best practices	4.64	Very important
9. Developing inventories of onboard systems with direct and indirect communication links	4.54	Very important
10. Determining the likelihood of cybersecurity vulnerabilities.	4.60	Very important

11. Reinstalling the operating system and software.	4.58	Very important
12. Restoring all the ports' connection to Automatic Identification System [AIS], Global Positioning System [GPS] and other sensors.	4.63	Very important
13. Reducing the potential impact of a vulnerability being exploited	4.62	Very important
14. Recovering from cyber-attacks.	4.63	Very important
15. Developing contingency plans to effectively respond to identified cyber risks.	4.61	Very important
16. Assessing the impact of the effectiveness of the response plan	4.64	Very important
Overall	**4.62**	**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 5 presents the weighted mean for each cybersecurity skill. 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.

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.

4.2.2 Differences on the responses of the seafarer-respondents

Hypothesis tests were conducted to determine the significant difference in perception of the seafarer-respondents based on their age, department, and training experience. After conducting the Shapiro-Wilk Test that resulted to non-normally distributed data (see Appendix D), Kruskal-Wallis Test, a nonparametric test, was used to test the hypothesis for age and department as they have more than two variables while the Mann-Whitney U Test was used for training experience, which only have two variables. Hypothesis tests results in figures and tables are presented in Appendix E.

4.2.2.1 By age

A Kruskal-Wallis test showed that in terms of age groups, there was no statistically significant difference in the perception of seafarers on the cybersecurity knowledge, $\chi^2(5) = 5.159$, p = 0.397, and skills, $\chi^2(5) = 6.383$, p = 0.271 as shown in Table 6.

Table 6.
Hypothesis Test Summary by Age (Kruskal-Wallis Test).

Null Hypothesis	**Sig.**	**Decision**
1. The distribution of cybersecurity knowledge is the same across categories of age.	.397	Retain the null hypothesis.
2. The distribution of cybersecurity skills is the same across categories of age.	.271	Retain the null hypothesis.

Note: Asymptotic significances are displayed. The significance level is .05

Therefore, the perception of importance of seafarers to cybersecurity knowledge and skills is the same regardless of age.

4.2.2.2 By department

Table 7 contains the hypothesis test summary for the perception of seafarers on the cybersecurity knowledge and skills in reference to the department where they belonged. As gleaned from the table, there were three departments: the Deck Department, the Engine Department and the Other Department.

A Kruskal-Wallis test showed that there was a statistically significant difference in the perception on cybersecurity knowledge between the different departments, $\chi^2(2) = 9.409$, $p = 0.009$, with a mean rank cybersecurity knowledge score of 202.06 for Deck Department, 205.79 for Engine Department and 29.75 for Other Department. The perception of the Engine Department is statistically higher than the perception of both the Deck Department and the Other Department.

However, excluding the Other Department, which is composed of four respondents, the same test resulted in no statistically significant difference in cybersecurity knowledge between Deck and Engine departments.

The null hypotheses that the distribution of cybersecurity knowledge and skills needed is the same between deck and other department, and engine and other department are therefore rejected. However, the null hypotheses that the distribution of cybersecurity knowledge and skills needed is the same between deck and engine department is retained.

Table 7.
Hypothesis Test Summary by Department (Kruskal Wallis Test).

Null Hypothesis	Sig.	Decision
Cybersecurity knowledge		
1. The distribution of cybersecurity knowledge is the same between deck and other department.	.008	Reject the null hypothesis.
2. The distribution of cybersecurity knowledge is the same between engine and other department.	.006	Reject the null hypothesis.
3. The distribution of cybersecurity	1.000	Retain the null

knowledge is the same between deck and engine department.		hypothesis.
Cybersecurity skills		
4. The distribution of cybersecurity skills is the same between deck and other department.	.026	Reject the null hypothesis.
5. The distribution of cybersecurity skills is the same between engine and other department.	.015	Reject the null hypothesis.
6. The distribution of cybersecurity skills is the same between deck and engine department.	1.000	Retain the null hypothesis.

Note: Asymptotic significances are displayed. The significance level is .05

The retention of the null hypotheses means that regardless of working in the deck or the engine department, seafarers have the same perception on the importance of cybersecurity knowledge and skills. With only four respondents, the researcher cannot conclude for the Other department.

4.2.2.3 By training

The result of the Mann-Whitney U Test showed that the knowledge score from the group with training was statistically significantly higher than the group without training (U = 17,560, p = .049), as shown in Table 8. However, there was no statistically significant difference in the perception of importance of cybersecurity skills between those with and without training (U = 18,293, p = .184).

The null hypothesis that the distribution of cybersecurity knowledge is the same with or without training, as reflected in the Hypothesis Test Summary in Table 7 is then rejected. However, the null hypothesis that the distribution of cybersecurity skills is the same with or without training is retained.

Table 8.
Hypothesis Test Summary by Training (Mann-Whitney U Test).

Null Hypothesis	**Sig.**	**Decision**
1. The distribution of cybersecurity knowledge is the same with or without training.	.049	Reject the null hypothesis.
2. The distribution of cybersecurity skills is the same with or without training.	.184	Retain the null hypothesis.

Note: Asymptotic significances are displayed. The significance level is .05

The perception of importance to cybersecurity skills is the same regardless if seafarers have training experience or none. On the contrary, seafarers with training experience perceive cybersecurity knowledge as more important compared to those who have no training experience.

4.3 Chapter summary

In summary, METIs included 29 cybersecurity knowledge and 16 cybersecurity skills in their cybersecurity courses. Some of these topics are common and some are unique to the delivering METIs. Further, these cybersecurity knowledge and skills taught by METIs were perceived by seafarers as very important regardless of their age, department, and training experience. Moreover, seafarers perceived the cybersecurity skills taught by METIs to have the same importance regardless of their age, department, and training experience. Similarly, all cybersecurity skills taught by METIs were valued the same by seafarers regardless of their age and department. Those with training experience, on the other hand, placed a higher regard on cybersecurity knowledge than those without.

5. Educational approaches and collaboration research findings, analysis and discussions

This chapter 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 chapter. 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 Chapter 2. The analysis and discussion for the role of collaboration is then presented. In general, this chapter is presented in the following structure:

- Educational approach and its aspects
- The educational approaches of the cases using the analytical framework
- Findings, analysis and discussion of the role of collaboration.

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 4.

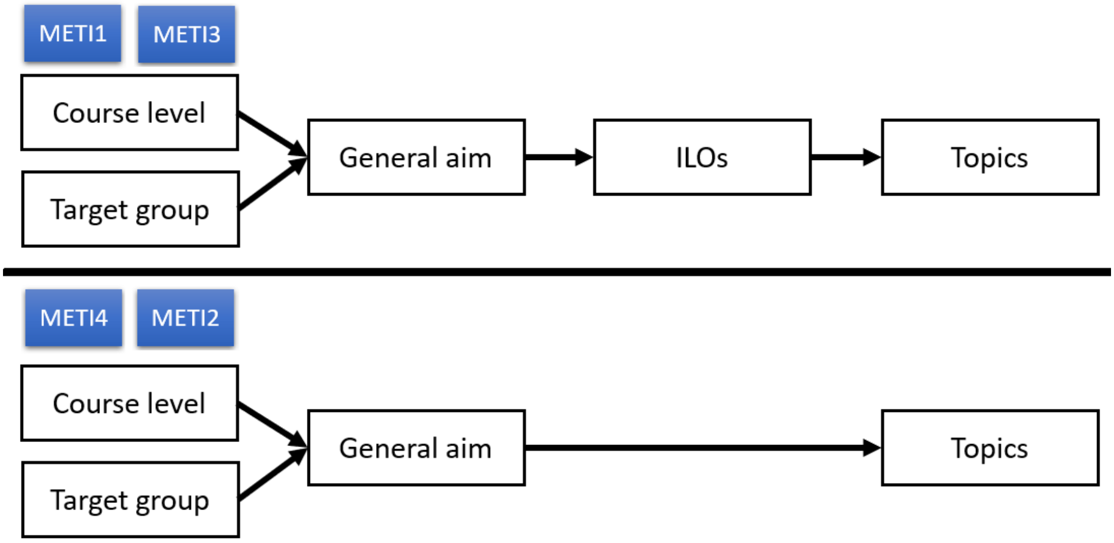


Figure 4. Process of how METIs came up with their Cybersecurity Course.

5.1.2 Aspects of educational approach

5.1.2.1 Topics

As mentioned in the previous chapter, METIs differed in the cybersecurity knowledge and skills that they teach. This section identifies the general topics delivered by METIs: knowledge, skills, or both.

Table 9.
Cybersecurity Topics that METIs Teach.

	Knowledge	Skills
METI1	YES	YES
METI2	YES	NO
METI3	YES	YES
METI4	YES	YES

Table 9 presents the topics delivered by METIs. All METIs delivered both cybersecurity knowledge and skills except for METI2 who only included cybersecurity knowledge in its cybersecurity course.

5.1.2.2 Teaching/learning activities

The researcher categorized the TLAs employed by METIs as those that address knowledge as cognitive TLAs and those that address skills as psychomotor TLAs. Table 10 shows the TLAs that were used by METIs in delivering their courses.

Table 10.
TLAs used by METIs.

METI1	Cognitive	Lecture, case studies, group discussion and presentation
	Psychomotor	Demonstration, simulator exercise, field visit
METI2	Cognitive	Plain reading and browsing of the course materials uploaded in its web-learning platform
METI3	Cognitive	Lecture by an “audio lecturer” in its web-learning platform
METI4	Cognitive	Lecture

Table 9 shows that METI1 employed various TLAs to address both cognitive and psychomotor domains. The rest of the METIs, on the other hand, only used TLAs that address the cognitive domain.

5.1.2.3 Modality

METIs used different modes of delivery in their cybersecurity courses as shown in Figure 5.

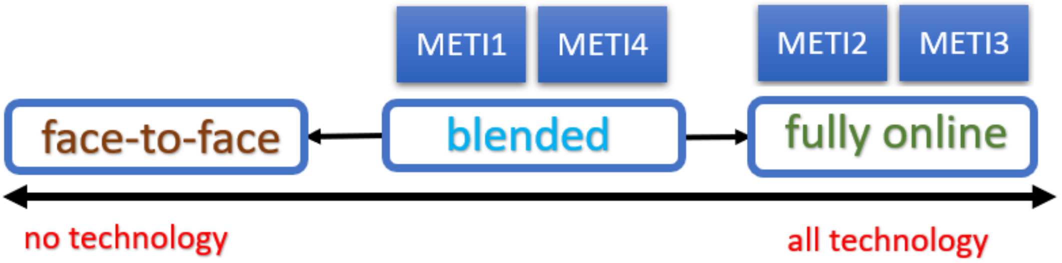


Figure 5. Modes of Delivery of METIs based from the Continuum of Technology-based Learning of Bates (2015).

METI2 and METI3 delivered their courses fully online and through asynchronous[4] classes. METI1, on the other hand, also had a module delivered in asynchronous manner, blended with online and face-to-face delivery. Meanwhile, METI4 used a blended learning approach for the conduct of its lectures.

5.1.2.4 Instructors

METI1 and METI4 employed instructors to deliver their cybersecurity course while METI2 and METI3 had self-learning courses, as shown in Table 11. METI1 had seven multinational instructors, all IT specialists, who discussed different topics according to their area of expertise. Cybersecurity topics of METI4, on the other hand, were being delivered by the instructors of the courses where the topics were embedded.

[4] Asynchronous learning occurs when there is no set time for learning to occur. Learners can study anywhere and at their own pace, acquiring knowledge about what they want to learn and when they need to know it (Malik & Fatima, 2017).

Table 11.
Instructors employed by METIs.

	With instructor	Self-learning
METI1	X	
METI2		X
METI3		X
METI4	X	

5.1.2.5 Tools and equipment

All METIs used tools and equipment to deliver their cybersecurity course. The researcher categorized the tools and equipment into the following:

- Classroom and its basic equipment (including computer);
- Web-learning platform (Learning Management System); and
- Specialized cybersecurity tools and equipment (ECDIS simulator, cyber laboratory, wi-fi router, USB port blocker lock, Security USB Data Blocker Smart Charger, Yubikey), as shown in Figure 6 and Figure 7.

Table 12.
Tools and equipment used by METIs.

	Classroom and its basic equipment	Web-learning platform	Specialized cybersecurity tools and equipment
METI1	X	X	X
METI2		X	
METI3		X	
METI4	X		

Table 12 shows that METIs varied in the tools and equipment they were using to deliver their cybersecurity courses. METI2 and METI3 both used a web-learning platform only while METI4 used the classroom and its basic equipment. Meanwhile, METI1 used all the tools and equipment mentioned. METI1 explained the reasons for using specialized cybersecurity tools and equipment.

METI1: To present or demonstrate the issues you can get when you log into open wi-fi network, we have hacked five wi-fi routers, which you can use for teaching purposes.

We use the university VPN service. And one way to practice it is to give to the students link to academic paper. If you're not log into the university's VPN, you can't download the paper. So, this is one way to show them how VPN works and how it is possible to browse safely.

I use all the equipment (USB port blocker lock, Security USB Data Blocker Smart Charger, Yubikey) *to present to the students so they can actually try it.*

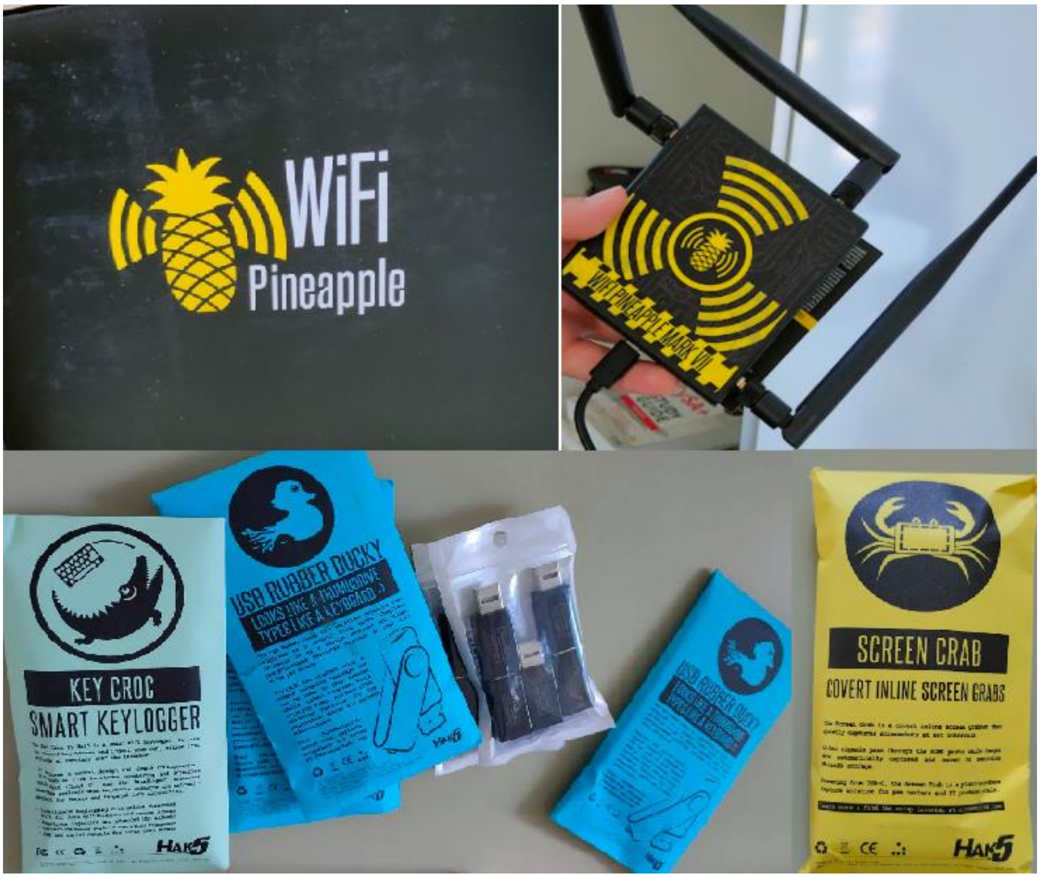


Figure 6. Other Tools and Equipment used by METI1.

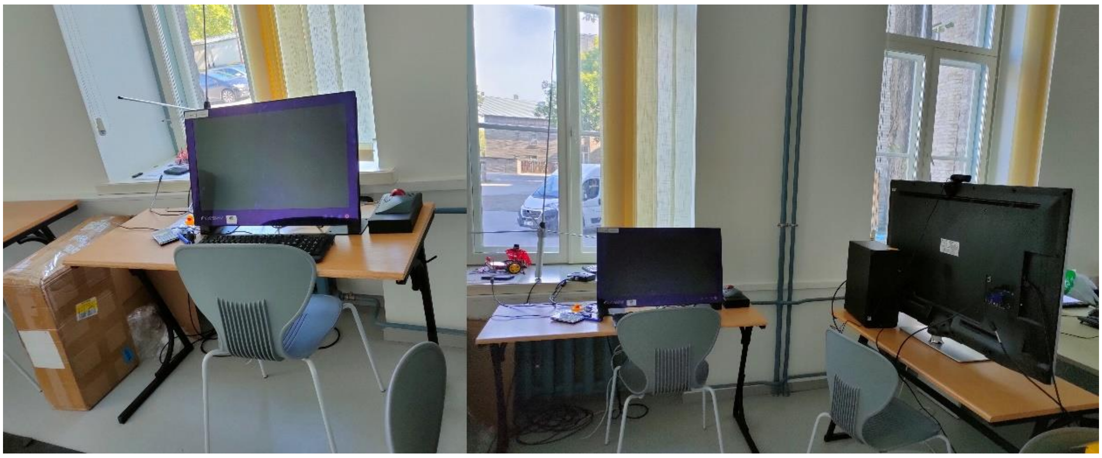


Figure 7. ECDIS Simulator in the Cyber Laboratory of METI1.

5.1.2.6 Assessment

METIs conducted assessments except for METI4, as shown in Table 13. METI1, in particular, conducted all types of assessment while METI2 and METI3 only administered formative assessment.

Table 13.
Assessments used by METIs in delivering their cybersecurity courses.

		Diagnostic	Formative	Summative
METI1	YES	X	X	X
METI2	YES		X	
METI3	YES		X	
METI4	NONE			

5.1.2.7 Summary of educational approaches employed by METIs

The table below is the summary of the aspects of educational approaches employed by METIs. The researcher used codes to describe each component.

Table 14.
Summary of Educational Approaches Employed by METIs.

	METI1	METI2	METI3	METI4
Content	KN, SK	KN	KN, SK	KN, SK
TLA	COG, PSY	COG	COG	COG
Modality	BL	OA	OA	BL
Instructor	YES	NO	NO	YES
Assessment	YES	YES	YES	YES
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
WEB – web-learning platform
SPE – specialized cybersecurity tools and equipment

The researcher presented them in a diagram as shown in Figure 8, which will be used in the discussion section.

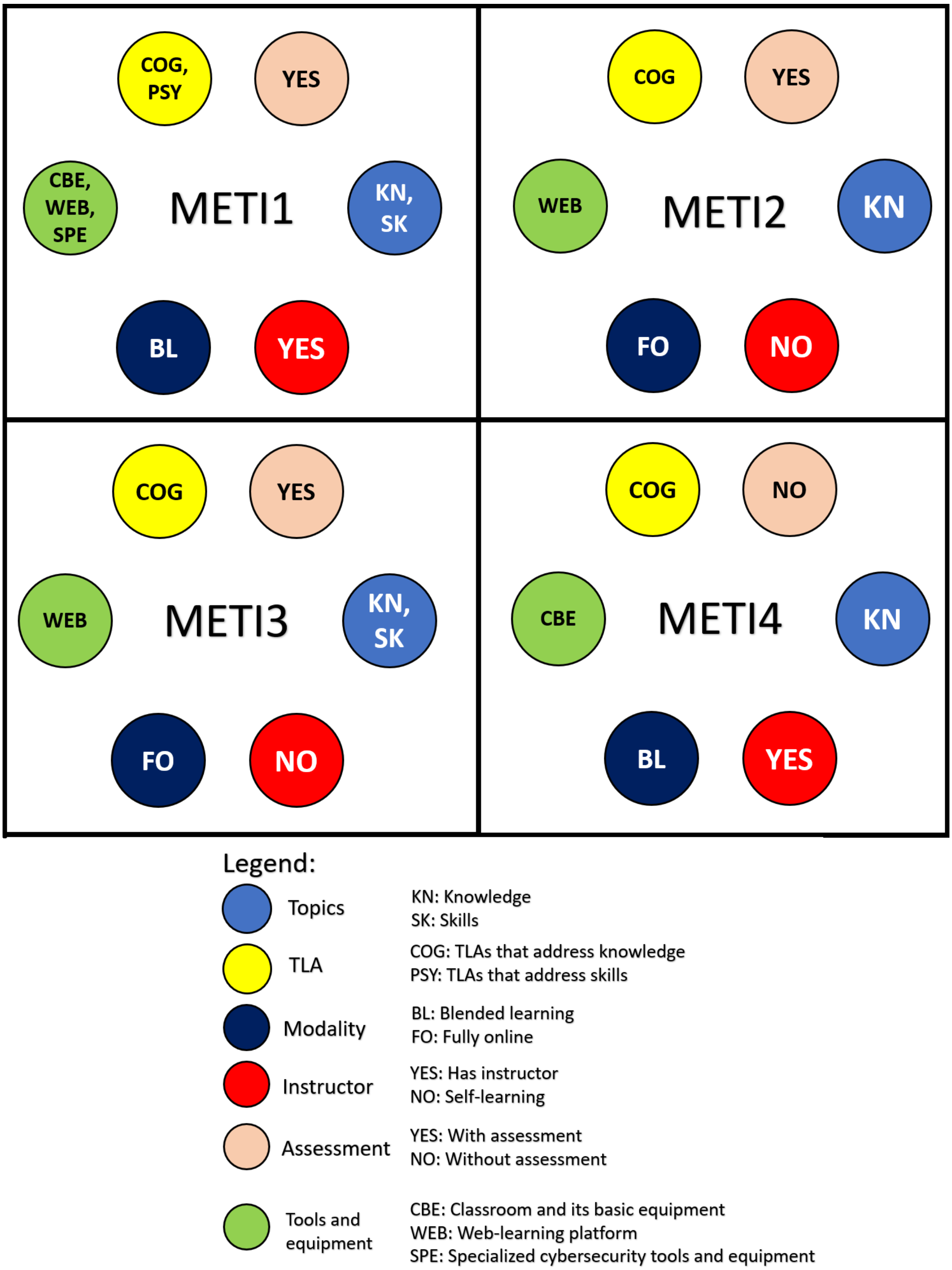


Figure 8. Summary of the Aspects of Educational Approach Employed by METIs in Delivering their Cybersecurity Course.

5.2 Discussion of educational approaches of METIs

The data presented above showed that different aspects and/or components are 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.

This study asserts that all the mentioned aspects should be present and complete in the course design and delivery of all METIs. As recalled from the literature review, 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 researcher 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 present in the observed cybersecurity courses. The researcher postulated 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.

To fully realize a training course's general aims, all the components present in a course, regardless if they are complete (in this case, six), 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 9. Training objectives can likewise be achieved when each component establishes positive relationships with the other components and maintains this consistency across all possible interactions. 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 15 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.

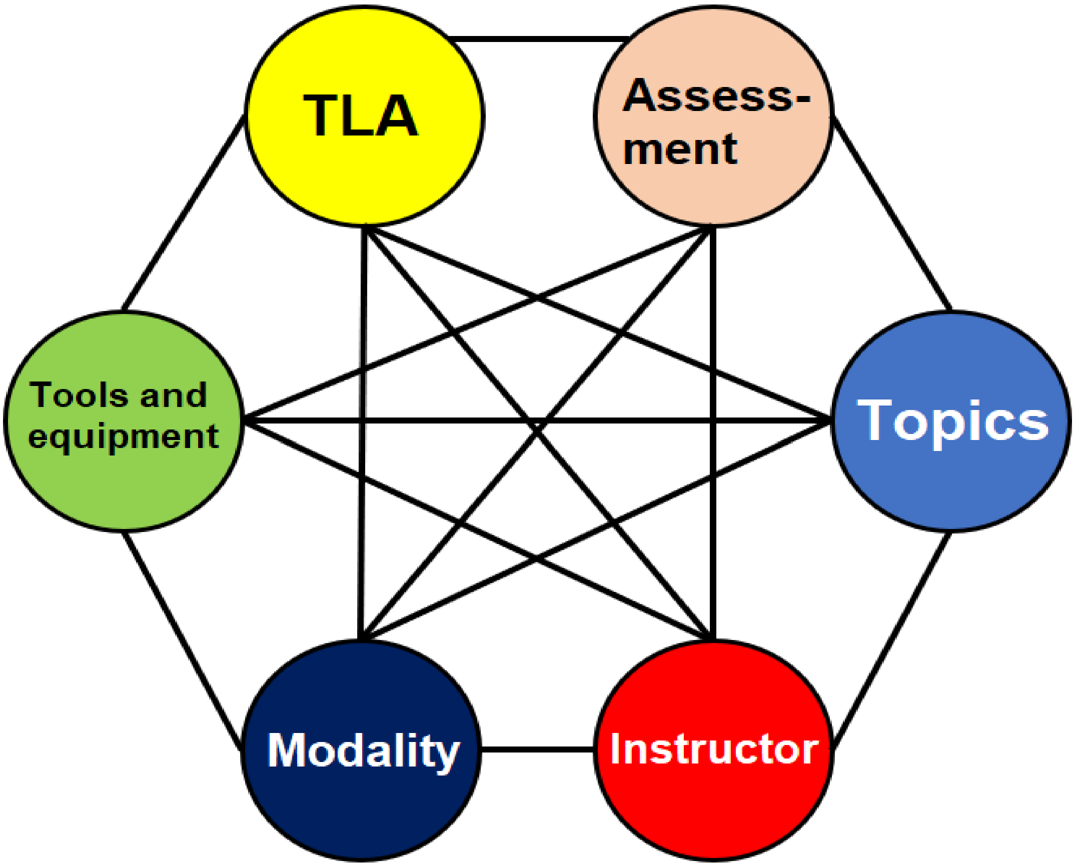


Figure 9. Analytical Framework of Strong Connection of the Aspects of Educational Approach.

Table 15.
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

5.2.1 Case 1: METI1

The educational approach of METI1 formed a ‘full lantern’ with solid lines, as shown in Figure 10.

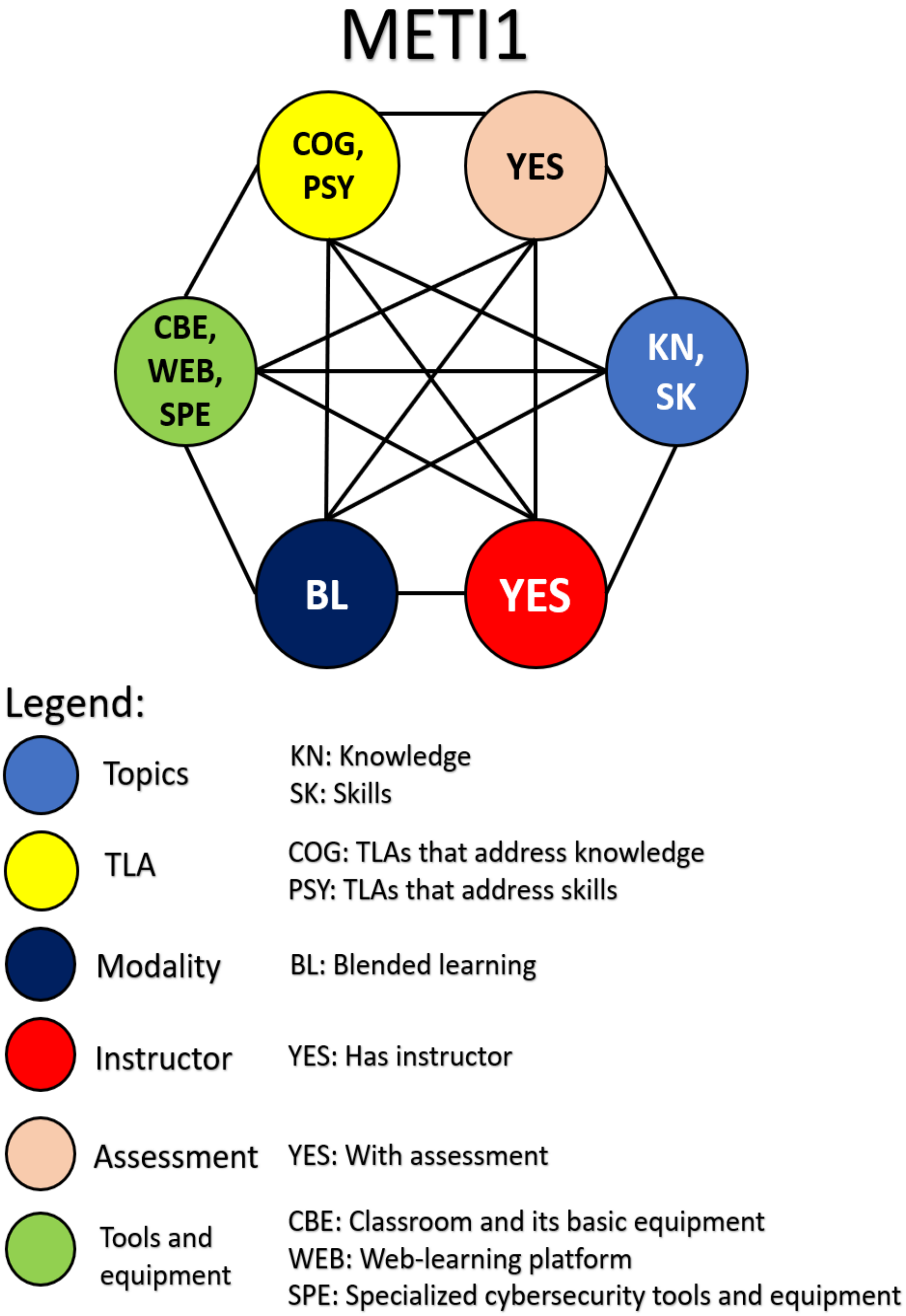


Figure 10. Visual Representation of the Educational Approach of METI1.

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 instructor is critical especially in conducting simulation exercises (Fisher & Muirhead, 2019). 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 11.

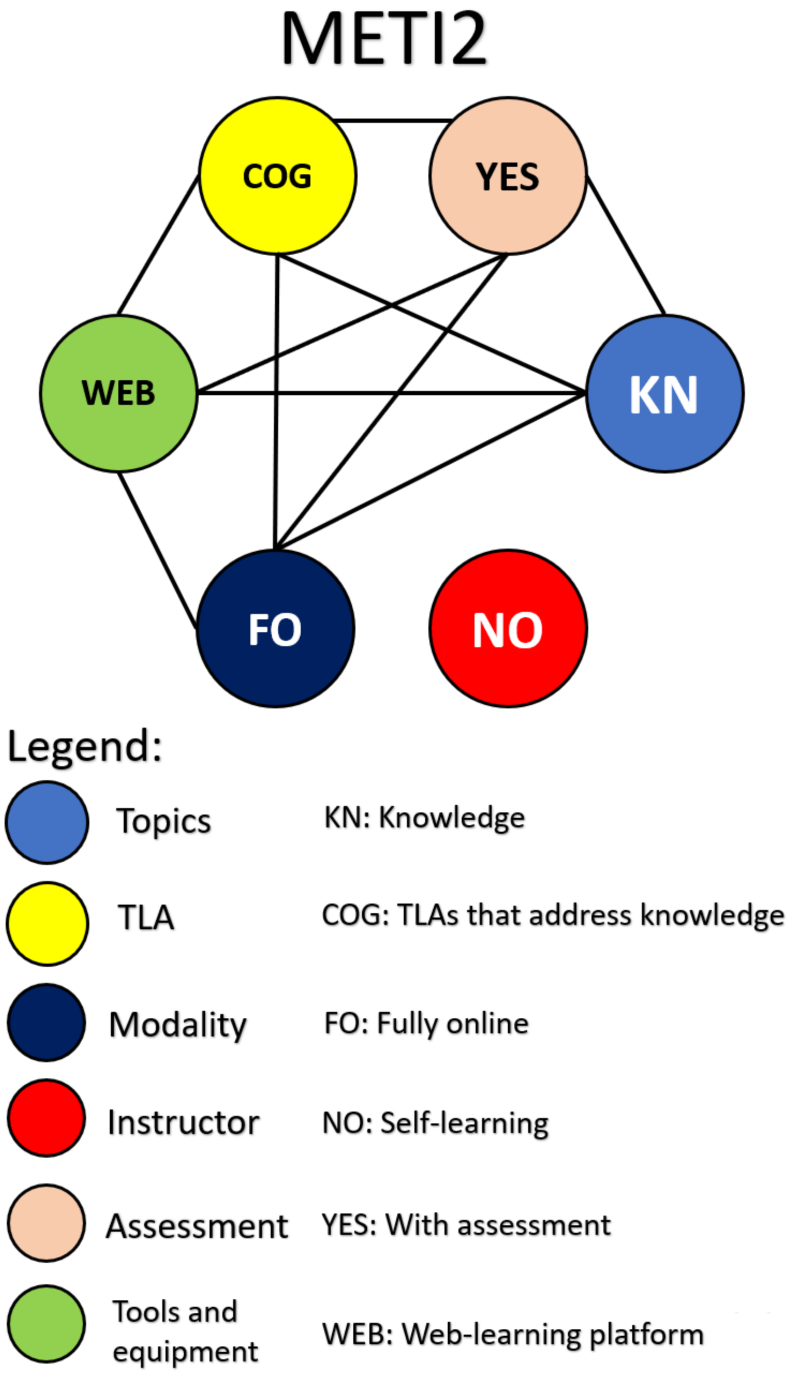


Figure 11. Visual Representation of the Educational Approach of METI2.

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 12.

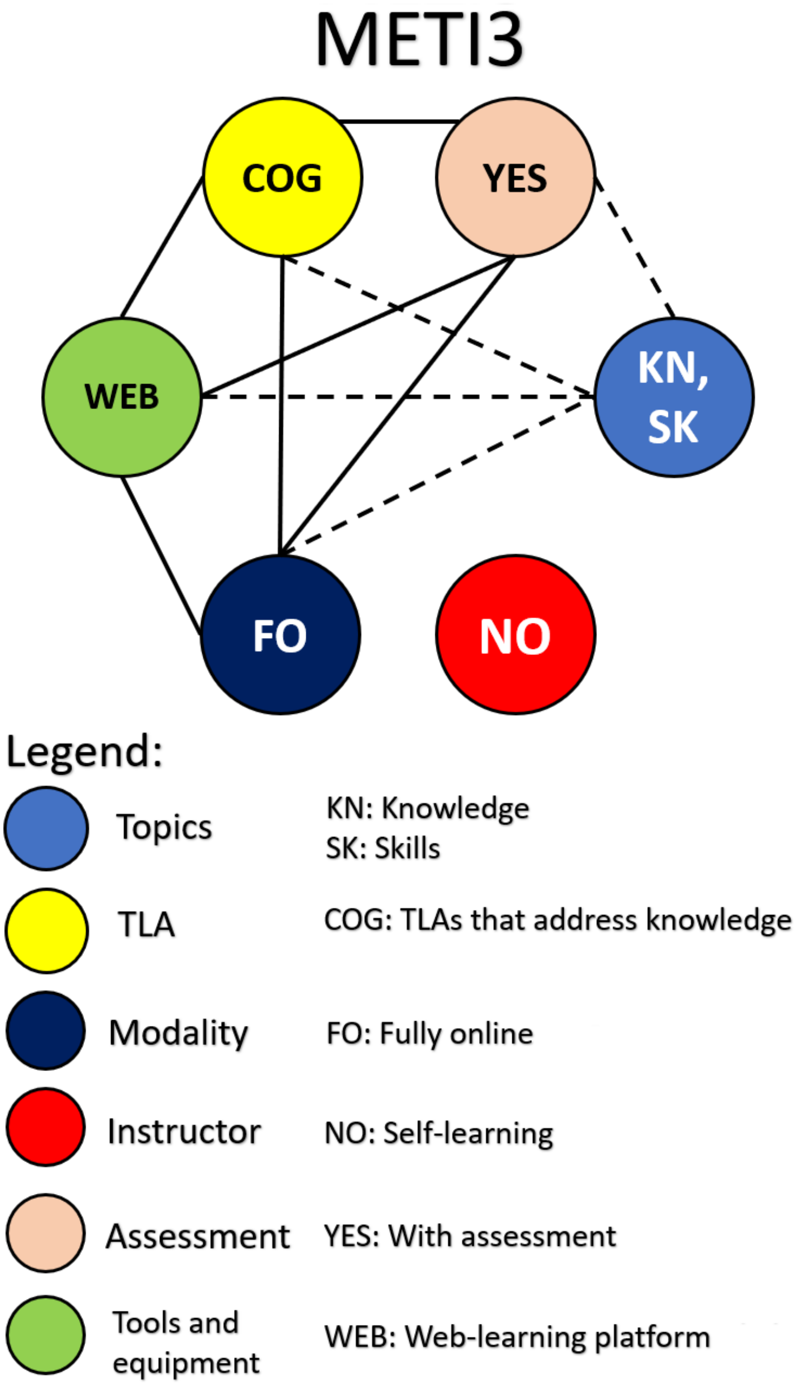


Figure 12. Visual Representation of the Educational Approach of METI3.

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., 2013), 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, it 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 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 13.

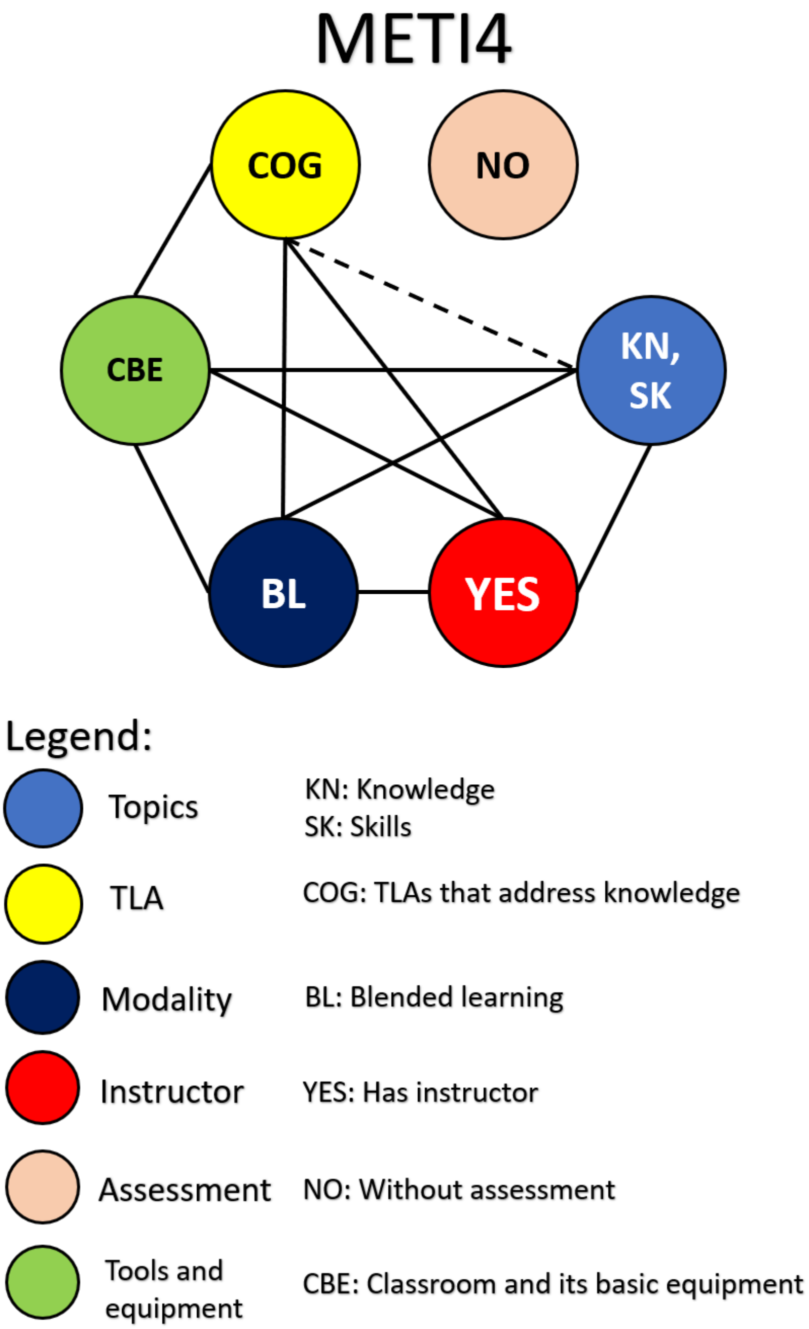


Figure 13. Visual Representation of the Educational Approach of METI4.

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, 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.

5.2.5 Convergence of cases

- METI1 and METI2

METI1 and METI2 have different educational approaches but both contributed to the attainment of their respective aims. METI1’s educational approach is described as ‘full lantern’ with all components having positive relationships with each other. Their goal is to offer a practical and skills-based cybersecurity course. On the other hand, METI2’s educational approach took the shape of an ‘incomplete lantern’ with solid lines wherein most components have positive relationships with all but the instructor. METI2’s educational approach is contingent on a full-online modality that focuses on self-paced learning of cybersecurity knowledge using a web-learning platform. The goal of METI2 was to raise awareness of cybersecurity and they deemed a self-paced online learning as adequate to attain this goal.

- METI2 and METI3

The educational approaches of METI2 and METI3 have practically the same structures with the only difference being their choice of topics. While the former focused on cybersecurity knowledge and their educational approach contributed to the attainment of their general aims, the same cannot be concluded for the latter. METI3 included skills in their training course however, their choice of modality, equipment, and TLAs do not sufficiently support the attainment of their general aims.

- METI3 and METI4

Where METI3 failed to calibrate their educational approach around the inclusion of skills in their training course, METI4 similarly did to a lesser degree and then some. The glaring omission of an assessment component sabotages their cybersecurity course and raises the question on whether any of their trainees attained the general aims of the training.

Overall, MET1 and METI2 employed distinct educational approaches that demonstrated harmony across component relationships and interactions and contributed to the attainment of their respective general aims. METI3 and METI4 failed to evaluate their educational approach as a whole for consistency, especially with the inclusion of skills in their training topics.

5.3 Collaboration

Based on the conducted interviews, all METIs that served as cases of this study valued collaboration with other agencies and/or stakeholders in the development of their courses or topics. METI1 and METI4 are members of SKILLSEA Project[5], and METI2 was involved in CYMET Project[6]. Both projects influenced the cybersecurity courses of the said cases. Moreover, METI1 and METI4 have collaborated with other organizations and stakeholders. The collaboration of METIs with other entities are shown in Figure 14.

[5] SKILLSEA is a multilateral project, engaging 27 partners from 16 European countries. It brings together social partners, maritime shipping industry, trade unions, research organizations, maritime academies and universities, education and training providers and public authorities. They all have solid expertise and knowledge on the maritime shipping sector, in order to produce a complete and sustainable strategy development cycle from skills needs identification and elicitation (current, medium and long term), design and delivery of VET, to pilot trainings, validation, revision, reapplication as well as stakeholders' mobilization and awareness raising as sustainable implementation (https://www.skillsea.eu/index.php/about/partners).

[6] Addressing Cyber Security in Maritime Education and Training (CYMET) is a project of The International Association of Maritime Universities (IAMU), a non-profit global network of leading maritime universities providing Maritime Education and Training (MET) of seafarers for the global shipping industry. CYMET is a joint project coordinated by Satakunta University of Applied Sciences (Finland) and accomplished in collaboration with Gdynia Maritime Academy (Poland) and Svendborg International Maritime Academy (Denmark)

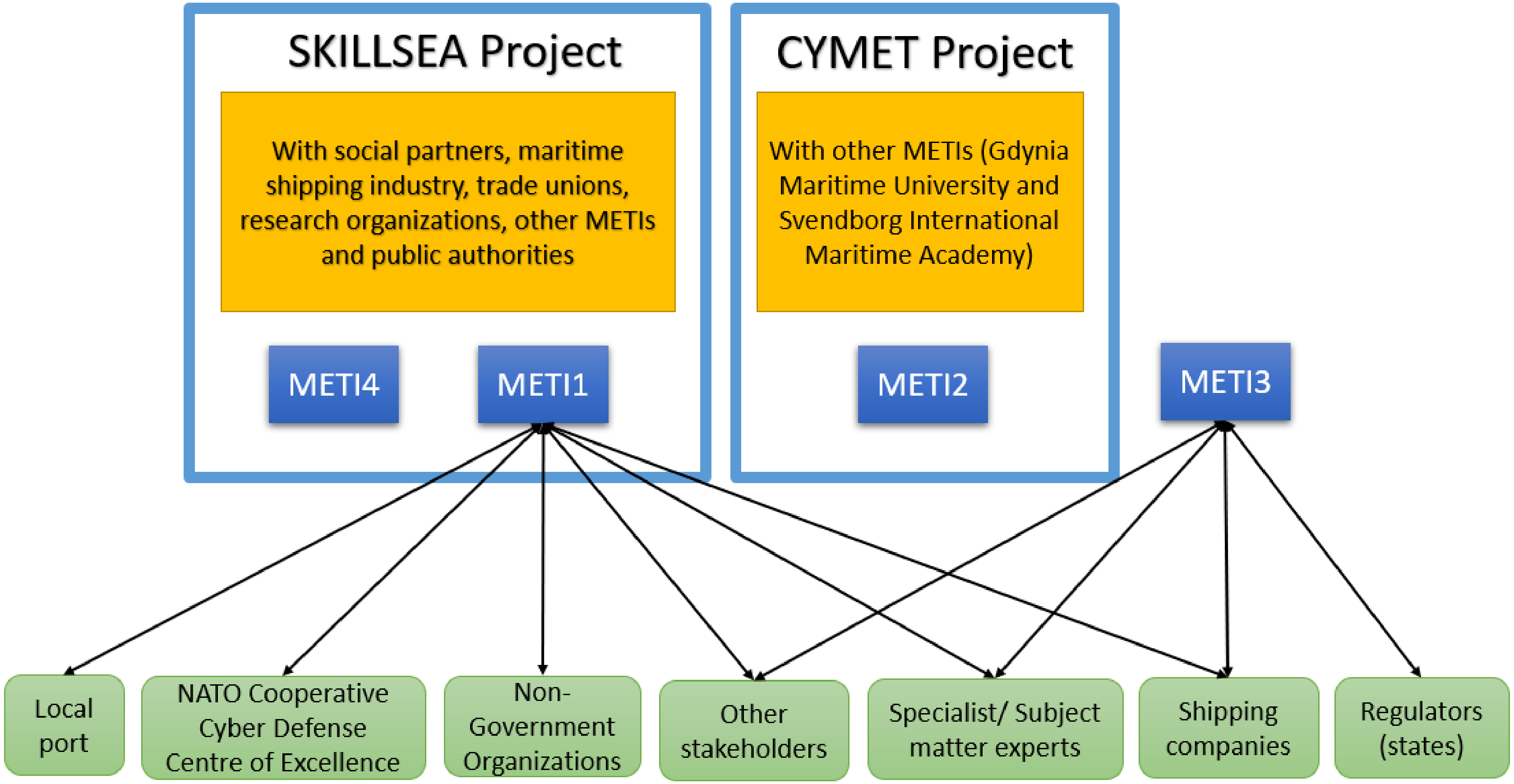

SKILLSEA Project
With social partners, maritime shipping industry, trade unions, research organizations, other METIs and public authorities
METI4
METI1
CYMET Project
With other METIs (Gdynia Maritime University and Svendborg International Maritime Academy)
METI2
METI3
Local port
NATO Cooperative Cyber Defense Centre of Excellence
Non-Government Organizations
Other stakeholders
Specialist/ Subject matter experts
Shipping companies
Regulators (states)

Figure 14. Collaboration of METIs with Other Entities.

METIs described the roles of collaboration in their cybersecurity courses as follows:

5.3.1 Collaboration guides the delivery of the course (METI1)

The collaboration of METI1 with NATO Cooperative Cyber Defense Centre of Excellence, the local port and shipping company helped them in deciding how to deliver their course in an effective way. In fact, the cybersecurity lecturer of METI1 used his learning in the collaborative project and the discussion with the port and shipping company to organize his course delivery. To quote:

> METI1: *One lecture we had there in the center* (NATO), *which is organizing the world's biggest cybersecurity exercises. The researcher* (lecturer) *is a major in Hungarian military. He gave the overview about cyber exercises; why they are important; and how they are being organized and carried out.*
>
> *What I am doing here is in parallel with one project we are doing with the shipping company and carrying out cyber risk management. Then I use that practical knowledge in classes.*

5.3.2 Collaboration helps in the development of quality reference materials (METI2)

With the contribution of the stakeholders and partner agencies, METI2 was able to use reference materials that are relevant and address the need of global seafarers. Since the contributors did not come from one university only, the pooling and organization of ideas put into a learning package ensured universality and comprehensiveness. METI2 further explained this when it quoted the final report of the project "Addressing Cyber Security in Maritime Education and Training" [CYMET] (Ahvenjärvi, 2018):

> *"One of the concrete outcomes of the CYMET project is a package of web-learning material on maritime cyber security management, developed by the partners SAMK, GMU and SIMAC and made available for all IAMU member universities. Even though it might be challenging to compose a uniform and unified set of training material produced by several teachers from different universities, this kind of collaboration can be very beneficial and rewarding. Wider collaboration between the member universities in production of web-*

> *learning material should be considered in IAMU. It could be used to enhance the quality of education and training of seafarers globally."*

The same quote also called for a wider collaboration among IAMU member universities so that the quality of education and training given to seafarers and perhaps even the would-be seafarers is optimized.

5.3.3 Collaboration enriches the content of the course (METI3 and METI4)

For METI3, collaboration is very important because through this, they make sure that what they are teaching are those that are really vital. Here, they admitted that they do not have the monopoly of the content of the course that is why they collaborate with the stakeholders.

> METI3: *The danger of not collaborating with the stakeholders in the industry who have a view, often on the topics that we are developing a piece of learning on, if you ignore them, then you might just miss one key message or a number of key messages that you really should or would want to have articulated in a piece of learning.*

METI3 was supported by METI4 and METI 1. According to METI4, their collaboration with SKILLSEA expanded the coverage of their course to be able to accommodate important and related cybersecurity topics.

> METI4: *The collaboration was very influential in the overarching design of the course. I* (course developer and instructor) *think that without the collaboration with SKILLSEA that, in my opinion*, *it would be a much narrower delivery. It will probably be more focused and limited to just the legal requirements and sort of the awareness of cyber threats.*

Through their dialogues with the local port and shipping company, METI1 was able to determine topics which were deemed necessary to develop competent seafarers; hence they should be included in the course.

> *METI1: We have quarterly meetings with a local port and a shipping company. And we ask for their feedback and discuss with them what they are expecting from seafarers who are joining their company in terms of automation, digitalization and cybersecurity.*

There were evidences that collaboration had made an impact in how the METIs designed their courses, particularly in deciding the topics to include in it. Collaboration was also beneficial in the delivery of the course, particularly for METI1. Furthermore, collaboration provides opportunities to enhance the quality of cybersecurity education and training for seafarers.

5.4 Chapter summary

This chapter 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 researcher, this paper also highlighted how the METIs regarded the relevance of the different aspects of educational approaches in their cybersecurity course. Although there were marked differences, all METIs agreed that collaboration with different stakeholders was very important since they worked with these entities in the development of their courses. Collaboration has contributed to their content formulation as well as in the delivery of their cybersecurity courses.

The contribution of collaboration with the different stakeholders to the METIs is undeniable. However, as evidenced by the data on educational approaches, the participating METIs came out lacking in either the content, the delivery or in the assessment. These deficiencies may be due to several factors as discussed in the findings section.

6. Conclusion and recommendations

6.1 Research conclusion

Any cybersecurity course, with all its aspects, is unique to each delivering METIs. 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 15. This framework will be a general guide to make the delivery of cybersecurity course of each METIs harmonized and systematized in order to achieve their course's aims and objectives.

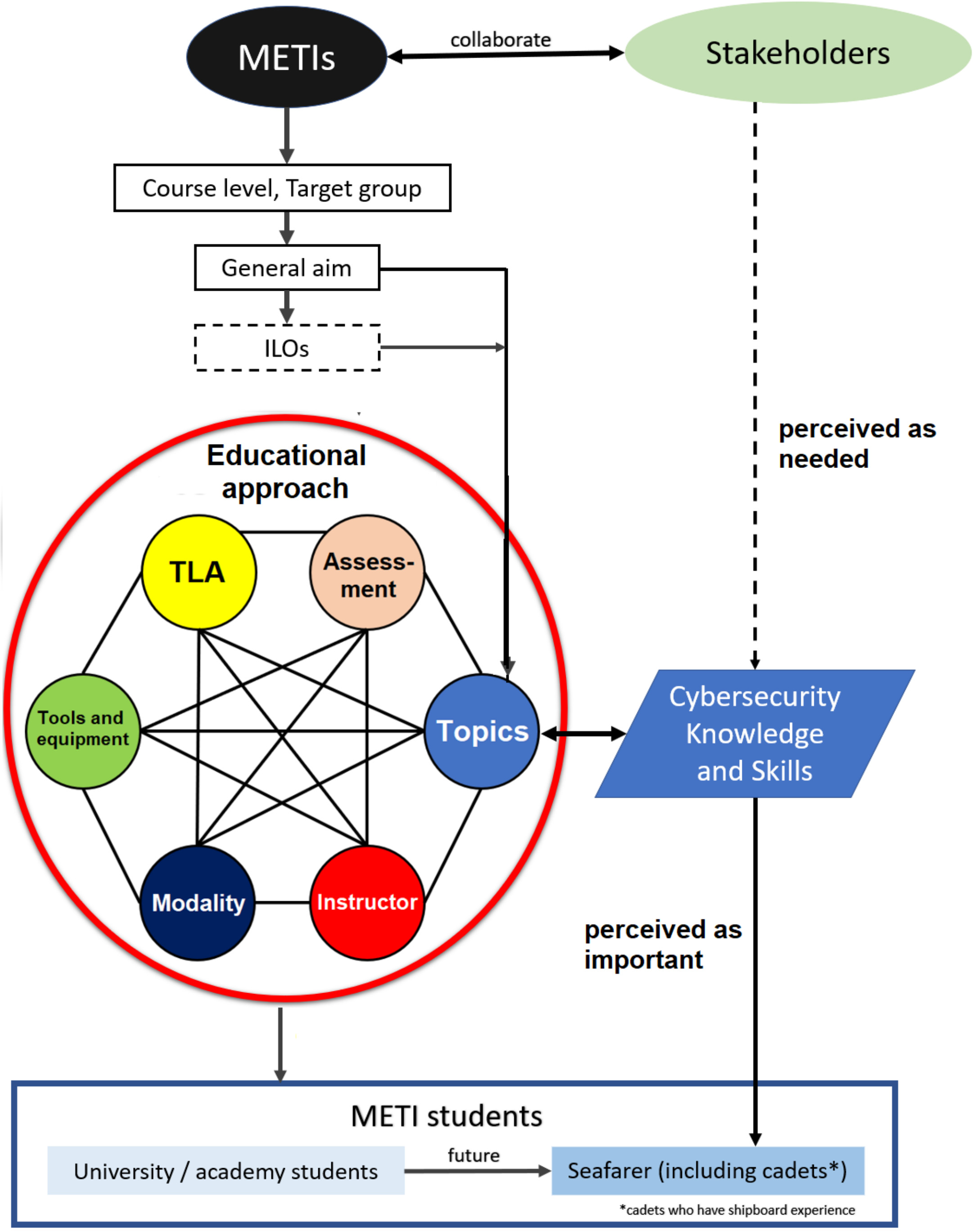


Figure 15. Overview of how the framework fits into cybersecurity education and training for seafarers.

With METIs collaborating with the stakeholders, they have identified 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 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. Further, the researcher grouped the respondents according to age, department and training experience and hypothesized that there were no significant differences in their perception. With the outcome of statistical analysis, the null hypothesis in all groups is accepted except for cybersecurity knowledge wherein those who have training experience perceive them to be more important than those who have no prior training in cybersecurity.

With active and regular collaboration with stakeholders, the common goal of making possible quality and meaningful learning experiences can be attained.

6.2 Recommendations

The following recommendations seem appropriate to the various entities within the maritime industry:

6.2.1 International Maritime Organization

- The rapid developments in maritime-related technology require novel knowledge and skills in cybersecurity, among other things. This only emphasizes the need to revisit the STCW Convention and make significant amendments that will enable seafarers to adequately perform their functions in an increasingly digitalized environment.

6.2.2 Administrations

- Incorporate maritime cybersecurity education and training in the Administrations' competence framework for seafarers in the absence of the standards prescribed by the STCW Convention in this regard.

6.2.3 METIs

- Existing METIs that deliver cybersecurity course 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.

6.3 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 researcher was 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.

- Out of 403 respondents, only three are from the galley department and one from other department in cruise/passenger ships. Future researchers can either add more respondents from these departments 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.

References

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

Alexander, R. D., & Panguluri, S. (2017). Cybersecurity Terminology and Frameworks. In: Clark, R., & Hakim, S. (Eds) *Cyber-Physical Security*, 19-47, Springer International Publishing. https://doi.org./10.1007/978-3-319-32824-9.

Alop, A. (2019). *The challenges of digital technology era for maritime education and training*. *2019 European Navigation Conference (ENC).* 10.1109/EURONAV.2019.8714176

Alsulami, A.A., & Zein-Sabatto, S. (2021). *Resilient cyber-security approach for aviation cyber-physical systems protection against sensor spoofing attacks*. [Paper presentation]. 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 565. https://10.1109/CCWC51732.2021.9376158

Ahvenjärvi, S., (2018). Addressing cyber security in training of the mariner of the future - the CYMET project. *International Association of Maritime Universities (IAMU) Secretariat.* http://iamu-edu.org/wp-content/uploads/ResearchProject_FinalReport/FY2018/20180107_Addressing-Cyber-Security-in-Maritime-Education-and-Training.pdf

Baik, C., & Larcombe, W. (2016). *Enhancing student wellbeing: Curriculum design*. unistudentwellbeing.edu.au

Bearman, M. & Dawson, P. (2013). Qualitative synthesis and systematic review in health professions education. *Medical Education, 47*(3), 252-260.

Bendovschi, A. (2015). Cyber-attacks – trends, patterns and security countermeasures. *Procedia Economics and Finance, 28*, 24-31. https://doi.org/10.1016/S2212-5671(15)01077-1

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

Bhasin, M. (2007). Mitigating cyber threat to banking industry. *The Chartered Accountant, 50* (10),1618-1624.

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

Biggs, J. & Tang, C. (2007). *Teaching for quality learning at university: What the student does* (3rd ed.). Society for Research into Higher Education & Open University Press.

BIMCO & International Chamber of Shipping [ICS] (2021). *Seafarer workforce report: The global supply and demand for seafarers in 2021*. Witherby Publishing Group.

Boyatzis, R. E., & Kolb, D. A. (1991). Assessing individuality in learning: The learning skills profile. *Educational Psychology, 11*(3/4), 279-295.

Burley, D. L., Eisenberg, J., & Goodman, S. E. (2014). Privacy and security: Would cybersecurity professionalization help address the cybersecurity crisis? *Communications of the ACM, 57*(2), 24-27.

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.

Cain, A. A., Edwards, M. E., & Still, J. D. (2018). An exploratory study of cyber hygiene behaviors and knowledge. *Journal of information security and applications*, *42*, 36-45.

Canfield, C. I., Fischhoff, B., & Davis, A. (2016). Quantifying phishing susceptibility for detection and behavior decisions. *Human Factors*. https://doi.org/10.1177/ 0018720816665025

Caponi, S., & Belmont, K. (2015). Maritime cybersecurity: A growing threat goes unanswered. *Intellectual Property and Technology Law Journal, 27* (1), 16-18.

Carlton, M., Levy, Y., Ramim, M. M., & Terrell, S. R. (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*, Ft. Worth, Texas.

Chao, R. J., & Chen, Y. H. (2009). Evaluation of the criteria and effectiveness of distance e-learning with consistent fuzzy preference relations. *Expert Systems with Applications*, *36*(7), 10657-10662.

Chi, M. T. H. (2006). Two approaches to the study of experts' characteristics. In K. A. Ericsson, N. Charness, P. J. Feltovich, & R. R. Hoffman (Eds.), *The Cambridge handbook of expertise and expert performance*, 21–30. Cambridge University Press. https://doi.org/10.1017/CBO9780511816796.002

Chicioreanu, T. D., & Amza, C. G. (2018). Adapting your teaching to accommodate the net generation/Z-generation of learners. *eLearning & Software for Education*, *3*.

Choi, M. S., 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) 2013 (Paper 29*), Milan, Italy. http://aisel.aisnet.org/wisp2012/29

Cimpanu, C. (2020). *All four of the world's largest shipping companies have now been hit by cyber-attacks.* https://www.zdnet.com/article/all-four-of-the-worlds-largest-shipping-companies-have-now-been-hit-by-cyber-attacks/

Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches.* (4th ed.). SAGE.

Creswell, J.W., & Creswell, J.D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches.* (5th ed.). SAGE.

Daum, O. (2019). Cyber security in the maritime sector. *Journal of Maritime Law and Commerce*.

Davis, B., Carmean, C., & Wagner, E. D. (2009). The evolution of the LMS: From management to learning. *e-Learning Guild*.

DeLeon, L., & Killian, J. (2000). Comparing modes of delivery: Classroom and on-line (and other) learning. *Journal of Public Affairs Education*, *6*(1), 5-18.

Dillon, H., & VanDeGrift, T. (2021). Creating an inclusive engineering student culture through diverse teams: Instructor-led and student-led approaches. In *2021 ASEE Virtual Annual Conference Content Access*.

DNV (2019). *KONGSBERG and DNV GL team up for maritime digitalization*. https://www.dnv.com/news/kongsberg-and-dnv-gl-team-up-for-maritime-digitalization-149430#

Fisher, D. and Muirhead, P. (2019). Practical teaching skills for maritime instructors. (3rd Ed.). WMU Publications*.*

Flick, U. (2018). *Doing triangulation and mixed methods*. SAGE. https://www.doi.org/10.4135/9781529716634

Fosch-Villaronga, E., & Mahler, T. (2021). Cybersecurity, safety and robots: Strengthening the link between cybersecurity and safety in the context of care robots. *Computer Law and Security Review, 41* (105528). 10.1016/j.clsr.2021.105528

Fry, H., Ketteridge, S., & Marshall, S. (Eds.). (2004). *A handbook for teaching and learning in higher education*. Kogan Page India Pvt. Ltd.

Furnell, S. (2021). The cybersecurity workforce and skills. *Computers & Security*, *100*, 102080.

Ha, E. H., & Lim, E. J. (2018). Peer-led written debriefing versus instructor-led oral debriefing: Using multimode simulation. *Clinical Simulation in Nursing*, *18*, 38-46.

Hareide, O., Jøsok, Ø, Lund, M., Ostnes, R., & Helkala, K. (2018). Enhancing navigator competence by demonstrating maritime cyber security. *Journal of Navigation, 71*(5), 1025-1039. 10.1017/S0373463318000164

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In *5th International Conference on Maritime Technology and Engineering, Lisbon, Portugal*. 10.1201/9781003216582-6

Hmelo-Silver, C. E., Duncan, R. G., & Chinn, C. A. (2007). Scaffolding and achievement in problem-based and inquiry learning: A response to Kirschner, Sweller, and. *Educational psychologist*, *42*(2), 99-107.

IMO (2017). STCW Inc. 2010 Manila Amendments, 2017 Edition.

Inmarsat (2020). *Inmarsat's most powerful satellite services enters service.* https://www.inmarsat.com/en/news/latest-news/corporate/2020/inmarsat-s-most-powerful-satellite-enters-service.html

Irons, A. (2019). Delivering cybersecurity education effectively. In *Cybersecurity Education for Awareness and Compliance* (pp. 135-157). IGI Global.

Iwendi, C., Anajemba, J.H., Biamba, C., & Ngabo, D. (2021). Security of things intrusion detection system for smart healthcare. *Electronics*, 10, 1375. 10.3390/electronics10121375

Johnson, R. B., & Christensen, L. (2019). *Educational research: Quantitative, qualitative, and mixed approaches*. SAGE.

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).

Ledger Insights (2021). *IBM, Maersk's TradeLens blockchain signs 10 Chinese partners.* https://www.ledgerinsights.com/ibm-maersk-tradelens-blockchain-signs-10-chinese-partners/

Levy, Y. (2005). A case study of management skills comparison in online and on-campus MBA programs. *International Journal of Information and Communications Technology Education, 1*(3), 1-20. doi:10.4018/jicte.2005070101

Light, G., Cox, R., & Calkins, S. (2009). *Learning and teaching in higher education: The reflective professional* (2nd ed.). Sage Publication Ltd.

Manuel, M. (2021). *EDU106 Lecture Slides*. *World Maritime University.*

McCusker, K., & Gunaydin, S. (2015). Research using quantitative, qualitative, or mixed methods and choice based on the research. *Perfusion,* 1-6. https://doi.org/10.1177/0267659114559116

Morgan, S. (2020). Cybercrime to cost the world $10.5 trillion annually by 2025. *Cybersecurity Ventures.* https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Murati, R., & Ceka, A. (2017). The use of technology in educational teaching. *Journal of Education and Practice*, *8*(6), 197-199.

National Initiative for Cybersecurity Careers and Studies [NICCS] (2014). *Cyber Glossary*. http://niccs.us-cert.gov/glossary#cybersecurity

Oksavik, A., Hildre, H.P., Pan, Y., Jenkinson, I., Kelly, B., Paraskevadakis, D. & Pyne, R. (2020). *SkillSea future skill and competence needs*. https://www.skillsea.eu/images/Public_deliverables/D1.1.3%20Future%20Skills%20and%20competence%20needs_final%20version(1).pdf

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.

Patton, M. Q. (2015). *Qualitative research & evaluation methods* (4th ed.). SAGE.

Pellegrino, W., Chudowsky, N., & Glaser, R. (Eds.). (2001). *Knowing what students know: The science and design of educational assessment.* http:///www.nap.edu/catalog/10019.html

Print, M. (1993). *Curriculum development and design* (2nd ed.). Allen & Unwin*.*

Ramsden, P. (2003). *Learning to teach in higher education* (2nd ed.). RoutledgeFalmer.

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.

Rolls-Royce (2018). *Rolls-Royce opens autonomous ship research and development centre in Finland*. https://www.rolls-royce.com/media/press-releases/2018/25-01-2018-rr-opens-autonomous-ship-research-and-development-centre-in-finland.aspx

Salah, K., Hammoud, M., & Zeadally, S. (2015). Teaching cybersecurity using the cloud. *IEEE Transactions on Learning Technologies*, *8*(4), 383-392.

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). Science learning in special education: The case for constructed versus instructed learning. *Exceptionality*, *15*(2), 57-74.

Smith, A., Ling, P., & Hill, D. (2006). The adoption of multiple modes of delivery in Australian universities. *Journal of University Teaching and Learning Practice*, *3*(2), 67-81.

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

Suri, H., & Clarke, D. (2009). Advancements in research synthesis methods: From a methodologically inclusive perspective. *Review of Educational Research, 79*(1), 395–430. https://doi.org/10.3102/0034654308326349

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. (2020). The use of cyber ranges in the maritime context: Assessing maritime-cyber risks, raising awareness, and providing training. *Maritime Technology and Research, 3*(1). https://doi.org/10.33175/mtr.2021.241410

Tokola, T. J., Schaberreiter, T., Quirchmayr, G., Englbrecht, L., Pernul, G., Katsikas, S. K., Preneel, B., & Tang, Q. (2019). A collaborative cybersecurity education program. In *Cybersecurity Education for Awareness and Compliance* (pp. 181-200). IGI Global.

Trigwell, K. (2006). An analysis of the relations between learning and teaching approaches. *Lifelong learning: Concepts and contexts*, 108-116.

The Maritime Executive (2018). *COSCO reports cyberattack at its U.S. operations*. Maritime-executive.com

United Nations Conference on Trade and Development [UNCTAD] (2020). *Review of maritime transport 2020*. United Nations Publications.

Wang P., Hayes N., Bertocci M., Williams K., & Sbeit R. (2020). The role of industry partnerships and collaborations in Information Technology education. In: Latifi S. (eds) 17th International Conference on Information Technology–New Generations (ITNG 2020). Advances in Intelligent Systems and Computing, vol 1134. Springer, Cham. https://doi.org/10.1007/978-3-030-43020-7_2

Wehr, J. (1988). Instructor-led or computer-based: Which will work best for you?. *Training & Development Journal*, *42*(6), 18-22.

Xu, L., Huang, D., & Tsai, W. T. (2013). Cloud-based virtual laboratory for network security education. *IEEE Transactions on Education*, *57*(3), 145-150.

Yin, R. K. (2018). *Case study research and applications: Design and methods.* (6th ed.). SAGE.

Zec, D., Maglic, L., Šimić, H. M., & Gundić, A. (2020). Current skills needs: Reality and mapping. https:// www.skillsea.eu/index.php/news-events/spotlight/106-read-the-full-report-on-currents-skills-needs

Appendices

Appendix A: Interview Instrument

This interview aims to determine the cybersecurity knowledge and skills taught by METIs, their educational approaches in the delivery of their cybersecurity courses and the role of collaboration in cybersecurity education and training for seafarers. Your participation is voluntary and without any payment. Your responses will be treated with the utmost confidentiality and will be kept anonymous. You may withdraw from the research at any time. Your participation is highly appreciated.

Name (optional): ____

METI: ____

Position: ____

Number of years in position: ____

This interview will be centered around the following questions:

1. What are the topics of cybersecurity knowledge and skills that you teach in your cybersecurity course?
2. What are the educational approaches that you use in delivering your cybersecurity course?
3. What is the role of collaboration in your cybersecurity course?

Thank you.

Appendix B: Survey Questionnaire

Cybersecurity Knowledge and Skills of Seafarers

Greetings!

This questionnaire is a part of the study, "Maritime Cybersecurity: Educational Approaches", a dissertation of a student taking up MSc in Maritime Affairs, specializing in Maritime Education and Training at the World Maritime University. This survey intends to find out the perception of seafarers to the cybersecurity knowledge and skills taught by METIs.

This survey questionnaire would take not more than 10 minutes of your time. The information you will provide in this form is for academic purposes only and will therefore be treated with maximum confidentiality. Your participation is very much appreciated and will form part of the success and realization of the study.

Name (optional): ___________________________

Section 1: Demographics

- Age: __ below 25 __ 25-30 __ 31-35 __ 36-40 __ 41-50 __ above 50
- Current/last vessel type boarded: __ Dry cargo __Tanker ________ Other
- Department and rank onboard: ___________________________________

Section 2: Cybersecurity Training Experience

- Have you taken cybersecurity or any related training/course before?
  __ YES __ NO
- If your answer to the previous question is YES, what cybersecurity or any related training/s or course/s did you take?

  ____

Section 3: Perception to cybersecurity knowledge and skills taught by METIs

Cybersecurity knowledge	Very important	Important	Neutral	Less important	Not important
1. External cybersecurity threats to the ship					
2. Internal cybersecurity threats posed by inappropriate use and poor cybersecurity practices					

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)					
4. How cyber risks can be reduced					
5. How to respond to a cybersecurity breach or attack					
6. The need for constant vigilance and reviews of the cyber risk management plan					
7. Importance of each individual's role and how he/she can protect himself/herself and his/her organization against cyber security threats					
8. Elements of Cybersecurity Management					
9. Password and remote connection requests					
10. Your responsibilities with cybersecurity					
11. Most common methods used by cyber attackers					
12. What to do if you become a victim of a cyber-attack					
13. What to do if your computer is infected by ransomware					
14. Risks that can occur through overuse of smart phones, tablets, laptops and social media					
15. How to achieve a					

healthy balance between work and leisure, offline and online					
16. Best practices of cyber hygiene					
17. How positive online behaviors can help to maintain concentration and focus while at work					
18. Considerations to be made before posting on social media					
19. Key steps to ensuring cyber security on board is maintained					
20. Concept of security					
21. Terminologies of cybersecurity					
22. Cybersecurity rules, guidelines, standards, and legal frameworks developed for maritime sector					
23. Cybersecurity ethics					
24. Digital forensics					
25. Risks of connecting to wi-fi					
26. Importance of secured messaging					
27. Importance of backup files					
28. Ship's vulnerability points to cyber risks					
29. Capabilities and limitations of existing protection measures onboard					

Cybersecurity skills	Very important	Important	Neutral	Less important	Not important
1. Responding to and recovering from cyber security incidents using the contingency plan.					
2. Safely using devices that can be abused by cyber attackers such as					

smart phones, personal computers and USB sticks					
3. Using VPN (Virtual Private Network)					
4. Using encrypted email services					
5. Creating back up files					
6. Cleaning the ECDIS infected with ransomware; reinstall the operating system and software and restore all the ports’ connection to AIS, GPS and other sensors					
7. Configuring firewall					
8. Facilitating information sharing and knowledge exchange of best practices					
9. Developing inventories of onboard systems with direct and indirect communication links					
10. Determining the likelihood of vulnerabilities being exploited by external cybersecurity threats.					
11. Determining the likelihood of vulnerabilities being exposed by inappropriate use.					
12. Determining the security and safety impact of any individual or combination of vulnerabilities being exploited.					
13. Reducing the likelihood of vulnerabilities being exploited through protection measures.					
14. Reducing the potential impact of a vulnerability being					

exploited.					
15. Developing contingency plans to effectively respond to identified cyber risks.					
16. Assessing the impact of the effectiveness of the response plan and re-assess threats and vulnerabilities					

END OF QUESTIONNAIRE

Appendix C: Reliability test

Because Likert scale was used in the self-made questionnaires, it is imperative to report the internal consistency reliability determined by Cronbach's Alpha coefficient. The questionnaire measuring the scale perception of importance of cybersecurity knowledge needed by seafarers yielded an excellent reliability (29 items, α = 0.976). Likewise, the set of questions measuring the importance of cybersecurity skills has an excellent reliability (16 items, α = 0.966).

Reliability Test Result

Scale	**Cronbach's Alpha**	**N of items**	**Interpretation**
Knowledge	0.976	29	Excellent
Skills	0.966	16	Excellent

Appendix D: Normality Test

Normality tests for age, department, and training experience

		Shapiro-Wilk		
Age		Statistic	df	Sig.
Cybersecurity-Knowledge	Below 25	.795	104	.000
	25-30	.739	147	.000
	31-35	.720	106	.000
	36-40	.734	32	.000
	41-50	.653	8	.001
	Above 50	.770	6	.031
Cybersecurity-Skills	Below 25	.799	104	.000
	25-30	.771	147	.000
	31-35	.791	106	.000
	36-40	.653	32	.000
	41-50	.637	8	.000
	Above 50	.612	6	.001
Department				
Cybersecurity-Knowledge	Deck	.790	221	.000
	Engine	.712	178	.000
	Other	.946	4	.694
Cybersecurity-Skills	Deck	.769	221	.000
	Engine	.731	178	.000
	Other	.927	4	.574
Training experience				
Cybersecurity-Knowledge	No	.775	234	.000
	Yes	.706	169	.000
Cybersecurity-Skills	No	.755	234	.000
	Yes	.768	169	.000
p > 0.05: normal distribution p < 0.05: non-normal distribution				

The above table presents the results from Shapiro-Wilk Test, which was used to test our numerical means of assessing normality. The Shapiro-Wilk Test is more appropriate for small sample sizes (< 50 samples), but can also handle sample sizes as large as 2000.

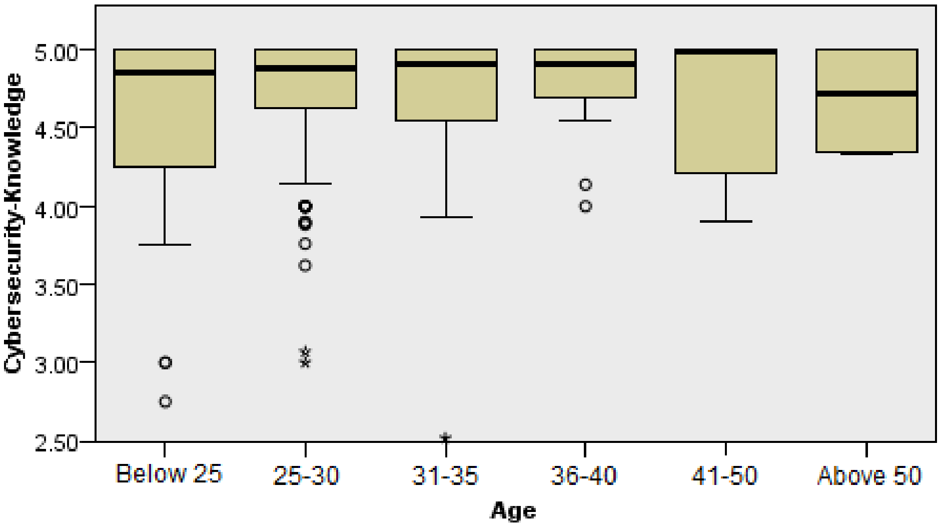
For the different groups for age, training experience, and department (except for Other), the dependent variable, “knowledge” and “skills”, was non-normally distributed (p < 0.05).

Appendix E: Hypothesis tests results for age, department, and training experience

.

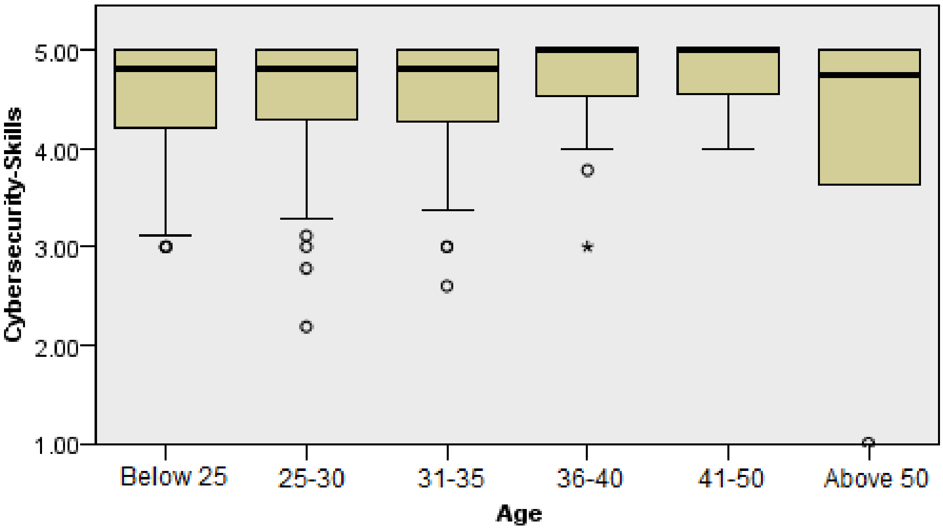
A. Kruskal-Wallis Test by Age

Independent-Samples Kruskal-Wallis Test



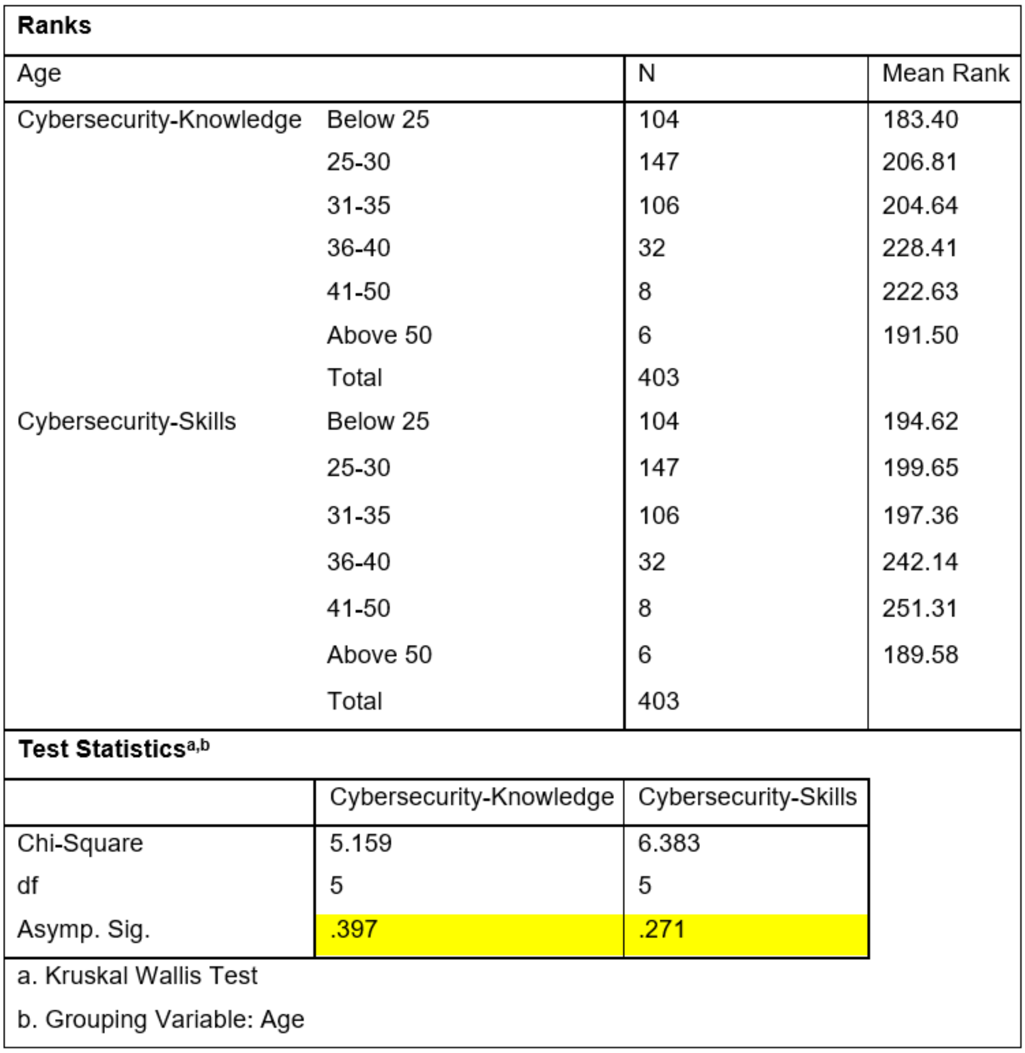
Cybersecurity knowledge

Independent-Samples Kruskal-Wallis Test



Cybersecurity skills

Table of hypothesis test results for age



Ranks

Age		N	Mean Rank
Cybersecurity-Knowledge	Below 25	104	183.40
	25-30	147	206.81
	31-35	106	204.64
	36-40	32	228.41
	41-50	8	222.63
	Above 50	6	191.50
	Total	403	
Cybersecurity-Skills	Below 25	104	194.62
	25-30	147	199.65
	31-35	106	197.36
	36-40	32	242.14
	41-50	8	251.31
	Above 50	6	189.58
	Total	403	

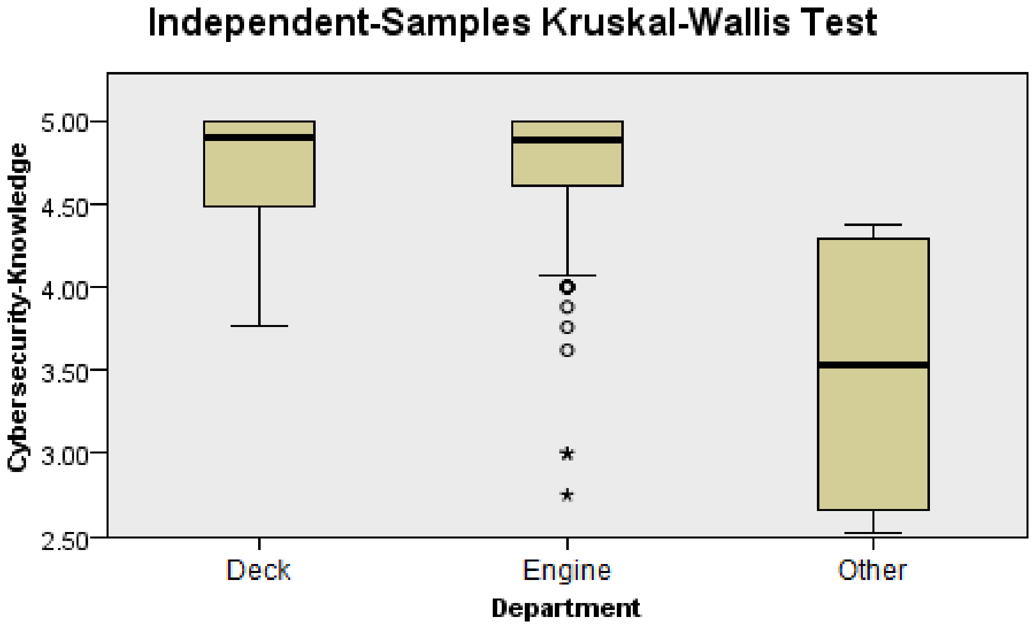
Test Statistics[a,b]

	Cybersecurity-Knowledge	Cybersecurity-Skills
Chi-Square	5.159	6.383
df	5	5
Asymp. Sig.	.397	.271

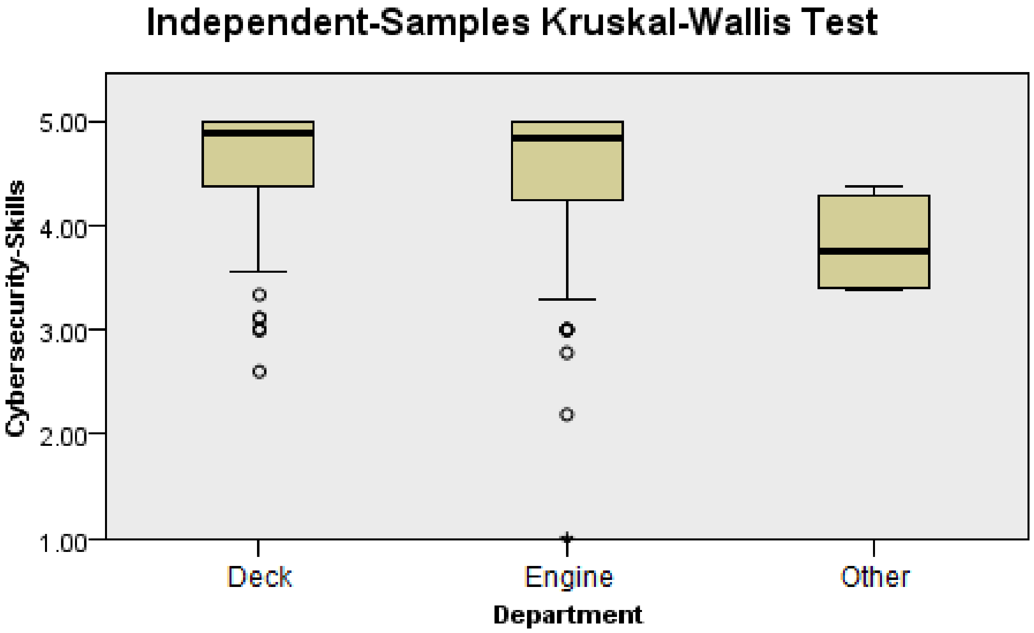
a. Kruskal Wallis Test

b. Grouping Variable: Age

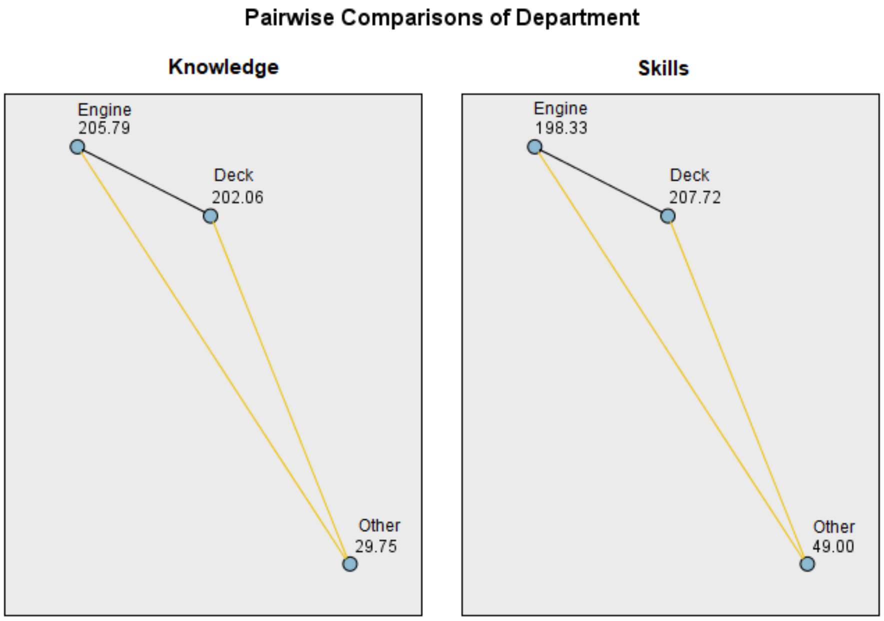
B. Kruskal-Wallis Test by Department



Cybersecurity knowledge



Cybersecurity skills



The pairwise comparison of departments shows that deck and engine departments do not have a statistical significant difference in terms of perception of importance to cybersecurity knowledge and skills.

Table of hypothesis test results for department

Ranks

Department		N	Mean Rank
Cybersecurity-Knowledge	Deck	221	202.06
	Engine	178	205.79
	Other	4	29.75
	Total	403	
Cybersecurity-Skills	Deck	221	207.72
	Engine	178	198.33
	Other	4	49.00
	Total	403	

Test Statistics[a,b]

	Cybersecurity-Knowledge	Cybersecurity-Skills
Chi-Square	9.409	8.169
df	2	2
Asymp. Sig.	.009	.017

a. Kruskal Wallis Test

b. Grouping Variable: Department

C. Mann-Whitney U Test by Training

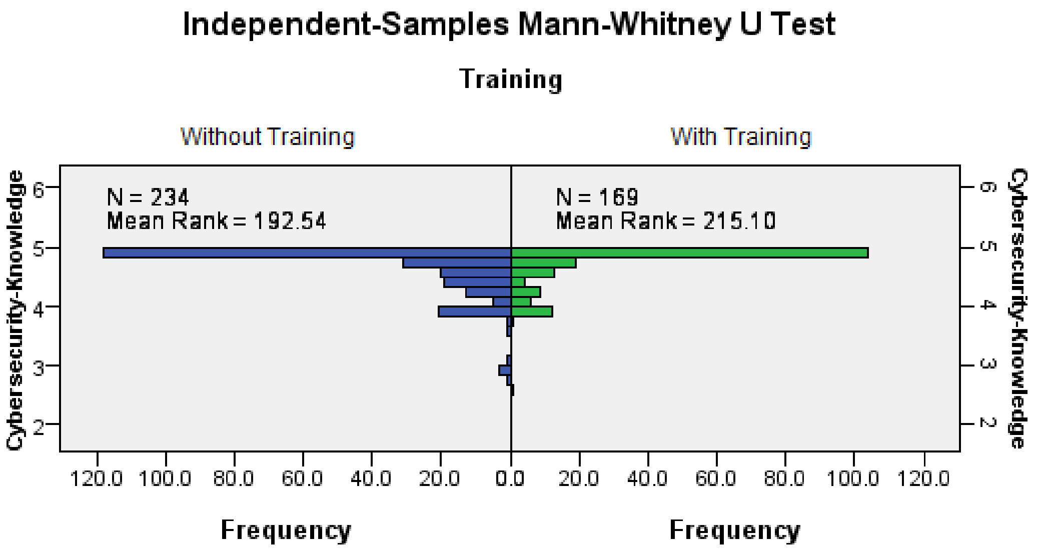
Ranks

Training		N	Mean Rank	Sum of Ranks
Cybersecurity-Knowledge	No	234	192.54	45054.50
	Yes	169	215.10	36351.50
	Total	403		
Cybersecurity-Skills	No	234	195.68	45788.50
	Yes	169	210.75	35617.50
	Total	403		

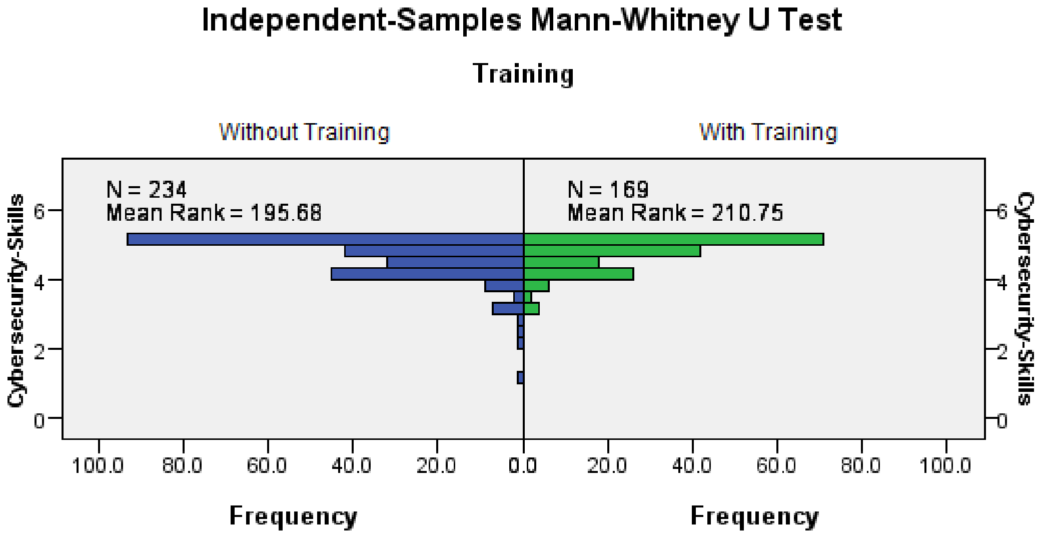
Test Statistics[a]

	Cybersecurity-Knowledge	Cybersecurity-Skills
Mann-Whitney U	17559.500	18293.500
Wilcoxon W	45054.500	45788.500
Z	-1.968	-1.328
Asymp. Sig. (2-tailed)	.049	.184

a. Grouping Variable: Training



Cybersecurity Knowledge



Cybersecurity Skills