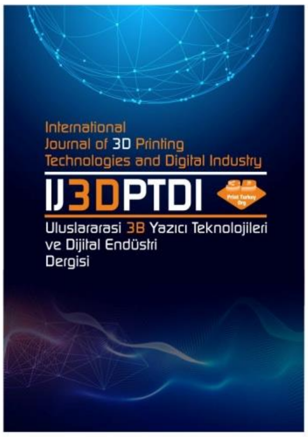
International
Journal of 3D Printing
Technologies and Digital Industry
IJ3DPTDI
Uluslararasi 3B Yazıcı Teknolojileri
ve Dijital Endüstri
Dergisi

ULUSLARARASI 3B YAZICI TEKNOLOJİLERİ
VE DİJİTAL ENDÜSTRİ DERGİSİ

INTERNATIONAL JOURNAL OF 3D PRINTING
TECHNOLOGIES AND DIGITAL INDUSTRY

ISSN:2602-3350 (Online)

URL: https://dergipark.org.tr/ij3dptdi

AN EVALUATION OF STUDENTS' CYBERSECURITY AWARENESS IN THE MARITIME INDUSTRY

Yazarlar (Authors): İsmail Karaca*, Ömer Söner

Bu makaleye şu şekilde atıfta bulunabilirsiniz (To cite to this article): *Karaca İ., Söner Ö., “An Evaluatıon of Students' Cybersecurıty Awareness In The Marıtıme Industry” Int. J. of 3D Printing Tech. Dig. Ind., 7(1): 78-89, (2023).*

DOI: 10.46519/ij3dptdi.1236264

Araştırma Makale/ Research Article

Erişim Linki: (To link to this article): https://dergipark.org.tr/en/pub/ij3dptdi/archive

AN EVALUATION OF STUDENTS' CYBERSECURITY AWARENESS IN THE MARITIME INDUSTRY

İsmail Karaca[a,b]*, Ömer Söner[b],

[a]İstanbul Technical University, Maritime Faculty, Maritime Transportation Management Engineering Department, Türkiye
[b]Van Yüzüncü Yıl. University, Maritime Faculty, Maritime Transportation Management Engineering Department, Türkiye

* *Corresponding Author: ismailkaraca@yyu.edu.tr*

(**Received:** 16.01.2023; **Revised:** 21.03.2023; **Accepted:** 25.04.2023)

ABSTRACT

Maritime operations have now become faster, safer, and more secure than before, as technological changes in the maritime industry have increased significantly over the past decade. However, no matter how advanced the technology is, removing the human variable from maritime operations is still impossible. Cybersecurity is one of the primary concepts that both enhance human adaptation to technology and reduce risk within the maritime industry. Training and raising situational awareness of maritime cybersecurity are the most basic of many defences to reduce vulnerabilities resulting from human beings not adopting technological changes. Therefore, this study proposes that maritime students' cybersecurity awareness should be investigated. For this purpose, a questionnaire is used, including 3 attitude scales. This is presented and applied to a sample group including 168 participants representing the population. This evaluation of students' cybersecurity awareness is aimed to provide taking the first steps to raise cybersecurity awareness in the maritime industry. In this study after a comprehensive investigation, quite striking findings have been obtained regarding awareness of maritime students' cyber security, and suggestions are made to increase students' cybersecurity awareness in the maritime industry.

Keywords: Awareness, Cybersecurity, Human Factor, Maritime Students.

1. INTRODUCTION

Despite all that it offers, the effects of the usage of technology cannot be predicted even using new technological methods [1]. According to [2], technology is widely used in many industries due to its advantages such as increased security and easy accessibility. (Matt et al [3]) says that there has been an increase in the number of initiatives to explore new digital technologies and take advantage of their benefits and that these initiatives often involve the transformation of core business operations, products, processes, organizational service structures, and management concepts. As a requirement of the global economy, the concepts of Operational Technology (OT) and Information Technology (IT) are gaining more and more importance [4]. According to [5], there are multi-level effects of using OT and IT in ensuring the sustainability of digitalization. Undoubtedly, the maritime industry has been and will continue to be affected by digitalization. Even [5] stated that OT and IT have the potential to completely change maritime operations and ship-related activities.

IT and OT are not new concepts for industries, being instead similar concepts to the Internet of Things (IoT) [6]. When IoT is mentioned, it should not be understood that only devices connect to the internet. When objects are equipped with sensors and electronic circuits, they gain abilities to communicate with people and update their status information [7]. In recent years, digitization like IoT has emerged as an important economic driving force that accelerates growth and facilitates job creation because its digital connectivity services have been adopted by consumers, businesses, and governments. In the maritime industry, with

technological developments such as the IoT and digitization, there have been seen transformations that provide huge economic gains, as in the example of Singapore [8]. Digitalization and IoT offer great opportunities for stakeholders of the maritime industry, whenever the right planning is made, and the plan can be implemented with the right tools.
The goal, of course, is that ships should be completely unmanned, and autonomous ships may be introduced. The International Maritime Organization (IMO) is the United Nations (UN) specialized agency responsible for the safety and security of shipping and is creating regulations to deal with completely unmanned maritime transportation [9]. According to the most recent IMO regulations, except for fully autonomous degrees, all ships require certain human operators and commands. In short, human beings are an important element of maritime transportation and will continue to be so soon. However, human adaptation to technological developments within the maritime industry leads to vulnerability. This vulnerability may be predicted but cannot be forestalled by taking precautions. Defining and determining maritime cyber vulnerabilities to attacks and threats, as well as defences, should be adopted as an integral part of each maritime operation. There is a problem with people's familiarity with cybersecurity.

Cybersecurity is defined as a computing-based discipline involving the creation, operation, analysis, and testing of secure computer systems [10-11]. Maritime cyber vulnerabilities include those in offices on shore, terminals, the supply chain, and the onboard infrastructure. Maritime cyber-attacks include malware, social engineering, phishing, water holing, port scanning, built-in software weaknesses, third-party contributions, brute force, distributed denial of service (DDoS), spear-phishing, and subverting the supply chain; maritime cyber threats are categorized as targeted, untargeted, intentional, and unintentional. The human factor is separately examined and considered to be a threat [12]. Maritime cyber defences are not exactly specific, but legislation and educations are essential for defences. Therefore, first of all, it is necessary to measure seafarers' awareness of cyber security.

Within (IMO [13]), the IMO developed and adopted some legal policies such as recommendations for managing cyber risks in the maritime industry, cyber risk management in maritime security management systems, and Resolution MSC. 428 (98), recommendations for cybersecurity on ships. Other authorities like BIMCO, which is an international organization, the US Coast Guard, and the UK government worked to arrange legislation to prevent cyber threats [14–16]. However, technological developments are not only improving maritime transportation but also cybercrime. Cyber threats and attacks are developed swiftly so there are still deficiencies regarding what these threats are and the measures to be taken against them [17] IMO regulations are basic legislations ensuring ship safety and security internationally and include the International Convention for the Safety of Life at Sea (SOLAS), Standards of Training Certification and Watchkeeping (STCW), MET, the International Safety Management (ISM) Code, and the International Ship and Port Facility Security (ISPS) Code. These all work to deal with the ever-growing threat of cyber security. Comprehensive and detailed legislation, including entirely new regulations, is necessary because technological developments have the potential to change all maritime operations via maritime safety and security.

When maritime legislation regarding technological developments is well-regulated, its contribution is obvious. This contribution lies in it providing shipping, accelerating the cargo handling operations of the ships, and making the commands and manoeuvres of the ships more safe and secure [18]. ECDIS, AIS, communication devices, and similar technological devices speed up maritime operations and ensure less human activity. However, the human factor is not completely removed from operations and, for safe navigation of the ship, continue to be an essential part of maritime operations. This in turn leads humans to be a cause of maritime accidents and incidents [19]. There could be security vulnerabilities that result from the adaptation of humans to advanced technology [20]. Furthermore, according to [21] human and machine intelligence are complementary for solving maritime operations problems. Until completely unmanned maritime operations are achieved, humans will continue to be a key factor in maritime operations. Human errors however have caused new maritime losses [22].

Especially human nonadaptation to technological developments could bring about maritime losses. For instance, cyber incidents can lead to loss of life, loss of control over ships or sensitive data, as well as ship and/or cargo hijacking [23]. Cybersecurity awareness measurement, which is the first step in achieving adaptation, is essential.

Just as the human factor is the key factor for maritime operations, it is also highly important for cybersecurity. The human factor is the weakest link within maritime cybersecurity [12]. What needs to be done to prevent economic and operational losses because of cyber-attacks is clear: to improve education and increase maritime cybersecurity [24]. Together with technological developments in the maritime industry, many issues of Maritime Education and Training (MET) programs need to be addressed and investigated to identify their strengths and limitations [25]. The most important of these issues is maritime cybersecurity. It can be thought that cyber security measures can be achieved in this way, but it is necessary to measure students' cyber security awareness in order to develop METs.
Maritime cybersecurity is a basic concept of not only maritime security but also all maritime operations including maritime safety, navigation, loading and discharging operations, and maritime communication because, in these operations, technological devices, networks, and connections are used. There is an awareness of increased technological developments in maritime companies, but it was stated by (Wang et al. [26]) that this should be supported by training. Situational awareness on this topic must urgently be raised because of the dramatic increase in technological developments in the maritime industry. According to (Kimberly et al. [27]), training to raise awareness is the first line of defense against cyber and cyber-physical threats, as well as future threats.

In recent years, maritime science has drawn attention to cybersecurity awareness. In some studies that present cyber security threats and weaknesses that may be encountered in navigation, the lack of cybersecurity awareness has been pointed out [28–30]. Suggestions have been made regarding the cyber security threat to ships, such as the study conducted for ECDIS, which is a technological and mandatory requirement on ships [31]. In recent years, some unexpected events like the Covid-19 epidemic have accelerated digitalization. This increase has underlined the importance of the concept of cybersecurity for ships, and the concepts of cyber awareness have come to the fore in such studies [32]. There has been also a study that draws attention to the importance of education in cyber awareness [20]. In a further study that included a cyber risk assessment, awareness was likewise highlighted [33]. It is seen that awareness and training are considered two important topics in the cybersecurity management system [34]. Survey studies on seafarers also mention the lack of cyber security awareness among seafarers [17] [35]. It has been found that sharing rules and information does not have a positive effect in terms of cybersecurity awareness in the maritime industry [36]. The common conclusion of all the studies encountered is this: there are deficiencies in ships' cybersecurity awareness [37]. In light of previous studies, it is clear that raising cybersecurity awareness is one of the most important conditions required to ensure more safe and more secure maritime operations, faster and larger volume transportation, and the many benefits of technological developments for the maritime industry are raising cybersecurity awareness.

The next question to be asked is to whom this training should be first targeted. Maritime students are the future of the maritime industry. Existent seafarers' awareness is important but younger students need also to adopt cybersecurity. It is assumed by many that maritime students, being largely digital natives, are more familiar with cyber security; however, this assumption has not been proven. For this reason, in this study maritime students' cybersecurity awareness is investigated. It is, therefore, possible to interpret the issue of education promoting cybersecurity, thanks to maritime students, who are the output of MET.
This study uses a comprehensive 5-point Likert-type questionnaire to evaluate students' cybersecurity awareness, applies the aforementioned questionnaire to the sample representing the relevant universe, and evaluates the data formed with the results of the applied questionnaire with the analyses accepted in the literature. The aim is to have evaluated maritime students' cybersecurity awareness, as a first step to raising cybersecurity awareness in maritime

transportation. The target of this study is to take the first step of predicting incidents caused by human error, by evaluating maritime students' cyber security awareness. After that, researchers will more easily be able to ascertain ways to improve maritime cybersecurity awareness.

In this study, firstly, the hypothesis created for the evaluation of maritime students' cybersecurity is explained in section 2 and the method used to evaluate the hypothesis defined previously is explained in section 3. The necessary analysis for assessment of the method is explained in section 4, the findings and results are included in section 5, and discussions of this study are included in section 6. Finally, conclusions are drawn in section 6.

2. HYPOTHESIS

There are many cyber threats in shipping. If they are categorized in the literature, nine categories exist physical access, operating system support, and security patches, operating system configuration, Internet connection establishment, authorized access, awareness, policies and procedures, training, continuous evaluation, and improvement [31]. The crew's lack of awareness of general cyber procedures is considered a threat. It is assumed that the youth growing up at this age are aware of the general cyber security required by all forms of technology. Our first motivation, which is the starting point of this study, is to investigate whether this assumption is true.

H1 Maritime students have been made aware of general cyber security operations.

One of the most important pillars of cybersecurity is the right to protect personal data. For this reason, information security is also considered in cyber security [38]. Before investigating cybersecurity awareness on ships, it is necessary to measure information security awareness, which is essential for maritime cybersecurity awareness. It is thought that students have general knowledge about information security, just as they have general cyber security awareness. Therefore, our second hypothesis in this study is that students are familiar with information security.

H2 Maritime students have taken the necessary precautions against cyber security threats related to information security.

Maritime authorities have intensified their cybersecurity awareness studies over the last 10 years. Therefore, in its "Guidelines on Maritime Cyber Risk Management", the IMO stated that effective cyber risk management would be possible if all seafarers, starting from the highest rank, adopt maritime cyber risk awareness [39]. In this respect, awareness of maritime students who would take part in all levels of the maritime industry is essential. It is vital for seafarers, including maritime students, to be aware of the cyber security hazards and precautions required on board, in terms of cyber security [29]. This is also expected from maritime students.

H3 Maritime students are familiar with cyber threats on ships and the precautions to be taken against these threats.

3. METHOD

In this study, alternative hypotheses explained in section 2 are used. In line with the hypotheses, a questionnaire is created using the items shown in Table 1, and a 5-point Likert scale (from (5) strongly agree to (1) strongly disagree) is used for the questionnaire. Items in the questionnaire are shown in Table 1.

Table 1. Item number and items descriptions.

Number	Item
I1	I know the requirements for a strong password.
I2	I am aware of the need for a strong password.
I3	I would never share my passwords with a friend.
I4	I use one strong password for different websites and accounts.
I5	I prefer my devices to be updated automatically.
I6	I am careful when opening email attachments and links.
I7	I only use reliable and reputable sites when surfing the web or downloading content.
I8	I take care not to discuss sensitive/critical information in public.
I9	I am familiar with appropriate methods for transmitting, storing, labelling, and processing sensitive/critical information.
I10	I routinely back up my sensitive/critical data.

I11	I always make use of encryptions when emailing my sensitive/critical data.
I12	I know how/when hardware and mobile devices should be encrypted.
I13	I am aware that posting messages on social sites or posting sensitive data or using third-party storage may violate policies or regulations.
I14	I know how to protect myself from "social engineering" "phishing" and "cyber-crime".
I15	I understand that the web address displayed in an email may differ from the link to which it will redirect.
I16	I know that emails with attachments are the most common method of cyber-attack.
I17	I know what a DDoS attack is and how it can disrupt or slow down the ship's IT systems or network services.
I18	I am familiar with the manipulations of seafarers to gain access to the ship's critical systems and networks and to break a ship's security procedures.
I19	I know the negative effects of seafarers using their own devices on board.
I20	Seafarers are a key factor in cybersecurity vulnerabilities.

Concepts of general cyber security and information security are interchangeable concepts. However, in this study according to hypotheses these concepts are different from each other based on a similar study in literature [40]. The general concept of cyber security specifically addresses what comes with technology, such as passwords, emails, automatic updates, and these risks. In the concept of information security, information security topics such as information, critical/sensitive information, and data are investigated.

Scales for hypothesis, items for scales, and their references given are shown in Table 2 and are taken as a basis. As a result of the hypotheses explained in section 2, the scales and items in Table 2 are determined to test the hypotheses. They are taken from the references listed in Table 2. Items are decided to literature given by references considering the hypotheses. They are accepted scales by literature.

Table 2. Hypothesis, Scale, Item number, References.

Hypothesis Number	Hypothesis	Scale	Item number	References
H1	Maritime students have been aware of general cyber security operations	General Cybersecurity Awareness	I1, I2, I3, I4, I5, I6, I7, I14, I15, I16	[40]
H2	Maritime students have taken the necessary precautions against cyber security threats related to information security	Information Security Awareness	I8, I9, I10, I11, I12, I13	[40]
H3	Maritime students are familiar with cyber threats on ships and the precautions to be taken against these threats	Ship Cybersecurity Awareness	I17, I18, I19, I20	[23]

The participants in this study are students at all levels studying in Turkish Maritime Institutes (Maritime High School, Maritime junior technical college, Maritime faculty, Advanced degree institute for Maritime Studies). Convenience sampling has been used as the sampling method due to easy accessibility, volunteerism, and low cost [41]. The questionnaire is implemented to the participants via the internet [42]. Google Forms is used for administering the questionnaire to the participants and obtaining the data. The link is shared with the sampling group representing the population. In Turkey, there are totally 22,276 maritime students, 12,165 students are in high school, 10.111 students are in associate degree and bachelor's degree (amount of students in advanced degree are insignificant) [43]. These students are the population for this study. 168 participants constitute the sampling group. The sampling group represents the full population because their categorical distribution, shown in Table 3, is almost the same as that of the sample group. The data is converted to be used in SPSS.

Therefore, this sample group can be used for the population. It doesn't look like men and women are equally spread out in Table 3, but women constitute a very little bit of currently active seafarers. So, this is an acceptable distribution.

Table 3. Categorical distribution of participants' demographical and educational information.

%	%	%	%
Student of	Age	Class	Sex
27.38	26.19	8.33	88.69
High school	13-17	Preparatory	Male
2.38	60.12	25	11.31
Associate degree	18-23	First-year	Female
69.64	12.5	19.05	
Bachelor's degree	24-30	Second-year	
0.6	1.19	17.26	
Advanced degree	30+	Third-year	
		30.36	
		Fourth-year and more	

To continue, the next step is analysis. In this study, descriptive analysis is used to investigate the hypothesis. However, Analyses regarding the validity and reliability of the data used in the study will be explained in the next section.

4. ANALYSIS

For analysis, IBM SPSS Statistics 20 is used in this study. Cronbach's coefficient alphas are used for Reliability analysis. The value of the number of components, and Cronbach's Alpha, are given for all scales in Table 4 for reliability analysis. KMO values and Cumulative (%) rotation values are used for the adequacy of the sample and the validity of the descriptive analysis to be made. The cumulative rotation is reasonable and does not suffer from an insufficient number of participants.

Table 4. Results for reliability and validity analysis.

Scale	Number of components	Cronbach's Alpha	KMO value	Cumulative (%) rotation
General Cybersecurity Awareness	10	.925	.911	62.89
Information Security Awareness	6	.914	.888	70.25
Ship Cybersecurity Awareness	4	.852	.723	69.32
Total	20	.957	.932	56.67

Also, for advanced analysis, a Normality test is conducted. Skewness and Kurtosis values were found to be between -1.5 and +1.5 for all items. It is possible to say that the data is normally distributed [44]. Therefore, a parametric test is convenient, and the data is suitable for descriptive analysis [45].

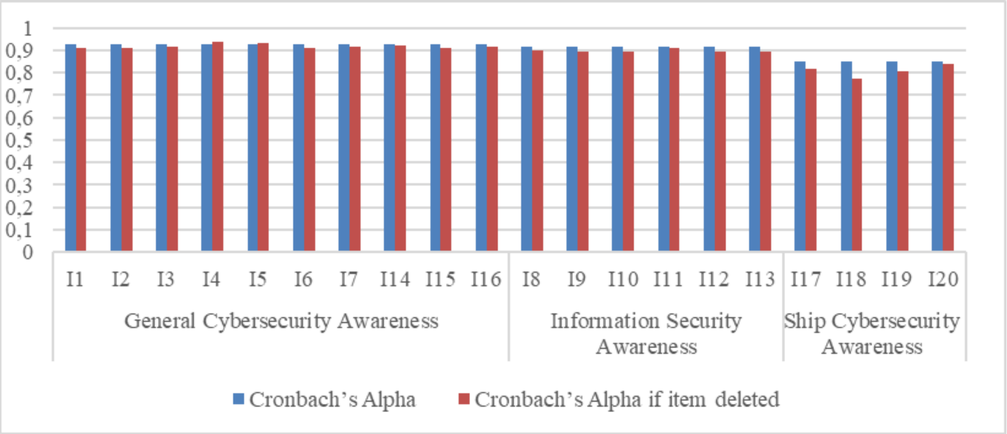

Figure 1. Cronbach's Alpha and Cronbach's Alpha if an item is deleted for items according to scales.

5. FINDING AND RESULTS

Firstly, basic statistics are examined for all items, considering scales.

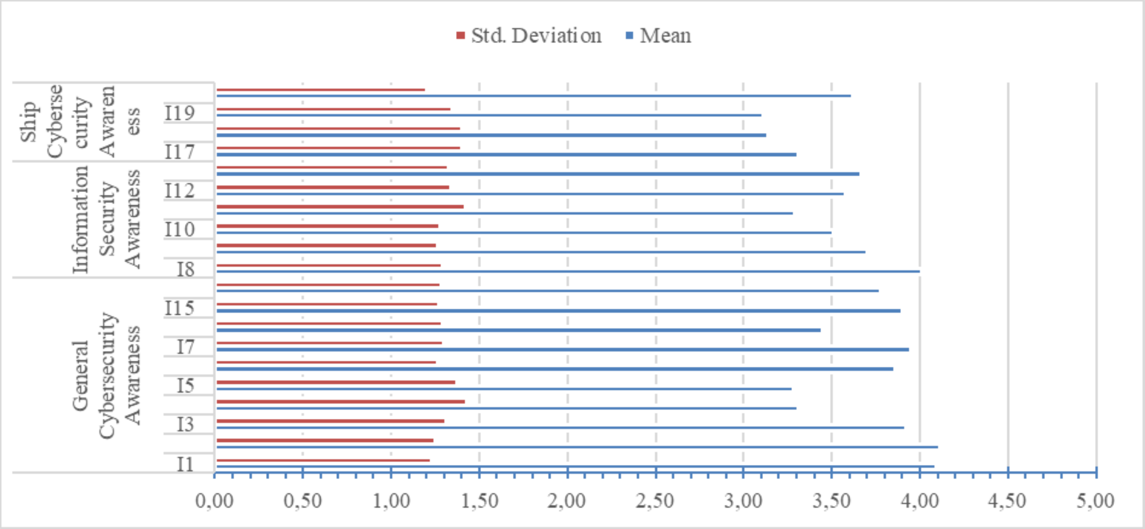

Figure 2. Values of items' basic statistics according to scales.

As a result of the normality test explained in the section Analysis, it was said that our data were normally distributed. It is possible to achieve meaningful results by interpreting values of mean and standard deviations. In Figure 2, all values for all items according to scales are shown. It appears that, although the items have included simple and general cybersecurity measures such as strong passwords and critical information, which are concepts that students are expected to be familiar with, items' mean, and standard deviation values show that maritime students' awareness levels for all scales are not sufficient for the safe usage of technological devices within the industry. There was no significant difference in score between the scales' items' values of mean and standard deviation because maritime students' awareness levels for all scales are average or below average. To be satisfactory, it must be influenced. Therefore, maritime students' awareness of all scales should raise.

For the scale of ship cybersecurity awareness, items' mean, and standard deviation values show that ship cybersecurity awareness needs to rise because participants' responses to items are unsatisfactory. The deficiency in ship cybersecurity awareness is at the point where it cannot be ignored, and ship cybersecurity awareness is needed urgently. Human beings should adopt technological changes in the maritime industry because students are the primary resource of the future maritime industry. Cybersecurity is one of the basic concepts to ensure human adaptation to technological development. The future maritime industry will include more complex technology and will need more complex concepts-based cybersecurity. Therefore, situational cybersecurity awareness must improve.

In Figure 2, one of the most remarkable values is I20's values, which are in the scale of ship cybersecurity awareness. I20 is “I know Seafarers are an important factor for ship cyber security.” Students responded "agree" to I20. It was stated in the previous chapter that human beings are a cause of loss from cyber-attacks, whether intentionally or unintentionally. The descriptive statistic of I20 is proof that students’ intentions are not bad. It can be deduced from this that attention should be paid to the classification of unintentional cyber threats. This finding will help to determine precautions to raise awareness on this topic. In addition, this statistic explains that there is an awareness among students that they are important to cybersecurity.

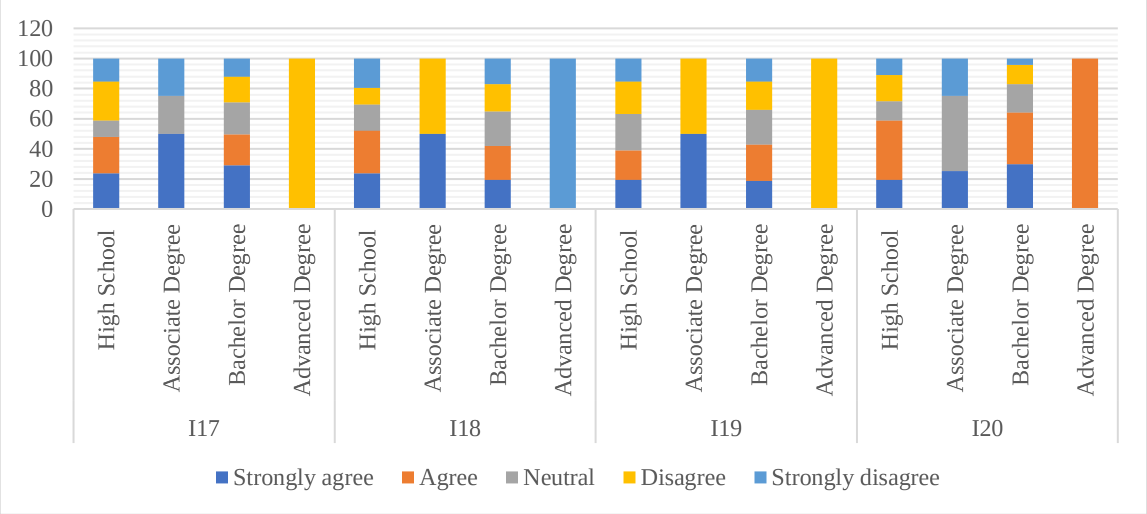

Figure 3. Items’ distribution for ship cybersecurity awareness scale according to education level.

Items’ distribution for ship cybersecurity awareness scale according to education level is shown in Figure 3. Advanced degree is omitted because the number of students in advanced degree programs is not sufficient to interpret. According to Figure 3, as the level of education increases, awareness increases for I20. This confirms literature and supports the motivation of this study. [26][23]. In general, it is seen Figure 3 that the response distributions at education levels are similar except for I20. For I17, I18, and I19, response distributions of students in all education are similar. Therefore it is thought that all METs stakeholders are raising cybersecurity awareness similar level. This level is not satisfactory. If MET is thus updated to include maritime cybersecurity, situational awareness is ensured.

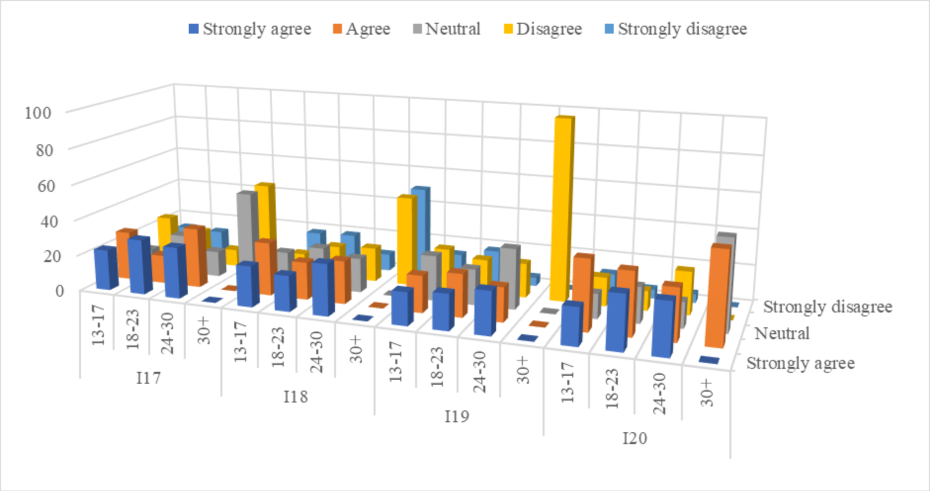

Figure 4. Items' distribution for ship cybersecurity awareness scale according to education level according to age.

Variation of items belonging to the scale of ship cyber security awareness according to age is shown in Figure 4. 30+ is omitted because the number of students aged 30+ is not sufficient to interpret. The rates of responses "Agree" and "Strongly agree" increased with increasing age. It is also possible to say that awareness increases with age. Although the rate of young individuals in technology use is high, it can be considered according to Figure 4 that as age increases, careful usage of technology also increases. It can be interpreted that careful use of technology should be ensured for young people.

Values of Cronbach's Alpha and Cronbach's Alpha if the item is deleted according to scales are shown that Figure 1. This figure shows that all items have relatively high internal consistency.

6. DISCUSSION

The maritime industry will grow and develop with the benefits of technological development like IT and OT, IoT, and digitization. Undoubtedly, safer, more reliable, faster, and more sea transportation is possible with technology. For the latest technology that automatic vehicles are introducing, IMO has even arranged the process for automatic ships [9][19][21]. Although the maritime industry has been convinced of the importance of awareness of cybersecurity, maritime training does not support that and situational awareness for seafarers does not ensure it completely. This is an issue that needs urgent action. The number of cyber threats will grow in the future and cyber-attacks will also be more challenging [11]. If human adaptation to technology development in the maritime industry is to be ensured, the question of how to deal with the cyber vulnerability that may occur in the future should be discussed [21].

Human beings, one of the most crucial factors causing accidents in maritime transportation and trade, have not adapted to technological developments in the maritime industry. This means that the worker who is the cause of accidents may cause new accidents without being aware of technological developments. A human being can be the cause of cyber incidents and losses both intentionally and unintentionally. Neither METs nor STCW, the most important legal basis of METs, are compliant with cybersecurity [10]. With this study, it was noticed that maritime students do not have sufficient awareness of cybersecurity, and this may jeopardize the safety of the industry in the future. Several steps need to be taken to ensure this. First, STCWs must be regulated; secondly, MET must offer new training about cybersecurity; then the training needs to develop. Otherwise, not ensuring awareness of cybersecurity will cause marine losses. These losses will lead to larger economic losses for the maritime industry and the global economy [17].

The vulnerability caused by not ensuring complete awareness of cybersecurity affects all maritime operations [21]. Trade, loading, discharging, anchoring, navigation, and safety operations are affected by cybersecurity vulnerabilities. These operations are a part of huge economic activities. These operations are related to not only maritime stakeholders such as the ship and port but also to also coastal stakeholders. Cybersecurity attacks in the maritime industry affect coastal units where maritime operations are located and indeed the entire region could be affected. Therefore, cybersecurity awareness in the maritime industry should be enhanced [35]. The importance of increasing this should be discussed as soon as possible.

7. CONCLUSION

Because completely unmanned vehicles do not yet exist in the maritime industry, human beings are not yet remote from maritime operations. Although there are many vulnerabilities resulting from human adaptation to technological developments in the maritime industry, reducing these vulnerabilities is possible by investigating maritime cybersecurity, precautions for maritime cyber threats, and defenses against maritime cyber-attacks. Raising situational awareness and developing training about cyber security will facilitate human adaptation to technological developments in the maritime industry. Therefore, in this study, cybersecurity awareness was investigated, and this investigation was conducted on students engaged in maritime training, the future leaders of the industry. The study presented a first-step investigation to raise maritime students' cybersecurity awareness.

Although it is expected that students' cyber security awareness should be satisfactory since they are digital natives, the cybersecurity awareness of maritime students' needs to be improved swiftly. Students' cybersecurity awareness in the maritime industry is at a lower level than expected. In a period when technology advances and cyber-attacks are intensifying and developing, measures should be taken to close the gap caused by humans or to reduce the risk arising from this gap. Raising awareness and new training in cybersecurity for the maritime industry should be the target. Situational awareness of cybersecurity and maritime training is not sufficient to educate students who will have to deal with cyber-attacks. Technological developments in the maritime industry will supply faster, safer, and more secure maritime operations and these operations will ensure a larger trade volume for the global economy if situational awareness and training about cybersecurity in the maritime industry are achieved. Otherwise, no matter how much technology improves, the losses caused by cyber security vulnerabilities may be as great as the returns of it.

There is a requirement that studies examine cybersecurity in METs. They could portray the different stances among the younger generations and how this would change the curriculum of MET. Besides, this study is a local study conducted in Turkey, and a future study can be expanded internationally. It covered students' awareness: this can also be expanded. This is also a first step study, and future studies must be done to raise students' cybersecurity awareness.

ACKNOWLEDGES

Authors can refer to companies, businesses, public institutions or projects that contributed to the study in this section.
There is no people/institutions for their support during the research and specify funding institution with grant number.
The studies have been approved by the appropriate institutional research ethics committee and have been performed in accordance with the ethical standards as laid down in the 1964 Declaration of Helsinki and its later amendments or comparable ethical standards.

REFERENCES

1. S. O. Hansson, "Coping with the Unpredictable Effects of Future Technologies", Philosophy & Technology, Vol. 24, Issue 1, Pages 137-149, 2011

2. S. T. M. Peek, E. J. M. Wouters, J. van Hoof, K. G. Luijkx, H. R. Boeije, and H. J. M. Vrijhoef, "Factors influencing acceptance of technology for aging in place: A systematic review", Int. J. Med. Inform., Vol. 83, Issue 4, Pages 235–248, 2014

3. C. Matt, T. Hess, and A. Benlian, "Digital Transformation Strategies", Bus. Inf. Syst. Eng., Vol. 57, Pages 339-343, 2015

4. C. Chauhan, V. Parida, and A. Dhir, "Technological Forecasting & Social Change Linking circular economy and digitalisation technologies : A systematic literature review of past achievements and future promises", Technol. Forecast. Soc. Chang., Vol. 177, Page 121508, 2022

5. Y. Ichimura, D. Dalaklis, M. Kitada, and A. Christodoulou, “Shipping in the era of digitalization: Mapping the future strategic plans of major maritime commercial actors”, Digit. Bus., Vol. 2, Issue 1, Page 100022, 2022
6. I. C. Ehie and M. A. Chilton, “Understanding the influence of IT/OT Convergence on the adoption of Internet of Things (IoT) in manufacturing organizations”, Comput. Ind., Vol. 115, Page 103166, 2020

7. F. Wortmann and K. Flüchter, “Internet of Things: Technology and Value Added” , Bus. Inf. Syst. Eng., Vol. 57, Issue 3, Pages 221–224, 2015

8. K. Sabbagh, R. Friedrich, B. El-Darwiche, M. Singh, and A. Koster, “Digitization for Economic Growth and Job Creation: Regional and Industry Perspectives”, World Econ. Forum, Pages 35-42, 2013.

9. IMO, “Outcome of the Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS)”, 2021.

10. K. Cabaj, D. Domingos, Z. Kotulski, and A. Respício, “Cybersecurity education: Evolution of the discipline and analysis of master programs”, Comput. Secur., Vol. 75, Pages 24–35, 2018

11. A. M. Shabut, K. T. Lwin, and M. A. Hossain, “Cyber attacks, countermeasures, and protection schemes - A state of the art survey”, 10th Int. Conf. Software, Knowledge, Inf. Manag. Appl., Pages. 37–44, 2017

12. S. Lagouvardou, “Maritime Cyber Security: concepts, problems and models,” Master thesis, Kongens Lyngby, Copenhagen, 2018

13. IMO, “Maritime Cyber Risk Management In Safety Management Systems”, 2017
14. BIMCO, “The Guidelines on Cyber Security Onboard Ships,” Int. Chambber Shipp. Shipp., Vol. 4, Pages 1–53, 2021

15. H. Boyes and R. Isbell, Code of Practice: Cyber Security for Ships. 2017

16. C. South, “USCG issue Cyber Risk Management Guidelines,” 2022

17. S. Karamperidis, C. Kapalidis, and T. Watson, “Maritime Cyber Security_ A Global Challenge Tackled through Distinct Regional Approaches”, J. Mar. Sci. Eng., Vol. 9,Pages. 1–17, 2021

18. E. Peynirci, “The rise of emerging technologies : A quantitative-based research on ‘ maritime single window ’ in Turkey”, Res. Transp. Bus. Manag., Vol. 1, Issue 1, Page 100770, 2021

19. M. Ramos, I. Utne, and A. Mosley, “On factors affecting autonomous ships operators performance in a Shore Control Center” , 14th Probabilistic Safety Assessment and Management, Pages 16-21, Los Angeles, 2018

20. G. Potamos, A. Peratikou, and S. Stavrou, “Towards a maritime cyber range training environment”, IEEE Int. Conf. Cyber Secur. Resilience, Pages 180–185, 2021

21. Ü. Öztürk, M. Akdağ, and T. Ayabakan, “A review of path planning algorithms in maritime autonomous surface ships: Navigation safety perspective”, Ocean Eng., Vol. 251, Pages 111010, 2022

22. A. Galieriková, “The human factor and maritime safety,” Transp. Res. Procedia 40, 2019

23. I. Mraković and R. Vojinović, “Evaluation of Montenegrin Seafarers’ Awareness of Cyber Security” , Trans. Marit. Sci., Vol. 09, Issue 02, Pages 206–216, 2020

24. C. Parka, W. Shib, W. Zhangb, C. Kontovas, and C.-H. Changa*, “Evaluating cybersecurity risks in the maritime industry: a literature review”, The International Association of Maritime Universities (IAMU) Conference, Pages 79–86, 2019

25. I. Milić-Beran, D. Milošević, and S. Šekularac-Ivošević, “Teacher of the Future in Maritime Education And Training” , Knowl. Int. J., Vol. 46, Issue 1, Pages 119–125, 2021

26. H. Wang, O. L. Osen, G. Li, W. Li, H. N. Dai, and W. Zeng, “Big data and industrial Internet of Things for the maritime industry in Northwestern Norway,” IEEE Reg. 10 Annu. Int. Conf. Pages 1-5, 2016

27. T. Kimberly, K. Moara-Nkwe, and K. Jones, “The Use of Cyber Ranges in the Maritime Context”, Marit. Technol. Res., Vol. 3, Issue 1,Pages 16–30, 2020

28. O. S. Hareide, O. Josok, M. S. Lund, R. Ostnes, and K. Helkala, “Enhancing Navigator Competence by Demonstrating Maritime Cyber Security”, J. Navig., Vol. 71, Issue 5, Pages 1025–1039, 2018

29. I. Mraković and R. Vojinović, “Maritime cyber security analysis – How to reduce threats?”, Trans. Marit. Sci., Vol. 8, Issue 1, Pages 132–139, 2019

30. B. Svilicic, M. Kristić, S. Žuškin, and D. Brčić, “Paperless ship navigation: cyber security weaknesses”, J. Transp. Secur., Vol. 13, Issue 3–4, Pages 203–214, 2020

31. B. Svilicic, “Assessing ship cyber risks : a framework and case study of ECDIS security” , WMU Journal of Maritime Affairs, Vol. 18, Pages 509–520, 2019

32. K. Kuhn, S. Bicakci, and S. A. Shaikh, “COVID-19 digitization in maritime: understanding cyber risks,” WMU J. Marit. Aff., Vol. 20, Issue 2, Pages 193–214, 2021

33. T. Kimberly and K. Jones, “MaCRA: a model-based framework for maritime cyber-risk assessment” , WMU J. Marit. Aff., Vol. 18, Issue 1, Pages 129–163, 2019

34. B. Svilicic, I. Rudan, V. Frančić, and M. Doričić, “Shipboard ECDIS cyber security: Third-party component threats,” Pomorstvo, Vol. 33, Issue 2, Pages 176–180, 2019

35. I. Mraković and R. Vojinović, “Evaluation of Montenegrin seafarers’ awareness of cyber security”, Trans. Marit. Sci., Vol. 9, Issue 2, Pages 206–216, 2020

36. P. Bolat and G. Kayişoğlu, “Antecedents and Consequences of Cybersecurity Awareness: A Case Study for Turkish Maritime Sector”, J. ETA Marit. Sci., Vol. 7, Issue 4, Pages 344–360, 2019

37. Lv, Fang-Yuan. "Issues in Maritime Cyber Security Joseph Direnzo III, Nicole K. Drumhiller, Fried S. Roberts (Eds.)(2017)”, Marine Policy, Volume 117, Pages 568, 2020

38. M. Turhan, “Siber Güvenliğin Sağlanmasi, Dünya Uygulamalari,” Bilgi Teknolojileri Ve İletişim Kurumu, Master Thesis, [Ensuring Cyber Security, World Practices] [Thesis in Turkish], Information technology and communications agency, Ankara, 2010

39. IMO, “ Guidelines On Maritime Cyber Risk Management”, 2017

40. University of Louisville Information Security Office, “Information Security User Awareness Assessment.”, https://louisville.edu/security/files/user-awareness-questionnaire-pdf , December 12, 2022

41. V. D. Sousa, J. A. Zauszniewski, and C. M. Musil, “How to Determine Whether a Convenience Sample Represents the Population”, Applied Nursing Research, Vol. 17, Issue 2, Pages 130-133 2004

42. İ. Karaca, “Denizcilik Öğrencilerinin Siber Güvenlik Farkındalıklarının Değerlendirilmesi Anketi”, [survey in Turkish], https://docs.google.com/forms/d/e/1FAIpQLSdQUuXyZK2xtUlK1iuGrWmswms_xNEwCMKklptLwLsTLGCvUw/viewform?usp=sf_link, December 12, 2022.

43. Deniz Ticaret Odası, “The Guidelines on Cyber Security Onboard Ships,” Deniz Ticareti, Vol. 6, Pages 28, 2022.

44. F. Barbara, Tabachnick; Sanford, “Using Multivariate Statistics (sixth ed.)”. Pearson, Boston, 2013.

45. L. Sthle and S. Wold, “Analysis of variance (ANOVA)”, Chemom. Intell. Lab. Syst., Vol. 6, Issue 4, Pages 259–272, 1989