Int. j. adv. multidisc. res. stud. 2026; 6(6):805-819

Received: 29-09-2026
Accepted: 09-11-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Cyber Security, Fifth Generation (5G) Technology Awareness, and Digital Readiness Among Maritime Students

[1] Larry V Gubatayao, [2] Felix C Laruscain, [3] Rolando A Alimen
[1, 2] Master of Science in Maritime Education (Teaching Competency), Iloilo City, Philippines
[3] Adviser, Master of Science in Maritime Education (Teaching Competency), Iloilo City, Philippines

DOI: https://doi.org/10.62225/2583049X.2026.6.6.7190
Corresponding Author: **Larry V Gubatayao**

Abstract
The rapid digitalization of maritime operations requires future seafarers to possess adequate knowledge of cybersecurity and emerging communication technologies such as 5G. In response to this need, this descriptive–correlational study aimed to determine the level of cybersecurity awareness, 5G technology awareness, and digital readiness among maritime students, as well as to examine the relationships among these variables. Specifically, the study sought to assess whether awareness of cybersecurity and 5G technology is associated with the digital readiness of maritime students in adapting to modern maritime systems. The respondents of the study consisted of 148 maritime students from three maritime schools in Iloilo City. A researcher-constructed questionnaire was used to measure the respondents' levels of cybersecurity awareness, 5G technology awareness, and digital readiness. The collected data were analyzed using both descriptive and inferential statistical techniques.
Descriptive statistics, including mean and standard deviation, were used to determine the levels of the variables, while inferential statistics such as the independent samples t-test, one-way analysis of variance (ANOVA), and Pearson product–moment correlation coefficient (Pearson r) were employed to test differences and relationships among the variables. All statistical analyses were conducted at the 0.05 level of significance. The findings revealed that maritime students demonstrated awareness of cybersecurity and 5G technology and were generally digitally ready. Moreover, the results indicated significant relationships among cybersecurity awareness, 5G technology awareness, and digital readiness. These findings suggest that strengthening students' awareness of cybersecurity and emerging digital technologies may contribute to improving their preparedness for the increasingly digitalized maritime industry. The study recommends that MHEIs establish cybersecurity awareness resource centers with cyber-range simulators for OT systems within (ECR, ECDIS) within 12 months, offer 24/7 drop-in training via Moodle, and prioritize 3rd-year students to close year levels and achieve 100% faculty cybersecurity certifications by 2027, shifting training for STCW/IMO compliance and Industry 4.0 readiness.

Keywords: Cyber Security, 5G, Philippines

1. Introduction

Background and Theoretical Framework of the Study

Globally, the international maritime sector is increasingly threatened by cyber risks specifically aimed at OT such as Machine Automation Systems (MAS) and Engine Control Systems (ECS) (Badea *et al*., 2025) [3]. The IMO Resolution MSC.428(98) demands the incorporation of cybersecurity risk management in Safety Management System (SMS) starting January 2021 (International Maritime Organization [IMO], 2017) [21]. Nonetheless, cybersecurity threats still occur because of the use of the outdated programmable logic controller (PLC) and supervisory control and data acquisition (SCADA) systems in the maritime environment (European Union Agency for Cybersecurity [ENISA], 2020) [14].

The Philippines, being the largest producer of seafarers in the world, Philippine Ports Authority managed a total volume of 1.2 million TEUs in 2025. Results from studies conducted by MSUF indicate that students in marine engineering have general knowledge in cybersecurity, but are unaware of MAS and ECS needed in smart ports (PASCUA *et al*., 2023) [36].

There is an international standardization, yet the BSMarE curricula under-researches the OT vulnerabilities specific to engineering, and it requires the demographic analysis of students to provide appropriate measures related to Industry 4.0.

Maritime industry experiences cybersecurity challenges because of the quick changes in digital transformation and OT. Machine automation systems (MAS) such as PLCs, SCADA, and Engine Control Systems (ECS) may be subject to ransomware attack, unauthorized remote connection and DDoS that can cause failures in propulsion and cargo handling operations. It should be admitted that Filipino marine engineers know the basic cybersecurity, yet do not possess special knowledge related to MAS/ECS protection and may face difficulties in Industry 4.0 operations (Karaca & Soner, 2023 [23]; The Maritime Executive, 2026).

Modern technologies, such as AIS (Automatic Identification System), GNSS (Global Navigation Satellite Systems), and ECDIS (Electronic Chart Display and Information Systems), became indispensable in maritime operations. According to Li *et al*. (2024) [26], these systems are interconnected and vulnerable to various cyber-attacks. In turn, Tam and Jones (2018) note that there is an increased dependence of global shipping on digital technologies, which implies that it is necessary to introduce cybersecurity strategies and policies.

One of the major triggers behind this change is the adoption of 5G technology. The ultra-low latency, high bandwidth, and connectivity of devices through 5G make it possible for this technology to become one of the revolutionary tools for maritime communications, facilitating real-time data transfer among the ships, ports, and control centers. According to Alqurashi *et al*. (2022) [1], it is important to note that the adoption of new technologies increases the attack surface of cybercriminals.

Regarding the management of risks, Rajaram *et al*. (2022) [38] pointed out that it is necessary to implement proactive approaches to cybersecurity concerning shipboard operational technology (OT) systems through risk assessments, secure configuration, cyber hygiene practices, and crew training programs. Besides that, Wong *et al*. (2022) [52] noted that some 5G technologies, such as network slicing can facilitate the improvement of cybersecurity and efficiency of communications, but there are challenges concerning its cost, interoperability, and isolation from security concerns. Likewise, Carrara (2022) [5] pointed out that with the increasing automation and interconnection of ship systems, cyber resilience needs to be improved.

The core of this change lies in the human aspect of the matter. Maritime graduates must be prepared to work in an increasingly changing environment where the combination of traditional seamanship and contemporary technological skills is needed. According to recent research findings, cybersecurity in the maritime sector is highly impacted by human behavior, namely, awareness, training, and decision-making (Li *et al*., 2024; Raymaker *et al*., 2025) [26, 39]. Nonetheless, recent studies find that maritime students and future seafarers frequently display the lack of cybersecurity readiness and have no experience with operational technology risks (Karaca & Soner, 2023 [23]; Cortez *et al*., 2024). Hence, there appears to be a constant gap between theoretical preparation and demands of cybersecurity on practical aspects of maritime operations. Thus, improving cybersecurity education and embedding Industry 4.0 skills in maritime education become vital to adequately prepare undergraduates for new digital challenges (Dillon, 2023) [12].

Notwithstanding the significance of educational establishments for developing cybersecurity skills, Garcia (2025) highlights some approaches to strengthening the readiness of maritime graduates. Those include curriculum development in terms of 5G and cybersecurity education, simulation-based learning experiences, industry partnerships and developing a cybersecurity mindset.

The readiness for cybersecurity has to go further than just theory. The current literature pays a lot of attention to the growing complexity of the cyber threat faced in the maritime environment that includes malware, phishing, and ransomware aimed at damaging the critical maritime infrastructure (Soner *et al*., 2024; Li *et al*., 2024) [46, 26]. Such threats do not only affect the continuity of operations but may cause safety concerns at sea and environmental hazards because of the failure of cyber-physical systems (Ammar & Khan, 2024). Highly integrated and digitized maritime infrastructures are vulnerable to cyber threats of different kinds in both IT and OT domains (Martinez *et al*., 2024; Clavijo Mesa *et al*., 2024). Consequently, graduates have to become adaptive professionals able to deal with technologically based complex risks.

Taking into consideration the high standards of education in regards to seafarers, there is one challenge that should be faced, especially regarding the development of the skills of using 5G technology and innovation in the area of Cyber Security. In today's digital world, the maritime sector needs professionals who are highly skilled not only in seamanship but also in technologies (Delgado, 2023).

It is imperative for educational institutions to provide knowledge and expertise to fresh graduates in order for them to handle issues of cybersecurity and 5G technology. It is important to incorporate digital literacy, which includes new technologies in developing maritime professionals in the context of smart shipping and connectivity (Santos & Li, 2022) [43].

Educational institutions are crucial for preparing workers with adequate skills, but the existing mismatch is posing challenges for fresh graduates. There is a mismatch between what is taught and what the industry requires, and therefore, graduates might be knowledgeable but not ready for technology-based maritime operations (Tanaka, 2021) [48].

MHEIs have been addressing this problem by implementing several strategies to incorporate 5G and cybersecurity skills into education (Rodriguez & Kim, 2023) [41]:

- Curriculum Integration – Incorporating 5G into IT and engineering courses will make sure that students understand telecommunications frameworks that are important in maritime operations (Rodriguez & Kim, 2023) [41].
- Hands-on Training – Students receive simulated environments in which 5G applications are put to the test and are taught how they work. This is an essential part of hands-on learning that is very important for developing skills (Chen *et al*., 2022).
- Industry Collaborations – Working with telecoms on research projects and internships improves the practical experience of the students and establishes ties between educational institutions and industry (Lopez & Singh, 2023) [28].
- Developing Security Mindset – Education in secure coding, monitoring of the network, and assessing risks in 5G develops a security mindset among the students (Ahmed & Torres, 2021) [2].

The implementation of 5G technology means faster data transmission, better connectivity, and enhanced access to the internet via mobile devices. Nevertheless, with all these improvements comes another set of issues, and among them

is that of cybersecurity. According to Davis (1989) [8], the use of technology, including cybersecurity principles and new digital technologies is dependent on the perception of usefulness and ease of use, which are fundamental concepts in the Technology Acceptance Model (TAM). The research is based on literature in technology adoption (Davis, 1989) [8], cybersecurity (National Institute of Standards and Technology [NSIT], 2018) [32], and digital literacy (Eshet, 2004) [13] for comprehending the reaction of new graduates to the cyber security issues amid the potential of 5G technology.

The theoretical framework of this study revolves around the Protection Motivation Theory at Macquarie University (2025) [29] in the cyber era, highlighting the role of threat appraisal (5G as a genuine threat) as being the strongest predictor of protective behavior.

PMT serves as the underlying framework for the variable "awareness". A lack of awareness regarding a 5G connected vessel will result in a lack of motivation towards security practices.

This is complemented by the Unified Theory of Acceptance and use of technology (UTAUT) was developed by Venkatech *et al*. (2003) is the gold standards for measuring how professionals transition into using complex new systems – like 5G in maritime industry.

In this study, UTAUT provides the framework for digital readiness through four key pillars: (1) Performance expectancy: Do maritime students believe that mastering 5G cybersecurity will actually make them more effective officers or more employable?; (2) Effort expectancy: Do they perceived 5G security protocols as user-friendly); (3) Social influence: To what extent do their instructors, peers, and maritime industry at large perceive them to be digitally literate:; (4) Facilitating condition (The Readiness Pillar): This is the most critical in this study for it measures whether students believe that have the necessary resources – such as 5G simulators, updated curricula, and technical support to actually be "ready", which extensive research (DNV 2024 [9], IMO 2025) has documented the technical implementation of 5G in maritime sector, a significant research gap existed concerning the human element, especially, there is lack of empirical data connecting a student cognitive trait appraisal (awareness) to their functional ability to navigate 5G - integrated bridge systems (readiness). This study addresses this void by being one of the first to apply an integrated PMT – UTAUT framework to the 2026 maritime graduating students.

As the maritime industry adapts 5G, standalone network and autonomous navigation, the "Human Element" remains the most critical firewall. If there is a disconnection between cadets knows (awareness) and what they can do (readiness) the safety of global chain is at risk.

As chief engineer observation goals that all are aware of cybersecurity threats (phishing, ransomware) IMO protocols and basic risk management, however MNO/ECS-specific proficiency remains limited, indicating they to purchase gaps critical for industry 4.0 engineering roles. However, as observed, before merged 5G technology maritime applications have limited understanding of 5G-specific risks (edge DDoS, jamming) quite depending among engineering crew, managers, connected operational technology systems, chief engineers and electro-technical officers have a very strong cyber-physical systems proficiency, while deck officers lag in OT cybersecurity integration.

This study is undertaken to validate and prove that in digital era 2026, a seafarers' "readiness" is defined as their ability to read a physical chart and by applying a rigorous statistical lens to human technology interface, ensuring that findings are not first anecdotal but a data driven blue print for more secure maritime future.

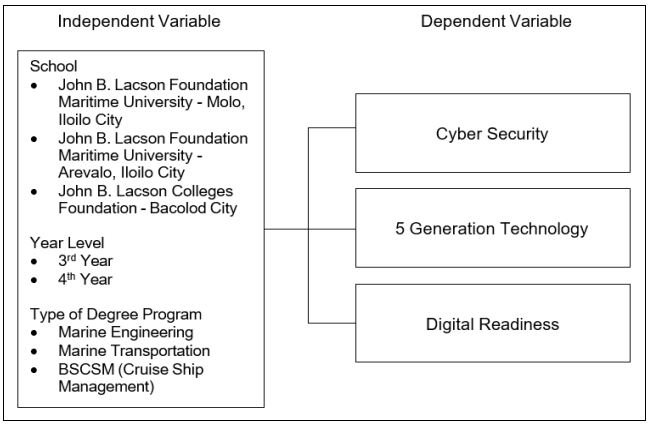

Fig 1: Schematic Diagram Showing the Relationship between the Dependent and Independent Variables

Statement of the Problem and Hypothesis

This study aims to assess the level of awareness of Cyber Security and 5G Technology and digital readiness among the maritime students. It would also find out the significant difference on cyber security, 5G technology awareness, and digital readiness as to school, year level, and degree program. Further, it would also determine the relationship among cyber security, 5G technology, and digital readiness of the maritime students.

Specifically, the study seeks to answer the following questions:

1. What is the level of awareness on cybersecurity of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
2. What is the level of awareness on 5G technology of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
3. What is the level of digital readiness of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
4. Is there a significant difference in the level of awareness on cybersecurity among maritime students when grouped according to school, year level, and degree program?
5. Is there a significant difference in the level of awareness on 5G technology among maritime students when grouped according to school, year level, and degree program?
6. Is there a significant difference on the digital readiness of the maritime students when grouped according to school, year level, and degree program?
7. Is there a significant relationship among cybersecurity, 5G technology awareness, and digital readiness of the maritime students?

To address the problems stated, the following hypotheses will be tested:

1. There is no significant difference in the level of awareness on cybersecurity among maritime students

when grouped according to school, year level, and degree program.
2. There is no significant difference in the level of awareness on 5G technology among maritime students when grouped according to school, year level, and degree program.
3. There is no significant difference on the digital readiness of the maritime students when grouped according to school, year level, and degree program.
4. There is no significant relationship among cybersecurity, 5G technology awareness, and digital readiness of the maritime students.

Definition of Terms

The following terms are conceptually and operationally defined for better understanding.

5G Technology

5G Technology is a wireless communication standard design to deliver the ultra-high speeds, ultra-low latency, massive device connectivity, and energy efficiency through advanced spectrum use and network slicing (Fortinet, n.d.).

In this study it refers to the 5th generation mobile network that can connect a huge number of devices simultaneously enhancing Internet of things IoT (Internet of Things).

5G Technology Awareness

The degree to which maritime students are informed about the capabilities, benefits, and challenges of Fifth Generation (5G) wireless technology, particularly its application in maritime operations such as real-time vessel tracking, automation, and smart port communication (Wang, *et al*., 2020) [51].

In this study, it describe as fully aware, aware, moderately aware, unaware, and very unaware.

Cybersecurity

Cybersecurity refers to the protection of IT systems onboard ship, hardware, and sensors and the data from unauthorized occurs that could cause shipping-related operational, safety, and security failures (International Maritime Organization, 2021) [22].

In this study cybersecurity encompasses the tangible processes, tools, policies, and principles aimed at "ensuring" the confidentiality, integrity, availability of information assets in cyberspace related to marine engineering such as machine automation system and engine control system.

Cybersecurity Awareness

Cybersecurity awareness is an ongoing process of educating and training employees about the threats that lurk in cyberspace, how to prevent such threats and what they must do in the event of a security incident. It also helps to inculcate in them a sense of proactive responsibility for keeping the company and its assets safe and secure (Spanning Cloud Apps, 2022) [44].

In this study, it refers to the level of understanding among maritime students regarding potential cyber threats, risks, and the basic practices needed to protect maritime digital systems, including shipboard IT and operational technologies. This includes knowledge of malware, phishing, unauthorized access, and cyber hygiene practices.

Digital Readiness

The preparedness of maritime students to effectively utilize digital tools, systems, and technologies, including cybersecurity measures and 5G applications, in maritime practice and shipboard operations (Ng & Cullinane, 2020) [33].

In this study, it refers to the preparedness of digital technology, describe as fully ready, ready, emerging readiness, low readiness, and not ready.

Maritime Education and Training

Maritime Education and Training refers to the structured academic and practical programs designed to prepare individual for career in the global shifting and logistics industries (Del Rosario *et al*., 2020) [11].

In this study, the same definition was used.

Maritime Students

Students enrolled in CHED-recognized maritime higher education institutions (MHEIs), taking programs such as BSMT and BSMarE that comply with national and international maritime education standards (Commission on Higher Education (CHED) & Maritime Industry Authority (MARINA), 2019).

In this study, a Maritime Student is a third year and fourth year students under the College of Maritime Education, taking a Bachelor of Science in Marine Engineering and Nautical Science marine transportation has not yet undergone onboard training or apprenticeship.

Significance of the Study

This study is timely in helping to address the issue of the digitalization process of the maritime industry. It will provide empirical evidence that can help in addressing the issue of the balance between advancement in technologies and the ability of people to work on it. The following groups will definitely benefit from the study:

Maritime Students (The Cadets)

The future career of these cadets is directly affected by the study since it will inform them about the readiness level that they have. With the knowledge gained in the study, the cadets will understand what kind of digital seamanship will make them ready for the 2026 job market.

Curriculum Planners

CHED/MARINA planners can use validated variables to incorporate them in BSMT/BSMarE curriculums and make 5G-Cyber electives mandatory accoridng to IMO SMS and digital benchmarks.

Maritime Education and Training (MET) Institutions

This study acts as curriculum blueprint for academies. The findings of the study will help the institutions invest in the high fidelity 5G simulators and cyber security laboratories.

Shipping and Ship Management Companies

The current research provides a benchmark for HR/recruitment so that they can maintain the digital baseline of manning junior officers, minimizing the possibility of human error leading to security breach on 5G enabled anchore vessels.

Graduating Students
The current findings will help the seniors utilize their digital preparedness skills to gain internships, concentrating on protecting 5G enabled communication in order to increase their employability in smart fort facing threats.

Young Professionals
The new seafarer will benefit from the current findings when they are applied to onboard policies, ensuring that they have cyber hygiene in 5G enabled systems for safe voyages.

Maritime Instructors
The educators will benefit from the evidence of active learning, such as module-based triads training-bridge gaps to promote PMT/TAM in OT vulnerability lessons.

Maritime Higher Education Institution (MHEIs)
The findings can assist MHEIs in designing curricula that incorporates cyber-5G modules tailored to specific year levels (such as third-year). This will enable the institutions to meet SCTW requirements and align with Industry 4.0.

Future Researchers
The present research is expected to act as a source of future studies in the areas of technological literacy, technology competency, and decision making.

Scope and Limitation of the Study
This study focuses on assessing the level of cyber security awareness, 5G technology awareness, and digital readiness among the maritime students when taken as an entire group classified according to school, year level, and degree program.
This study identifies significant difference in the level of awareness in cyber security, 5G technology, and digital readiness when classified according to schools, year level, and degree program.
Simple random sampling was employed from among the respondents with relevant experiences and were included in the study. It was conducted Academic Year 2025-2026. Descriptive statistics used are: percentage, frequency count, mean, and standard deviation. The use of both t-test for independent samples, One-way Analysis of Varioance (ANOVA), and Pearson's r, with Alpha Level set at .05. Computerized statistical processing was made by using Statistical Package for Social Science (SPSS) software.
The responses gathered from John B. Lacson Foundation Maritime University - Molo, Iloilo City, John B. Lacson Foundation Maritime University - Arevalo, Iloilo City, and John B. Lacson Colleges Foundation - Bacolod City.
The measurement of awareness and readiness relies primarily on survey responses, which may risk overestimation in the absence of behavioral validation. The research is limited to the group of maritime students and consequently, does not involve the perspectives of seafaring individuals and teachers that may offer different opinions on technological preparedness. Additionally, 5G technology knowledge is evaluated without hands on experience of using the technology. Environmental factors like internet connection and technological facilities are not controlled within the research process.
The study's scope is limited by looking at specific variables, such as year level, school and major as independent variables. Quantitative data is preferred over the qualitative one in terms of seafarers' experiences.

2. Review of Related Literature

Cybersecurity in Maritime Education
Digitization has become an integral part of the maritime industry with ECDIS (Electronic Chart Display and Information System), AIS (Automatic Identification System), GPS and other satellite communications having an important role in the navigation of ships. While this has enhanced the efficiency in ship navigation and operation, it has also raised the cybersecurity concerns with respect to the vulnerability of the system to cyberattacks (Tom & Jones, 2019). With the further digitization in the maritime industry, cybersecurity becomes an urgent issue, especially in maritime training institutions that educate future seafarers (Kessler & Craiger, 2020) [24].
According to the IMO (International Maritime Organization), cyber risks may affect the safety of ships and port operations as well as the environment. The organization stated the importance of the integration of cyber security in the ISM code in its guidelines IMO. Thus, in order to respond to the current changes, maritime education should provide students not only with the knowledge of ships' operation but also with awareness of cyber risks.
Pascua *et al*. (2023) [36] conducted a survey of 277 MSEUF maritime students and found very high awareness levels regarding cyber threats, risks, and response actions but underlined the importance of specialized training in relation to MAS and ECS.
The study by Heering *et al*. (2021) [20] revealed cybersecurity education gaps among MET institutions in Europe. Specifically, a lack of courses addressing cybersecurity maritime education and training (CMET) despite the recommendation of the inclusion of CMET into STCW was noted. Inconsistency between theoretical and practical knowledge was revealed, especially in terms of cybersecurity training in respect of OT specific components like PCLs and SCADA systems.
A report by Karas (2023) indicated a 103% increase in maritime cyber incidents until 2025, where more incidents were noted in the form of ransomware attacks on Engine Control Systems (ECS) and Machine Automation Systems (MAS). It was stated by ENISA (2023) that 70% of vulnerabilities in vessels occurred due to legacy systems.
In addition, GPS spoofing, ECDIS disruptions and crew training failures were highlighted as cybersecurity issues in maritime operations.

Importance of Cybersecurity Training and Compliance in Maritime Education
To emphasize the significance of solving these issues, it is necessary to review several research papers, which point out the importance of cybersecurity training and compliance in the maritime industry and show what else should be done to address them.
Chen *et al*. (2020) [6] conducted research dedicated to maritime cybersecurity threats and their consequences, paying particular attention to the need for training and compliance programs to prevent cyberattacks and to ensure a comprehensive approach to cybersecurity.
Hernandez *et al*. (2021) [18] analyzed the effectiveness of cybersecurity training among seafarers, stating that scenario-based training would increase the ability of seafarers to

recognize cyberattacks and react to them.

Moreover, Fenech *et al*. (2021) explored the issue of challenges related to cybersecurity training of port facility staff, highlighting the need to conduct continuous training taking into account the involvement of different stakeholders in training program development.

Nowadays, the maritime industry has reached a "digital tipping point" when 5G awareness, cybersecurity, and digital readiness are not separate abilities but one competency. According to research of 2024-2026, the awareness about technologies is quite high but there is still a skill gap between them.

An examination of marine students during 2025 revealed that even though 80%, an overwhelming awareness regarding cyber threats, almost the same number had no experience using a cyber-lab or simulation system (Rakka, *et al*., 2025) [40].

The CodeSecure Solutions (2024) [7] mentioned maritime 5G security problems such as multi-hop DDoS and jamming attacks, calling for network segmentation to allow ship to shore communication. Lim (2023) [27] noted the application of 5G technology in digital twins and robotic assisted safety but mentioned lack of cybersecurity training while Safety4Sea (2022) [42] stressed on the use of 5G in remote crane operation services.

5G Technology in Maritime Operations

The use of 5G in maritime industry marks the emergence of groundbreaking change in the relationship between ships, ports and maritime students in terms of digital interaction. The fifth generation wireless technology has brought unprecedented fast connectivity speeds, very low latency levels and great ability of connecting devices, changing radically the maritime industry (Lee, 2020) [25]. As regards to maritime students, it is vital to know about the technology as it provides a greater opportunity to track the vessels, monitor cargo condition, improve navigation systems and optimize port operations (Huawei Technologies, 2021) [19].

As stated by Marpoint (2024) [31], young seafarers require high-speed internet no longer as a "perk" but as a necessity. This indicates that students are very well aware of 5G technology's presence and need for their mental welfare and task execution.

According to the results of a systematic review, students are aware of how 5G enables innovation, such as AR/VR training. They consider 5G technology as an essential foundation of their future education (Zapata and Cabanillas-Carbonell, 2024) [53].

5G Technology and Cybersecurity in Maritime Digital Transformation

The shipping sector is undergoing rapid digitalization and using new technologies like navigational systems, automation of engine rooms, and satellite communications.

Along with these changes comes the increased likelihood of cyberattacks against vital maritime infrastructure. As seafarers of the future, maritime students can ensure cybersecurity of vessels at sea to a high degree. Awareness and preparation of the students are extremely important in this case. Nevertheless, global research shows that while the maritime sector becomes more digitalized, there are serious issues with cybersecurity education in many MET institutions.

According to Onami, Satta and Thabet (2025) [35], the digital adaptability of students outcomes positively in that cadets who have high levels of digital comfort engage more with the immersive bridge simulator. The integration of AI, VR, and 5G in the training process has helped in improving practical readiness by 75% compared to conventional classroom methods, thus proving the theory that today's students are indeed "ready" for digitalization. In Ochea (2025)'s [34] study, it was discovered that, although the students had previous training on simulator, many of them find it hard to use the knowledge gained in practical shipboard training experience with advanced digital bridge systems. The navigational technologies that one encounters in real shipboard conditions are different from those encountered in the school simulators. Additionally, according to the report, many maritime students have theoretical understanding of cybersecurity but lack the necessary laboratory experience.

The Maritime Industry's Digital Revolution, 5G Technology, and Cybersecurity Challenges

The shipping industry is experiencing a drastic transition towards digitalization and is commonly known as the maritime digital revolution. The process is caused by the introduction of innovative technologies including Artificial Intelligenece (AI), Internet of Things (IoT), Big Data, autonomous naviagtion systems, as well as 5G connectivity in many cases (Guo *et al*., 2021) [17].

For instance, a study titled Maritime Cybersecurity Readiness and Training Standards in Indonesia writtern by Rakka *et al*. (2025) [40] used a descriptive quantitative methodology by conducting structured questionnaires in order to identiy organizational readiness, course curriculum implementation, instructor qualification, and facilitation support of the maritime education institutions. Data obtained from the survey were analyzed by using percentage distribution.

Furthermore, the research notes that "digital native" students studying at maritime academies are characterized by a high level of superficial knowledge of technology; however, their practical use of technology is limited. The study revealed that university students have a high level of cybersecurity awareness due to their extensive use of technology, such as social media and online platforms, which express them to a wide range of cyber threats (Ahamed *et al*., 2026).

Similarly, Tecno Scientifica (2025) [49] reported that maritime students worldwide tend to exhibit consistent levels of cybersecurity awareness. This consistency may be attributed to the efforts of many Maritime Higher Education Institutions (MHEIs) to standardize their curricula in accordance with the latest digital standards established by the International Maritime Organization (IMO).

Baldevarona, *et al*. (2024) [4] studied cadets on digitalized navigational bridges and found that despite high simulator scores, many struggled to apply knowledge during real-world shipboard tasks. They concluded that "awareness" does not equal "operational readiness." Supriadi (2024) [45] found a significant difference in readiness between campuses based on their physical infrastructure. Students at schools with 5G-enabled labs scored 40% higher in readiness assessments than those at schools with limited connectivity.

Several studies show that maritime students and cadets lack

sufficient awareness and training in cybersecurity and emerging technologies like 5G. While BSCSM students may have better familiarity with such topics.Marine Transportation and Marine Engineering students often receive little to no formal education on digital threats or network infrastructure (Flores *et al*., 2022) [16]. This gap in knowledge poses risks as future maritime officers may not be equipped to identify or mitigate cyber incidents.

Maritime Students' Implications for Digital Readiness in Maritime Practice

As the world turns to technology, such as fifth-generation mobile networks (5G), the Internet of Things (IoT), artificial intelligence (AI), and cyber-physical systems, to digitize the maritime industry, there emerges a need to prepare a new generation of maritime personnel who are not only proficient in seamanship and engineering but also capable and confident in using and managing these disruptive technologies (Guo *et al*., 2021) [17]. Digital readiness is defined as knowledge, skills, attitudes, and competencies that enable individuals to use and benefit from digital technologies and environments effectively and securely (Papadakis & Katsikas, 2021) [37]. It includes the ability to navigate digital tools, make sense of data, understand cybersecurity risks, and work with smart systems and processes in the maritime field.

Summary

With the growing digitization of the maritime industry, as it adopts ECDIS, AIS, GPS, and 5G, among other technologies, cybersecurity challenges have emerged as a significant concern. While these technological advancements provide more efficient and innovative solutions, such as smart ports and unmanned ships, they also create greater vulnerabilities. The IMO requires that cybersecurity considerations be integrated into safety regulations. The organization calls for educating the maritime workforce on the need to acquire cyber awareness and digital proficiency while emphasizing risk management, thus preparing them for the future of the industry. Students need to be aware of technologies such as 5G, AI, IoT, and other emerging digital innovations and their impact on the maritime industry; otherwise, they may be regarded as ill-prepared and unemployed.

3. Research Design and Methodology

Purpose of the Study and Research Design

The main objective of this study was to assess the level of awareness of cybersecurity and Fifth-Generation (5G) technology and the digital readiness of maritime students. Specifically, this study aimed to measure how the awareness of these two issues may affect the digital readiness and competency of the recently graduated maritime students from select Maritime Higher Education Institutions (MHEIs) in the Western Visayas against the backdrop of the global technological advancements, particulary in the maritime industry. By this, the study also aimed to highlight the problems encountered by maritime students in terms of their knowledge of cyber and 5G technology as well as recommend improvements in the maritime education and training programs that will foster and advance the students' knowledge and skills in cyber and 5G technology for greater preparedness.

The study employed a descriptive-correlational research design where the descriptive component focused on the level of the students' awareness of cybersecurity, 5G technology, and digital readiness, while the correlational component was meant to establish if there was a correlation between cybersecurity and 5G technology awareness and students' digital readiness in maritime operations. The decision to adopt this design was based on its ability to generate information regarding the patterns, trends, and relationships of the target phenomena through the analysis of data that were collected using a quantitative approach without manipulating the study variables during the experiment.

The study was conducted in the selected Maritime Higher Education Institutions (MHEIs) in Panay Island, among the students enrolled in the Bachelor of Science in Marine Transportation (BSMT), Bachelor of Science in Maritime Engineering (BSMarE) and Bachelor of Science in Cruise Ship Management (BSCSM) programs. These programs have been identified as appropriate settings to determine the level of knowledge and readiness of the students on 5G since they are exposed to various digital systems in their courses.

Method

This section includes the participants, instruments, and procedures used in this study.

Respondents

The population of this study consists of students who are currently studying in the third and fourth years of the Bachelor of Science in Marine Transportation (BSMT), Bachelor of Science in Marine Engineering (BSMarE), and Bachelor of Science in Cruise Ship Management (BSCSM) courses in different maritime higher educational institutions in Panay Island such as John B. Lacson Foundation Maritime University - Molo, Iloilo City, John B. Lacson Foundation Maritime University - Arevalo, Iloilo City, and John B. Lacson Colleges Foundation - Bacolod City.

Using the Raosoft sample size calculator, the researcher determined that here is a need for 148 samples from the total population of 240. From the calculated sample size, proportional random-sampling was done from each category.

In Table 1 below, respondents were divided into categories:

A stratified proportional random sampling procedure was done to have a representative sample of the study, achieving a sample size of 148 students selected from the three categories.

The students are chosen randomly due to their exposure to the theoretical and practical aspects of maritime education like the use of digital technologies on board and simulators.

Table 1: Distribution of the Respondents

Category	frequenc	%
Entire Group	148	100
School		
John B. Lacson Foundation Maritime University - Molo, Iloilo City	69	46
John B. Lacson Foundation Maritime University - Arevalo, Iloilo City	49	33
John B. Lacson Colleges Foundation - Bacolod City	30	21
Year Level		
Third Year	118	79
Fourth Year	30	21
Type of Degree Program		
Marine Engineering	39	26
Marine Transportation	79	53
BSCSM (Cruise Ship Management)	30	21

Sources of Data

The main data collection tool, which is a questionnaire, was designed by the researcher and validated by a panel of experts. The questionnaire consisted of three sections, namely: (1) Cybersecurity Awareness (15 items), (2) 5G Technology Awareness (15 items), and (3) Digital Readiness (15 items), yielding a total of 45 items. All items were scored using a 5-point Likert scale: Strongly Agree (5), Agree (4), Moderately Agree (3), Disagree (2), and Strongly Disagree (1).

The following scale of means and description for cybersecurity and 5G technology awareness:

Scale	Description	Interpretation
4.21 – 5.00	Fully Aware	The student possesses deep technical knowledge of 5G vulnerabilities and can identify complex cyber threats.
3.41 – 4.20	Aware	The student recognizes standards 5G security risks and understands the necessary safety protocols.
2.61 – 3.40	Moderately Aware	The student has heard of 5G cyber risks but lacks a clear understanding of how they differ from traditional threats.
1.81 – 2.60	Unaware	The student is oblivious to 5G specific risks, likely confusing them with basic IT issues.
1.00 – 1.80	Very unaware	The student has zero knowledge of 5G technology.

For digital readiness:

Scale	Description	Interpretation
4.21 – 5.00	Fully ready	The student is fully capable of operating 5G-enabled bridge systems independently and securely.
3.41 – 4.20	Ready	The student can operate the 5G systems with minimal supervision and follows cyber security SOP's correctly.
2.61 – 3.40	Emerging Readiness	The student has basic statistical skills but requires significant guidance to navigate a 5G-integrated environment.
1.81 – 2.60	Low Readiness	The student is prepared to handle 5G equipment and poses. A potential security risk to vessel.
1.00 – 1.80	Not ready	The student is completely unequipped for the digital requirements of modern vessel (digitally deficient).

The questionnaire was subjected to content validation by panel of experts and was reliability tested cyber security with r = .74, 5G technology with r = .76, and digital readiness win r = 73. All of the values are good for research purposes since it is .70 and above.

Data-gathering Procedure

Data collection commenced immediately upon approval, details on the data collection process and timeframe of the study were discussed by the researcher as well as the purpose and benefits of the study. The researcher identified or determined the total number of respondents for inclusion in the study and were randomly selected. The researcher clearly discussed the benefits and other valuable information of the study, including its limitation and securing of informed consent. The researcher ensured that the research process would not interfere with their work and would be done at a time most convenient for them.

The researcher secured written informed consent from the participants and ascertained that all information would be dealt with strict confidentiality and informed the participants that during the conduct of the study, they had the right to withdraw. The researcher explained and asked the participants to sign the Informed Consent.

The researcher facilitated each respondent and/or participants during the survey for an effective gathering of data. The data were processed through the Statistical Package for the Social Sciences (SPSS) software.

The researcher obtained approval from the institutional ethics review board and secured permission from the selected maritime institutions to conduct the survey.

A printed copy of the questionnaire was provided to possible respondents through face-to-face or on-site interactions. The dissemination was conducted based on the accessibility and preferences of student respondents to allow full participation and convenience. The 3rd year students and 4th year students' respondents were approached in the school's shared spaces, such as the school grounds, library, gym, canteen, classrooms, or during academic sessions.

Ethical Consideration

This study followed ethical rules that ensured respondents' participation was fully voluntary, assisted by a brief orientation prior to completing the questionnaire. The display of informed consent at the beginning of the survey informed respondents about ethical considerations. To comply with study ethics, respondents were verified to be of appropriate age and mental capacity for interaction. The researcher maintained strict confidentiality regarding any materials that may have an impact on them. In addition, respondents have the option to withdraw from the study at any time. The researcher also acknowledged the work of the other writers cited in this paper.

Statistical Treatment of Data

The researcher utilized the following statistical tools for treatment to analyze and interpret the data gathered:

Descriptive statistics

Descriptive statistics, which include the frequency/percentage, mean, rank, and standard deviation, were used to describe students' demographic profile, 5G awareness levels, and digital readiness.

Frequency/percentage was used to determine the number of respondents.

Mean was used to determine the level of cybersecurity awareness, 5G technology, and digital readiness.
Standard Deviation was used to determine the homogeneity and heterogeneity as to their perception on the level of cybersecurity, 5G technology awareness, and digital readiness.

Inferential Statistics
A t-test for independent samples was used to determine the level of cybersecurity, 5G technology awareness, and digital readiness, and to analyze significant differences in awareness and digital readiness with 2 categories.
One-Way Analysis of Variance (ANOVA) was used to determine the significant difference in cybersecurity awareness and 5G technology awareness with 3 or more categories.
Pearson's r was used to determine the relationship among cybersecurity awareness, 5G technology awareness, and digital readiness.

4. Results and Discussions

Descriptive Data Analysis

This study primarily attempted to determine the cybersecurity awareness, 5G technology awareness, and digital readiness of maritime students, categorized by school, year level, and degree program. For this purpose, the mean and standard deviation were the descriptive statistical tools used.

Level of Awareness of the Maritime Students on Cybersecurity When Taken as an Entire Group and When Classified as to School, Year Level, and Degree Program

Table 2 shows that the level of awareness of the maritime students was "aware" of cybersecurity (M = 4.05, *SD* = .56) when taken as an entire group. When taken to school, Molo (M = 3.99, *SD* = .63), Arevalo (M = 4.03, *SD* = .47), and Bacolod (M = 4.24, *SD* = .57). Of the three schools, Molo and Arevalo maritime students are "aware" of cybersecurity, while Bacolod students are "fully aware" of cybersecurity. As to year level, third year (M = 3.83, *SD* = .60), 4th year (M = 4.10, *SD* = .39). As to the degree program, Marine Engineering (M = 4.10, *SD* = .75), Marine Transportation (M = 4.11, *SD* = .52), and BSCSM (M = 4.83, *SD* = .57). All the means obtained from the year level to degree program showed a mean ranging from 3.41 – 4.20.
Generally, the current level of awareness of maritime students about cybersecurity issues is relatively high. It can be concluded from the article that students are familiar with most of the basic concepts related to protecting information technology systems used in modern ships. The industry source Maritime Cyber Priority 2024/25 issued by DNV covers the views of nearly 500 maritime professionals and stakeholders on the topic of cybersecurity. The report confirms that the awareness of cyber risks among maritime workers has grown significantly due to maritime transport's digital transformation and increased informatization. The report also points out the risk of a false sense of security due to the growing number of employees who work daily with information technology systems that have cybersecurity threats.
According to the source, the main reason for this overestimation of awareness is the lack of technical knowledge and training among maritime workers regarding Operational Technology systems. Navigation, propulsion, and various other systems on board are operated by these systems, making them attractive targets for attackers.
Techno Scientifica's report, published in 2025, explores the issue of cybersecurity awareness among students at Maritime Education and Training establishments. It was found that about 80% of respondents had a high level of theoretical awareness of the basics of cybersecurity. However, the authors of the report note that most educational institutions do not have the necessary cyber-range facilities, bridge simulators, and other technologies to increase students' practical skills in countering cyberattacks. Thus, students lack the practical knowledge and skills required to respond to cyber threats in real-life situations.
The research results described above confirm that awareness about cybersecurity among maritime students is rising steadily. However, the concept of cybersecurity awareness among students is far from being formed. It should be emphasized that most students have theoretical knowledge and skills about cybersecurity. Therefore, it is necessary to equip educational institutions with the necessary tools so that students can receive the required practical training in a simulator-based environment.
Table 2 follows.

Table 2: Means and SD's of the Level of Awareness of the Maritime Students on Cybersecurity when taken as an Entire Group and when Classified as to School, Year Level, and Degree Program

Category	Mean	SD	Description
(A) School			
JBLFMU (Molo)	3.99	.63	Aware
JBLFMU (Arevalo)	4.03	.47	Aware
JBLCF (Bacolod)	4.24	.57	Very Aware
(B) Year Level			
Third Year	3.83	.60	Aware
Fourth Year	4.10	.39	Aware
(C) Degree Program			
Marine Engineering	4.10	.75	Aware
Marine Transportation	4.11	.52	Aware
BSCSM (Cruise Ship Management)	3.83	.57	Aware
Over-all Mean	4.05	.56	Aware

Scale and Description: 4.21 – 5.00 (Fully Aware); 3.41 – 4.20 (Aware); 2.61 – 3.40 (Moderately Aware); 1.81 – 2.60 (Unaware); 1.00 – 1.80 (Very Unaware)

Level of Awareness of the Maritime Students on 5G Technology When Taken as an Entire Group and Classified as to School, Year Level, and Degree Program

The result showed that the maritime students were "aware" on 5G technology, (M = 4.02, *SD* = .63) when taken as an entire group. When classified as to school, Molo (M = 4.09, *SD* = .72), Arevalo (M = 3.81, *SD* = .47), Bacolod (M = 4.19, *SD* = .52). As to year level, the third year (M = 4.02, *SD* = .65) and the fourth year (M = 4.04, *SD* = .60). And as to degree program, Marine Engineering (M = 4.14, *SD* = .81), Marine Transportation (M = 3.96, S*D* = .55), and BSCSM (M = 4.04, *SD* = .60). All means shown from the three categories proved that the students are "aware" of 5G technology since the mean ranged from 3.41 – 4.20.
The students' awareness of the 5G technology under review matches modern trends and findings. According to MarPoint (2024) [31], young people in the maritime field do not consider the access to reliable and high speed networks as a bonus but rather as something that supports their mental

health and work efficiency. In turn, the pedagogical value of 5G networks falls under the jurisdiction of Zapata-Paulini and Cabanillas-Carbonell (2024) [53]. They state that students consider 5G as an "essential pillar" for the modern educational process. Indeed, young people highlight 5G networks as the main condition for implementing such breakthrough technologies as AR and VR in technical education.
Table 3 shows the data.

Table 3: Means and SD's of the Level of Awareness of the Maritime Students on 5G Technology when taken as an Entire Group and when Classified as to School, Year Level, and Degree Program

Category	Mean	SD	Description
(A) School			
JBLFMU (Molo)	4.09	.72	Aware
JBLFMU (Arevalo)	3.81	.47	Aware
JBLCF (Bacolod)	4.19	.57	Aware
(B) Year Level			
Third Year	4.02	.65	Aware
Fourth Year	4.04	.60	Aware
(C) Degree Program			
Marine Engineering	4.14	.81	Aware
Marine Transportation	3.96	.55	Aware
BSCSM (Cruise Ship Management)	4.04	.60	Aware
Over-all Mean	4.02	.63	Aware

Scale and Description: 4.21 – 5.00 (Fully Aware); 3.41 – 4.20 (Aware); 2.61 – 3.40 (Moderately Aware); 1.81 – 2.60 (Unaware); 1.00 – 1.80 (Very Unaware)

Level of Readiness of the Maritime Students on Digital Readiness when taken as an Entire Group and Classified as to School, Year Level, and Degree Program

Generally, the maritime students were "ready" on the use of digital technology when classified as to school, Molo (M = 4.12, *SD* = .63), Arevalo (M = 3.86, *SD* = .48), and Bacolod (M = 4.31, *SD* = .48). As to year level, third year (M = 4.06, *SD* = .60) and fourth year (M = 4.11, *SD* = .56). And as to degree program, Marine Engineering (M = 4.12, *SD* = .69), Marine Transportation (M = 4.03, *SD* = .56), and BSCSM (M = 4.11, *SD* = .55). All the means of the different categories registered a mean ranging from 3.41 – 4.20, showing that the finding that the maritime students are "ready" in the use of digital technology. However, only one school posted a mean of (M = 4.31, *SD* = .48) which indicated that they were "fully ready" on how digital technology be applied.

Recent studies report that maritime students are mostly 'digital ready' due to their high level of digital adaptability, which is explained as "the ability to interact with digital mediums and tools." However, the researchers added that the abovementioned is mostly on a theoretical or social level, and not actual practice. According to Onami *et al.* (2025) [35], students' digital adaptability has a substantial influence on their learning outcomes if they are exposed to "technologically advanced training". The study reports that cadets with higher levels of digital adaptability are able to engage better with the new tools such as bridge simulators and related equipment that are used in the advanced training courses. Similarly, the report by VETIR (2025) stated that the engagement of participants in maritime vocational education with new technologies of AI, VR and 5G networks increased their practical readiness by 27% compared to conventional training methods. However, the study by Tecno Scientifica Publishing (2021) [49] noted that about 50% of students had only theoretical knowledge about cybersecurity and were not adequately trained in related laboratories to gain practical skills. Thus, there is still a need for maritime educators to invest more in training students on practical skills using a new technology.
Table 4 shows the data.

Table 4: Means and SD's of the Maritime Students on Digital Readiness when taken as an Entire Group and when Classified as to School, Year Level, and Degree Program

Category	Mean	SD	Description
(A) School			
JBLFMU (Molo)	4.12	.63	Ready
JBLFMU (Arevalo)	3.86	.48	Ready
JBLCF (Bacolod)	4.31	.48	Fully Ready
(B) Year Level			
Third Year	4.06	.60	Ready
Fourth Year	4.11	.56	Ready
(C) Degree Program			
Marine Engineering	4.12	.69	Ready
Marine Transportation	4.03	.56	Ready
BSCSM (Cruise Ship Management)	4.11	.55	Ready
Over-all Mean	4.07	.59	Ready

Scale and Description: 4.21 – 5.00 (Fully Ready); 3.41 – 4.20 (Ready); 2.61 – 3.40 (Emerging Readiness); 1.81 – 2.60 (Low Readiness); 1.00 – 1.80 (Not Ready)

Inferential Data Analysis

This study further determined the significant difference in the cybersecurity, 5G digital technology awareness, and digital readiness of the maritime students as to school, year level, and degree program. Further, it would also determine the relationship among cybersecurity, 5G technology awareness, and digital readiness. In this regard, t-test for independent samples, One-way Analysis of Variance (ANOVA), and Pearson's r were used set at .05 level of significance.

Significant Difference on Cybersecurity, 5G Technology Awareness, and Digital Readiness of the Maritime Students as to Year Level

A significant difference existed in the cybersecurity awareness of the maritime students as to year level, t (146) = 2.33, p = .021, $p < .05$. However, no significant difference existed in 5G technology awareness, t (146) = 1.88, $p > .05$, and digital readiness, t (146) = .427, p = .850 all p's > .05. The result goes to show that the 5G technology awareness of the third year and fourth year students do not differ or are simply similar. However, the cybersecurity awareness of the third year students and fourth year differs and goes to show that the third year is more aware on cybersecurity.

The findings by Reyes and Tan (2025) corroborate the existence of an urban-rural digital divide in maritime education, noting that schools in urban centers consistently report higher digital readiness scores due to superior ISP reliability and more robust faculty development programs. By contrast, in the investigation of the participants' progress, the tendency appears to be toward homogeneity, as shown by similar levels of awareness of 5G technology awareness, t (146) = 1.88, p = .851, and digital readiness, t (146) = .427, p = .670, across the years of study. Thus, it could be concluded that institutions tend to pursue a standard for digital proficiency regardless of the students' degrees or years of experience. This assumption is supported

by the findings of Vasilakis and Papanikolaou (2025), who suggest that because of the convergence of technology and vessels into cyber-physical systems, the professional competencies of deck and engine officers will eventually overlap, at least partially.

Therefore, as the researchers predict, there will be a need for both deck and engine cadets to acquire at least some knowledge of 5G networks and cyber security.

Table 5 shows the data.

Table 5: t-test Results of the Significant Difference on Cybersecurity, 5G Technology Awareness, and Digital Readiness of the Maritime Students as to Year Level

Year Level	Mean	t-value	df	Sig.
(A) Cybersecurity				
Third Year	3.83	2.33*	146	.021
Fourth Year	4.10			
(B) 5G Technology				
Third Year	4.02	1.88	146	.851
Fourth Year	4.04			
(C) Digital Readiness				
Third Year	4.06	.427	146	.851
Fourth Year	4.11			

Note. *p>.05

Significant Difference of the Maritime Students' Awareness on Cybersecurity, 5G Technology, and Digital Readiness when Classified as to School and Degree Program

No significant difference existed on cybersecurity awareness of the maritime students when classified as to school, F (2,145) = 2.083, p = .132, p > .05 which means that cybersecurity awareness of the maritime students is almost similar. However, a significant difference existed in 5G technology awareness of the maritime students, F (2,145) = 4.293, p = .01, and digital readiness, F (2,145) = 6.362, p = .02, all the p's > .05. All of these indicate that 5G technology and digital readiness as to school differ.

As to degree program, no significant difference existed on cybersecurity awareness, F (2,145) = 2.702, p = .070; 5G technology, F (2,145) = 1.033; and digital readiness, F (2,145) = .383, p = .683. All the probability values are greater than .05, not significant, which showed cybersecurity awareness, 5G technology awareness, and digital readiness were more or less similar when classified as to school.

Recent studies indicate that the majority of maritime institutions provide the same level of cybersecurity education to their students. According to Techno Scientifica's research (2025), such organizations tend to implement similar curricula (MSC.428(98), which determine the minimum level of knowledge about cyber threats. It should also be noted that Mehta and Goliath (2025) did not find any significant difference in the degree of cybersecurity awareness among undergraduate and postgraduate students.

However, the awareness level about 5G technology is apparently different as indicated by Bala and Pandey's (2024) findings. The major reason behind the identified divergence is the students' location and level of education. According to the researchers, individuals who reside in developed countries tend to demonstrate a better understanding of emerging information and communication technologies (ICT).

Nevertheless, the overall level of cybersecurity and 5G awareness among students in various degree programs seems to be consistent with the results of Vasifakia and Papanikolaou's (2025) study. The authors concluded that Maritime 4.0 presumes a universal set of skills and competencies, which implies that deck and engine departments should function within the same digital framework.

Table 6 follows.

Table 6: One-way Analysis of Variance (ANOVA) Results for Significant Difference of the Maritime Students' Awareness on Cybersecurity, 5G Technology, and Digital Readiness when Classified as to School and Degree Program

Source of Variation	Sum of Squares	Df	Mean Square	F	Sig.
(A) School					
Cybersecurity					
Between Groups	1.348	2	.674	2.053	.132
Within Groups	47.613	145	.328		
Total	48961	147			
5G Technology					
Between Groups	3.355	2	1.67	4.293*	.01
Within Groups	56.667	145	.391		
Total	60.023	147			
Digital Readiness					
Between Groups	4.218	2	2.19	6.362*	.002
Within Groups	47.739	142	.332		
Total	51.957	147			
(B) Degree Program					
Cybersecurity					
Between Groups	1.799	2	.880	2.702	.070
Within Groups	47.202	145	.326		
Total	48.961	147			
5G Technology					
Between Groups	.843	2	.421	1.033	.359
Within Groups	59.180	145	.408		
Total	60.023	147			
Digital Readiness					
Between Groups	.274	2	137	.383	.683
Within Groups	51.683	145	.359		
Total	51.957	147			

*p<.05

Multiple comparisons showed that in 5G technology awareness and digital readiness at the school, Bacolod is significantly higher than Arevalo. The mean difference is significant at .05 level, as shown in Table 7.

Table 7: Comparison of the Means Using the Scheffe Test

Dependent Variables	School	School	Mean Difference	Sig
(A) 5G Technology Awareness	Bacolod	Arevalo	.37837	.036
(B) Digital Readiness	Bacolod	Arevalo	.46222	.033

Relationship among Cybersecurity, 5G Technology Awareness, and Digital Readiness among the Maritime Students

A significant relationship was found between cybersecurity awareness and 5G technology awareness, π =.72, p=.000, between 5G technology and digital readiness, r = .683, and between cybersecurity and digital readiness. This implies that cybersecurity, 5G technology and digital readiness are interrelated. The variables were found to affect each other. An increase in one variable caused the other to increase.

The positive correlation identified between 5G technology awareness and cybersecurity consciousness aligns with the findings of Zhang and Hillen (2024), who noted that the complexity of 5G-enabled Internet of Things (IoT) environments necessitates a heightened perception of digital risks. In addition, as reported by Hjort and Lindberg (2024), 5G awareness acts as a growth factor in that as learners become more aware of the nuances of high-speed connectivity, their perception of the risks posed by software-defined networks also grows. These results are an indication that 5G-connected devices and associated cybersecurity risks are quickly becoming an integral part of curricula, such as those of JBLMFU.

Table 8: Correlation

	Cybersecurity Awareness	5G Technology Awareness	Digital Readiness
Cybersecurity Awareness π	_____	.762*	.683*
Sig.		.000	.000
N		148	148
5G Technology Awareness π		_____	.759*
Sig.			.000
N			148

*p<.05

5. Summary, Conclusions, Implications, and Recommendations

Summary of the Problem and the Findings

The main purpose of this study was to find out the cybersecurity, 5G technology awareness, and technological readiness of maritime students.

Specifically, the study seeks to answer the following questions:

1. What is the level of awareness on cybersecurity of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
2. What is the level of awareness on 5G technology of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
3. What is the level of digital readiness of the maritime students when taken as an entire group and when classified as to school, year level, and degree program?
4. Is there a significant difference in the level of awareness on cybersecurity among maritime students when grouped according to school, year level, and degree program?
5. Is there a significant difference in the level of awareness on 5G technology among maritime students when grouped according to school, year level, and degree program?
6. Is there a significant difference on the digital readiness of the maritime students when grouped according to school, year level, and degree program?
7. Is there a significant relationship among cybersecurity, 5G technology awareness, and digital readiness of the maritime students?

Based on the preceding problems, the following null hypotheses were presented:

1. There is no significant difference in the level of awareness on cybersecurity among maritime students when grouped according to school, year level, and degree program.
2. There is no significant difference in the level of awareness of 5G technology among maritime students when grouped according to school, year level, and degree program.
3. There is no significant difference in the digital readiness of the maritime students when grouped according to school, year level, and degree program.
4. There is no significant relationship among cybersecurity, 5G technology awareness, and digital readiness of the maritime students.

The findings of this research were as follows:

1. The maritime students exhibited an "Aware" level of cybersecurity awareness and 5G technology awareness, and were generally "Digitally Ready."
2. A significant difference existed in cybersecurity awareness when maritime students were classified according to year level; however, no significant differences existed in 5G technology awareness or digital readiness across year levels.
3. A significant difference existed in 5G technology awareness and digital readiness when maritime students were classified according to school; however, no significant difference existed in cybersecurity awareness across schools.
4. No significant differences existed in cybersecurity awareness, 5G technology awareness, or digital readiness when maritime students were classified according to degree program.
5. Significant relationships existed between cybersecurity awareness and 5G technology awareness, as well as among cybersecurity awareness, 5G technology awareness, and digital readiness.

Conclusions

The maritime students are aware of cybersecurity. It could be inferred that Maritime Education and Training (MET) institutions have successfully socialized the concept of cybersecurity risk. Students no longer see cybersecurity as an IT problem but as a safety/seamanship issue, which is a major win for the industry's safety culture.

The maritime students are also aware of 5G technology. This suggests that the MET has done a good job of incorporating 5G concepts into the curriculum. The students have a foundational understanding and in this case, they know terminology and can talk about 5G maritime connectivity on a conceptual level.

The maritime students are prepared now. This suggests that the MET has transitioned out of the age of the blackboard, and that the hours spent in the 5G labs and VR simulators have paid off, producing graduates who can perform according to the new IMO 2020 regulations.

Cybersecurity awareness differs by year level (3rd, 4th year), which seems to show that cybersecurity awareness is a "learned competency" that grows as students move closer to professional licensure. As students gain more experience with maritime technology, their effort, exposure, and awareness become deeper.

The no significant difference in cybersecurity awareness across schools seems to show that JBLFMU has successfully standardized digital safety training and that the university has effectively bridged any potential "digital divide" between its locations, ensuring all students are

equally prepared for the modern maritime 4.0 fleet.

The significant difference in 5G technology and digital readiness at schools seems to show that certain campuses are currently outperforming others in 5G integration. While JBLFMU has a unified spirit, the practical application of 5G technology is currently uneven across the locations.

The lack of a significant difference in cybersecurity awareness, 5G technology awareness, and digital readiness shows that JBLFMU has successfully implemented a "total ship" approach to digital safety and further shows that general education subjects that cover 5G and cybersecurity are being delivered with equal quality across all colleges.

Cybersecurity and 5G technology awareness are significantly correlated with digital readiness. This result indicates that an academy can enhance students' readiness by strengthening its curriculum. As awareness of 5G and cybersecurity increases, digital readiness is also expected to improve. This suggests that a modern seafarer is no longer a passive user of technology. The correlation implies that "readiness" in 2026 requires a high level of cognitive engagement with the ship's digital nervous system.

Implications

For theory, the study implies that in a 5G environment, threat appraisal is no longer about individual computer safety but about systematic operational safety. While UTAUT is often used for simple app adoption, the study proves its validity in high-stakes, mission-critical environments, showing that "facilitating conditions" (academy infrastructure) are not just helpful—they are the absolute primary driver of readiness in 5G. The significant relationship between 5G and cyber awareness provides theoretical evidence that technological literacy is a prerequisite for security literacy, proving that as a system becomes more connected, the user's cognitive load for security trust increases proportionally.

For practice, the findings imply that classroom-only education is now obsolete. The practical implication is a mandate for immersive digital training. Academies must move from teaching about 5G to teaching within 5G. The study implies that "cyber" should no longer be a separate department. It must be integrated into STCW; cybersecurity is now as fundamental as "Firefighting" or "Life-Saving Appliances." Since there is a link between awareness and readiness, companies should use the survey instrument as a pre-employment screening tool to identify which junior officers are "digitally ready" and which require further training before being assigned to a 5G-enabled smart ship. The implementation is that "incident response" must include a 5G network specialist on the emergency team. Shipping companies must move from "IT helpdesk" to maritime security operations centers that monitor vessels in real time.

Recommendations

1. MHEIs may establish cybersecurity awareness resource centers with cyber-range simulators for OT systems (such as ECR and ECDIS) within 12 months, offer 24/7 drop-in training via Moodle, prioritize 3rd-year students to close year-level gaps, and achieve 100% faculty cybersecurity certifications by 2027 to shift training toward STCW/IMO compliance and Industry 4.0 readiness.

Since maritime students are aware of and understand 5G technology, MHEIs may add practical 5G labs showing real maritime uses (digital twins, smart cranes) combined with cybersecurity training on 5G networks by SY 2026–2027. They may partner with the PPA for live demos, ensuring 80% student participation to convert awareness into Industry 4.0 skills (technical and soft skill competencies required for cyber-physical system integration in smart maritime operations, including digital literacy, data analytics, cybersecurity practices, automation proficiency, and adaptive problem-solving).

Since maritime students are digitally ready, MHEIs may leverage this strength by introducing advanced Industry 4.0 labs featuring AI analytics, digital twins, and MASS simulator training by SY 2026–2027. They may partner with the PPA for smart port demonstrations, ensuring 80% participation, to build on readiness with cutting-edge applications like predictive maintenance and autonomous navigation systems.

2. For Curriculum Planners. Integrate mandatory cyber-5G-digital modules with hands-on simulation into the BSMT/BS MarE programs by 2027, using the study's identified year-level gaps to ensure uniform Industry 4.0 competencies across all years for STCW compliance.
3. For Shipping/Ship Management Companies. Launch cybersecurity internships for digitally-ready maritime graduates, focusing on 5G-enabled vessel operations and ECR protection to leverage their awareness while addressing application gaps.
4. For Maritime Students. Pursue DNV or Lloyd's cyber certifications and practice daily threat simulations to connect prior awareness/readiness into shipboard proficiency before graduation.
5. For Maritime Instructors. Shift to scenario-based training using cyber-range tools and Industry 4.0 case studies, targeting 3rd-year gaps to build on students' strong foundational knowledge.
6. For Future Researchers. Replicate this study with longitudinal tracking of post-graduation applications and test institutional resource effects on the cyber-5G-digital triad using SEM analysis.

6. Acknowledgement

This thesis could not be realized without the concerted efforts, help, and inspiration of the several persons. Thus, the researcher is thankful to the following:

Engr. Sylvino V. Tupas, PhD, Administrator of John B. Lacson Colleges Foundation - Bacolod City, for the motivation to the researcher; Mr. Robert O. Parcia, MSMM Administrator of John B. Lacson Foundation Maritime University - Arevalo, Iloilo City, for allowing the researcher to collect data from the marine transportation students of JBLFMU – Arevalo.

Engr. Roberto Neal S. Sobrejuanite, Administrator of John B. Lacson Foundation Maritime University - Molo, and C/E Reynold Libiano, JBLFMU – Molo, Dean of the Marine Engineering Department, allowed the researcher to collect data and approval of the study among the BSME and BSCM students.

Dr. Geneva M. Eler, Dean, Graduate School of JBLFMU-Arevalo for the support and encouragement; Dr. Rolando A. Alimen, adviser, for the generous assistance and valuable suggestions given to the researcher the inner desire to continue until the finalization of the study; Dr. Felix C. Laruscain, Dr. Alfred G. Espinosa, Dr. Lily S. Sumbi, and

Dr. Lourdes N. Morano, members of the panel, for invaluable suggestions for the refinement of the study.
Dr. Alfred G. Espinosa, member of the Graduate School committee for validating the data-gathering instrument; Riza De La Peña, academic member of JBLFMU Graduate School for the statistical processing of the data.
My wife, Ma. Shirley, my wonderful sons and daughter, Hansel, Gretel, and Cyril, who gave their strengths and spirit to work on and finish the study.
To my beloved nephew Dr. Rona Gonzaga, Dean of Trinity University of Asia - College of Medical Technology, who inspires and supports me in all my work towards the fulfilment of this study.
Above all, to Almighty GOD, who makes all things possible.

7. References

1. Alqurashi FS, *et al*. A Survey on UAV-Aided Maritime Communications: Deployment, Architecture, and Challenges, 2022. arXiv preprint arXiv:2209.09605.
2. Ahmed S, Torres M. Developing a proactive security mindset: Cybersecurity education in the age of 5G. Journal of Cybersecurity Education & Research. 2021; 4(2):112-128.
3. Badea A, Popescu D, Marinescu R. Cybersecurity challenges in maritime operational technology systems. Journal of Marine Science and Engineering, 2025.
4. Baldevarona GB, *et al*. Exploring maritime students' readiness on digitalized navigational bridge. East Asian Journal of Multidisciplinary Research. 2024; 4(4). Doi: https://doi.org/10.54476/apjaet/91820
5. Carrara E. Cyber resilience of automated and autonomous ships. Technology and Science for the Ships of the Future, 2022. Doi: https://doi.org/10.3233/PMST220027
6. Chen Z, Liu P, Lee S. Analysis and Evaluation of Maritime Cybersecurity Threats and Their Impacts. Marit. Policy Manag. 2020; 47:682-698.
7. CodeSecure Solutions. Maritime 5G security: High-speed communication protection. CodeSecure Solutions, 2024. https://codesecure.in/blog/maritime-5g-security-high-speed-communication-protection
8. Davis FD. Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly. 1989; 13(3):319-340. Doi: https://doi.org/10.2307/249008
9. DNV. Maritime Forecast to 2050: The role of 5G and autonomous technologies in decarbonization and safety. DNV GL AS, 2024.
10. Delgado M, *et al*. Digital transformation in maritime education: Building 5G and cybersecurity competencies for the modern seafarer. Journal of Maritime Research and Education, 2023.
11. Del Rosario C, Dalaklis D, Kitada M, Bolmsten J. Improving governance of maritime higher education institutions to ensure success of Filipino cadets. In Proceedings of the 14th International Technology, Education and Development Conference (INTED2020). IATED Academy, 2020, 946-953. Doi: https://doi.org/10.21125/inted.2020.0946
12. Dillon R. The future of cybersecurity in Southeast Asia along the Maritime Silk Road, 2023. arXiv. https://arxiv.org/abs/2308.06963
13. Eshet Y. Digital literacy: A conceptual framework for survival skills in the digital era. Journal of Educational Multimedia and Hypermedia. 2004; 13(1):93-106.
14. European Union Agency for Cybersecurity. Port cybersecurity: Good practices for cybersecurity in the maritime sector. ENISA. ENISA Maritime Cybersecurity Report, 2020.
15. Fenech F, Davidsson P, Ekstedt M. Cybersecurity Training for Port Facility Personnel. Transp. Res. Part C Emerg. Technol. 2018; 93:246-262.
16. Flores A, Cruz J, Villanueva M. Cybersecurity awareness and digital preparedness of maritime students in the Philippines. Journal of Maritime Studies and National Integration. 2022; 6(1):25-40. Doi: https://doi.org/10.14744/jmsni.2022.006
17. Guo Y, Zhang W, Liu Q. Digital transformation in the maritime industry: Challenges and opportunities. Maritime Policy & Management. 2021; 48(6):789-803.
18. Hernandez F, Lee J, Park S. Cybersecurity Awareness Training for Seafarers. J. Marit. Res. 2021; 18:245-263.
19. Huawei Technologies. 5G empowering maritime operations: Transforming ports and shipping. Huawei White Paper, 2021. Retrieved from Huawei Carrier Business Website: https://carrier.huawei.com/en/success-stories/Industries-5G/Wharfs
20. Heering D, Mermiris G, Bolmsten J. Cybersecurity Maritime Education and Training (CMET): Identifying competency gaps in maritime education. WMU Journal of Maritime Affairs. 2021; 20(4):503-522.
21. International Maritime Organization. Resolution MSC.428(98): Maritime cyber risk management in safety management systems. IMO, 2017. IMO Resolution MSC.428(98) PDF
22. International Maritime Organization. Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3/Rev.1). IMO, 2021.
23. Karaca İ, Söner Ö. An evaluation of students' cybersecurity awareness in the maritime industry. International Journal of 3D Printing Technologies and Digital Industry. 2023; 7(1):78-89. Doi: https://doi.org/10.46519/ij3dptdi.1236264
24. Kessler G, Craiger P. Cybersecurity in maritime education: Challenges and recommendations. Proceedings of the International Conference on Maritime Education and Training. 2020; 12:101-110.
25. Lee J, Lee H. Impact of 5G technology on the future of smart ports. Journal of Transport and Supply Chain Management. 2020; 14(1):1-9.
26. Li M, Zhou J, Chattopadhyay S, Goh M. Maritime cybersecurity: A comprehensive review, 2024. arXiv. https://arxiv.org/abs/2409.11417
27. Lim ZQ. Digital twins (DT), 5G connectivity, and future robotics applications in the maritime industry. MAritime Digital Efficiency (MADE) Online Magazine, Centre for Maritime Studies, National University of Singapore, September 29, 2023. Doi: https://doi.org/10.25542/rxn5-yhyc
28. Lopez R, Singh A. Industry-academia partnerships: Enhancing practical readiness for smart shipping operations. International Journal of Maritime Engineering. 2023; 165(A1):45-58.
29. Macquarie University. Protection Motivation Theory in the cyber-age: Threat appraisal as a predictor of digital protective behavior. [Institutional Research

Monograph/Internal Report], 2025.
30. Martínez F, Sánchez LE, Santos-Olmo A, Rosado DG, Fernández-Medina E. Maritime cybersecurity: Protecting digital seas. International Journal of Information Security, 2024. Doi: https://doi.org/10.1007/s10207-023-00800-0
31. MarPoint. Bridging Maritime's generation gap: Tech benefits and new risks, 2024. https://marpoint.gr/blog/maritime-generation-gap-tech-benefits-new-risks/
32. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. U.S. Department of Commerce, 2018. Doi: https://doi.org/10.6028/NIST.CSWP.04162018
33. Ng AKY, Cullinane K. Digitalization and the maritime industry: Trends, challenges, and opportunities. In K. Cullinane (Ed.), The Blackwell Companion to Maritime Economics (2nd ed.). Wiley-Blackwell, 2020.
34. Ochea SML. Exploring maritime students' readiness on digitalized navigational bridge. East Asian Journal of Multidisciplinary Research. 2025; 4(4):1723-1738. Doi: https://doi.org/10.55927/eajmr.v4i4.118
35. Onami S, Satla H, Thabet M. Technological Readiness and Learning Outcomes in Maritime Academies: An Empirical PLS-SEM Investigation, 2025. https://www.researchgate.net/publication/401130086
36. Pascua LA, *et al*. Level of awareness of maritime students on cyber security management. MSEUF Research Repository, 2023. https://mseuf.edu.ph/research/read/2387
37. Papadakis N, Katsikas S. Maritime cybersecurity and education: The way forward. In Cybersecurity and Critical Infrastructure Protection. Springer, 2021, 215-229.
38. Rajaram P, *et al*. Guidelines for cyber risk management in shipboard operational technology systems. Journal of Physics: Conference Series. 2022; 2311(1):012002.
39. Raymaker A, *et al*. A sea of cyber threats: Maritime cybersecurity from the perspective of mariners, 2025. arXiv. https://arxiv.org/abs/2506.15842
40. Rakka SGA, Gumilar B, Wijaya H, Ansar AA. Maritime Cybersecurity Readiness and Training Standards in Indonesia. Green Intelligent Systems and Applications. 2025; 5(2):205-216. Doi: https://doi.org/10.53623/gisa.v5i2.930
41. Rodriguez J, Kim D. Integrating 5G and cybersecurity into Maritime Higher Education (MHEI) curricula: Challenges and initiatives. Global Maritime Education and Training Journal. 2023; 15(1):22-39.
42. Safety4Sea. How 5G will accelerate shipping digitalization. Safety4Sea, July 13, 2022. https://safety4sea.com/cm-how-5g-will-accelerate-shipping-digitalization/
43. Santos A, Li KX. The role of maritime education in the era of smart shipping: Integrating 5G and cybersecurity literacy. Maritime Policy & Management, 2022.
44. Spanning Cloud Apps. Cybersecurity Awareness: Definition, Importance, Purpose and Challenges, June 30, 2022. Retrieved from Spanning: A Kaseya company. https://www.spanning.com/blog/cybersecurity-awareness/
45. Supriadi. Digital transformation in education: A study on school readiness for the implementation of e-reports in the context of datafication. Proceedings of the International Conference on Humanities Education, Law, and Social Science (ICHELS 2024), 2024, 646-655. https://www.scitepress.org/Papers/2024/134124/134124.pdf
46. Soner O, Kayışoğlu G, Bolat P, Tam K. An investigation of ransomware incidents in the maritime industry: Exploring the key risk factors. Transportation Research Record. 2024; 239(4). Doi: https://doi.org/10.1177/1748006X241283093
47. Tam K, Jones K. Maritime cybersecurity policy: The scope and impact of evolving technology on international shipping. Journal of Cyber Policy. 2019; 4(2):147-164. Doi: https://doi.org/10.1080/23738871.2019.1586990
48. Tanaka H. The readiness gap: Aligning academic instruction with the demands of technologically driven maritime operations. Maritime Policy & Management. 2021; 48(6):789-804.
49. Tecno Scientifica Publishing. Maritime cybersecurity readiness & training standards in Indonesia. Green Intelligent Systems & Applications. 2025; 5(2). https://tecnoscientifica.com/journal/gisa/article/view/930
50. Venkatesh V, Morris MG, Davis GB, Davis FD. User acceptance of information technology: Toward a unified view. MIS Quarterly. 2003; 27(3):425-478. Doi: https://doi.org/10.2307/30036540
51. Wang J, Xiao Y, Li T, Chen CLP. A survey of technologies for unmanned merchant ships. IEEE Access. 2020; 8:224461-224486. Doi: https://doi.org/10.1109/ACCESS.2020.3044040
52. Wong S, Han B, Schotten HD. 5G network slice isolation, 2022. arXiv. https://arxiv.org/abs/2203.01590
53. Zapata-Paulini J, Cabanillas-Carbonell M. 5G technology for innovative education: A systematic review. International Journal of Engineering Pedagogy (iJEP). 2024; 14(5):149-169. Doi: https://doi.org/10.3991/ijep.v14i5.48063
54. Maritime Industry Authority. MARINA, CHED, PMMA develop standard program for maritime education, November 29, 2019. https://marina.gov.ph/2019/11/29/marina-ched-pmma-develop-standard-program-for-maritime-education/