10-31-2022

Assessing maritime cyber security awareness in navies of the Gulf of Guinea countries: a case study of Ghana

Kwadwo Forson-Adaboh

WORLD MARITIME UNIVERSITY
Malmö, Sweden

ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA

By

KWADWO FORSON-ADABOH
GHANA

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

MASTER OF SCIENCE
in
MARITIME AFFAIRS

(MARITIME SAFETY AND ENVIRONMENTAL ADMINISTRATION)

2022

Declaration

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

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

(Signature): .....

(Date): **20 September 2022**

Supervised by: **Professor Dimitris Dalaklis**

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

Acknowledgements

First and foremost, my utmost appreciation goes to the Almighty God for His grace and favour upon me. Without Him, I could not have come to the successful completion of my MSc in Maritime Affairs.

My heartfelt appreciation to Professor Dimitris Dalaklis my supervisor, for his guidance, support, and direction right from my expression of interest to write a dissertation on this topic to the accomplishment of it. He offered valuable insights and discussions, coupled with essential documents and reading materials that he provided, which helped me conduct this research. Further, I appreciate all the Maritime Safety and Environmental Administration Professors for imparting to me immense knowledge that I will forever value in my professional career. I thank Professor Michael Ekow Manuel for his motivation and support. Additionally, to all other professors and the library staff who were always there to offer assistance, I say you are greatly appreciated.

I thank Vice Admiral Seth Amoama, the Chief of the Defence Staff of the Ghana Armed Forces, Rear Admiral Issah Adam Yakubu, Chief of the Naval Staff, Commodore Emmanuel Ayensu Kwafo, Flag Officer Commanding Eastern Naval Command, and the Ghana Navy for granting me the chance to further my education and for their enormous backing during my application process. To the Director General of Ghana Maritime Authority, Mr. Thomas Kofi Alonsi, I appreciate your support in enabling me to pursue this programme.

To Sasakawa Peace Foundation and Dr. Yohei Sasakawa, my journey at WMU would not have been possible without your support. I am truly grateful and proud to be a Sasakawa Fellow.

I deeply thank my wife, Major (Dr) Eunice Osei-Mensah, my Children, Nicole Pokua Forson-Adaboh, and Andrew Forson-Adaboh as well as my mum, Madam

Felicia Aboagye for their immense support, prayer and bearing the silence of my absence. May the Almighty God richly bless you all.

Abstract

Title of Dissertation: **ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA**

Degree: Master of Science

In the contemporary era, an area of security that has been acknowledged by security experts as an emerging threat is maritime cyber security. This threat in recent times has cost the maritime industry huge sums of money largely because of the low level of awareness on the part of personnel in the industry. Navies also rely on cyber systems and other interconnected technologies for their day-to-day operations. However, this reliance comes with potential cyber attack risks. Therefore, this study investigated the awareness of maritime cyber security in the Ghana Navy. The following objectives were assessed: the current state of maritime cyber security awareness in the Ghana Navy; the level of preparedness of the Ghana Navy to deal with Cyberattacks; and the proposal of an effective maritime cyber security framework for protecting the Ghana Navy. The research employed a mixed-method approach. The qualitative aspect, consisting of 17 interviews with personnel with cyber security backgrounds helped in achieving objective three (3). Furthermore, the study was undertaken on a sample size of 116 personnel from the Ghana Navy using formulated maritime cyber security survey questionnaires and disseminated through QuestionPro online software. This helped to address objectives one (1) and two (2) The quantitative data was analyzed using Statistical Package for the Social Sciences (SPSS) version 26 including multiple logistic regression analyses. However, the qualitative data was analyzed using MAXQDA Analytics Pro 2022 software. The study revealed that the level of awareness of maritime cyber security in the Ghana Navy was high. In terms of age, it was revealed that those in the age range of 31-40 years had a high level of awareness of maritime cyber security compared to the other age ranges. Additionally, the research revealed that the level of preparedness of the navy was average. Finally, a proposed maritime cyber security framework was developed to help guide the operations of the navy in the interim.

KEYWORDS: Maritime cyber security, Ghana, Training, Risk management, Cyber attacks, Cyber security framework.

Table of Contents

Declaration ..... **i**

Acknowledgements ..... **ii**

Abstract ..... **iv**

List of Tables ..... **vii**

List of Figures ..... **vi**

List of Abbreviations ..... **vii**

Chapter 1 Introduction **1**
1.1. Background and context……....1
1.2. Problem Statement……...2
1.3. Research aims and objectives……..……..4
1.4. Research questions……...4
1.5. Significance of the Research……6
1.6. Expected results……...6
1.7. Key assumptions and potential limitations……...6
1.8. Structure of the dissertation……8

Chapter 2 Literature review **9**
2.1. Introduction……..…..…..9
2.2. Overview of maritime security threats in the GoG……...9
2.3. Cyber attack incidents in the maritime industry ……..……..…..…....14
2.4. Human element as a weakness for cyber attacks……..…...…….17

Chapter 3 Methodology and methods……19
3.1. Methodology……..20
3.2. Research design……..20
3.3. Research methods……...21
3.4. Data collection ……..21
3.5. Data analysis……..22
3.6. Sampling, selection of participants……22
3.7. Research Ethics……...……...23
3.8. Summary of Chapters ……23

Chapter 4 Research Findings and Discussion **24**
4.1. Introduction……...24
4.2. Research Findings: Quantitative Analysis and Discussion…….……...……...25
4.2.1 Demographic characteristics of respondents…….…….25
4.2.2 Awareness of Maritime Cyber Security…….…….…...26
4.2.3 Association between demographic data and awareness of maritime cyber security …….....27
4.2.4 Multiple Logistic Regression of factors influencing Awareness……..27

4.3. Research Findings: Qualitative Analysis and Discussion…….30
4.4. Summary of Chapters ……..30.

Chapter 5 Conclusion and Recommendations……...40
5.1 Introduction…….……
5.2 Conclusion……..…….
5.3 Recommendation …….…..
5.4 Limitations and Future Research…….…...

References **44**

Appendices **51**
Appendix 1…….…..51
Appendix 2…….……..60
Appendix 3…….……..63
Appendix 4 …….….65

List of Tables

Table 1. Table 1: Demographic characteristics of respondent's (N=116). Source(Researcher)…….25

Table 2: Association between demographic characteristics and Awareness. Source (Researcher) ……....31

Table 3: Multiple Logistics regression of the factors associated with Awareness. Source (Researcher)……32

List of Figures

Figure 1. Composition of the Dissertation.
Source (Created by the Author)…….8
Figure 2. A summary of reported piracy incidents in four (4) GoG countries.
Source (Ofosu-Boateng, 2018)…….12
Figure 3. Top ten (10) cyber incidents based on categorization
Source (Meland et al., 2021)……15
Figure 4. Summary of Research Approach/Structure.
Source: (Created by the author)……...20
Figure 5. Respondents' level of Educational Distribution.
Source (Researcher)……....26
Figure 6. Maritime security threat perception in terms of awareness in the GoG.
Source (Researcher)…….....28
Figure 8. The results of respondents on formal training on maritime cyber security
Source (Researcher)…….....30
Figure 10. Results of one sample t-test Source (Researcher) …….....33
Figure 11. The three (3) themes assigned to the importance of maritime cyber security. Source (Researcher)……..…..…36
Figure 12: The four (4) themes assigned to maritime cyber security weak links.
Source (Researcher)……37
Figure 13. The five (5) themes assigned to components of maritime cyber security framework. Source (Researcher)……..…..38
Figure 14. Proposed maritime cyber security framework structure.
Source (Created by Author)……45

List of Abbreviations

ABS	American Bureau of Shipping
AIS	Automatic Identification System
AQIM	Al-Qaeda in the Islamic Maghreb
BIMCO	The Baltic and International Maritime Council
CIA	Confidentiality Integrity and Availability
COBIT	Control Objectives for Information Technologies
CSF	Cyber Security Framework
DRC	Democratic Republic of Congo
ECCAS	Economic Community of Central Africa
ECDIS	Electronic Chart Display and Information System
GGC	Gulf of Guinea Commission
GoG	Gulf of Guinea
GPS	Global Positioning Systems
IBM	International Business Machines Corporation
ICT	Information and Communications Technology
ISMS	Information Security Management Systems
IUU	IIIegal Unreported Unregulated Fishing
MDA	Maritime Domain Awareness
MDA	Maritime Domain Awareness
MMCC	Multinational Maritime Coordination Centre
MOC	Maritime Operations Centres
MOWCA	West and Central African States
NIST	National Institute of Standards and Technology
OT	Operations Technology
SMS	Safety Management System
SPSS	Statistical Package for the Social Sciences
UNCTAD	United Nations Conference on Trade and Development

WA	West Africa
WMU	World Maritime University

CHAPTER 1

INTRODUCTION

1.1. Background and context

Globally, security is one of the utmost concerns for all nations. It is related to the notion of peace and the elimination or stopping of the risk of threat in every facet of our life (Haque et al., 2022). In the contemporary era, an area of security that has been acknowledged by security experts as an emerging threat is maritime cyber security. (Dalaklis et al., 2022). According to Hareide et al. (2018) maritime cyber security is made up of two (2) terms namely 'maritime security' and 'cyber security. The same authors further indicated that maritime security has no definite meaning, however, it could be related to other concepts such as maritime safety and sea power as mentioned by Bueger (2015) where physical domain characteristics of maritime security are looked at. Though there is no single definition for maritime security, some proponents of security such as Dalaklis and Maximo (2022), Siebels (2020) and Okonkwo (2017) assert that this issue encompasses threats that include illegal fishing acts, piracy, armed robbery, trafficking of narcotics, arms proliferation including human trafficking.

Consequently, the second term cyber security has its roots in information security and it involves the practice or process whereby Information and Communications Technology (ICT) systems are preserved or protected in terms of their confidentiality, integrity, availability from, and defended against damage, unauthorized use or exploitation within the cyberspace (ABS, 2016; Dalaklis et al., 2021). To this end, maritime cyber security can be seen to be part of maritime security, associated with the defense from cyber risks or threats of all kinds of maritime cyber systems. Further, Hareide et al. (2018) support that, maritime cyber security is concerned with the lessening of the challenges of cyberattacks on

maritime operations, and naval operations are not immune from this challenge in cyberspace with the advent of digitalization.

The maritime industry, in recent times, has seen its ship Operational Technology[1] (OT) systems being intensively developed as a result of digitalization, integration and networking. Scholars such as Sanchez-Gonzalez et al. (2019) and Dalaklis (2018) argued that shipping in general which includes maritime operations as well as naval operations is under the influence of the digitalization phenomenon. As a result of this development, complex and computer-based technology systems have emerged, and hence there is a pressing need to safeguard the maritime industry including major stakeholders like Navies from cyberattacks and vulnerabilities (Tam et al., 2019; Hareide et al., 2018; Lee et al., 2017). Developing countries such as those bound to the Gulf of Guinea (GoG) are also adapting to this "new era" of technological advancement in their maritime industry and naval operations. For instance, navies like Ghana Navy, Nigerian Navy, and Cote d'Ivoire Navy to mention a few have established and operate Maritime Operations Centres (MOC) with shore-based surveillance equipment, and Ships with sophisticated technologies providing surveillance, reconnaissance, and intelligence in their maritime domain (Dalaklis, 2019).

Furthermore, with developments in electronically supported navigation where systems are progressively being networked and incorporated, examples like Automatic Identification System (AIS), Electronic Chart Display and Information System (ECDIS), Auto Pilot (AP), Radar, Global Positioning Systems (GPS) to mention a few, navies are ever more reliant on these cyber systems for safe and efficient navigation (Hareide et al., 2018). On the other hand, studies by BIMCO et al. (2017) and Progoulakis et al. (2022) indicates that the coming together of Information and Communications Technology (ICT) and OT generates possible

[1] Operational Technology is the application of both hardware and software to regulate and monitor physical processes, devices, and infrastructure

cyberattack vectors enemies with intent, and determination as well as resources to obstruct maritime operations and naval operations. The reliance on these interconnected technologies by the maritime industry including navies of the GoG countries comes with potential cyberattack risks. There are already recorded cases of cyber incidents in Africa such as the maritime cyberattack incident on Transnet in South Africa (Pieterse, 2021).

From the above, it is clear that cyber security is becoming an important dimension of maritime security, hence the need for GoG countries like Ghana to raise awareness on maritime cyber security among maritime industry stakeholders including personnel of the Ghana Navy. Awareness raising in navies of GoG countries should be viewed as paramount because the human factor or element forms the weakest link in the cyber security attacks (Zhang & Ghorbani, 2021; Canepa et al., 2021; Richardson et al., 2020; Mc Mahon, 2020; Ana et al., 2019). Thus, adding cyber security knowledge and skills to the safety ethos of Ghana Navy personnel at the MOCs and onboard ships is crucial. Accentuating this point, Alop (2019) supports that investing in education through awareness raising is necessary. In any case, assessing the level of maritime cyber security awareness of personnel in the Ghana Navy constitute the main subject of inquiry in this study. Further, this study seeks to find if the Ghana Navy is prepared to mitigate maritime cyber security.

1.2. Problem Statement

The maritime domain or space is open to all users, at the same time, it provides an opportunity for food security, transport, and recreation to mention a few. Navies worldwide use the maritime space as a means to protect their sovereignty and project the power of their states. Furthermore, commercial ships use it for the movement of cargo or goods thereby supporting trade globally. Due to globalisation and technological advancement, the increasing impact of modern technology in the maritime industry including navies cannot be overemphasized. However, as navies and other maritime industry stakeholders increase their usage of these technologies,

cyber attackers or cybercriminals are also assiduously working around to detect and exploit their feeblest links which most scholars have concluded as humans (Canepa et al., 2021; Mc Mahon, 2020). Hareide et al. (2018) in their study assert that notwithstanding the increase in media reportage on cyberattacks in the maritime industry of which navies are included, there seems to be insufficient understanding about the impact these cyber incidents could cause to navigation systems and other maritime installations.

In recent times, fierce storms and rough seaways are no longer the biggest threats to the maritime industry. Modern ships depend on computer systems and satellites communications and these make them vulnerable to cyberattacks on their navigational systems, critical software as well as operational systems. The maritime industry depends on equipment such the AP, GPS, AIS, and ECDIS to mention a few. These technologies are vulnerable to a cyberattack (Hareide et al., 2018 & Lee et al., 2017). Cyberattacks are progressively becoming common in present-day times. For example, the NotPetya wiper attack on A.P. Moller-Maersk in late 2017 cost the concerned company hundreds of millions of US dollars (Lee et al., 2017). Further, cybercriminals in recent times, have the ability to conduct cyberattacks that could cripple shipping business, maritime operations including operations of MOCs and patrols of naval ships, thereby compromising the safety and security of ship's crew as well as passengers (Minnaar, 2019). Navies are also victims of cyberattacks and was evident when AIS data was spoofed to fake a UK Royal Navy destroyer HMS Defender in Russian waters (Cronje and Martin, 2021).

Considering Ghana Navy as a reflection of other navies of GoG countries, it relies on the five (5) MOCs across the country, which provides a quite robust Maritime Domain Awareness (MDA) capability for effective monitoring of the maritime space using effective electronic monitoring systems on the nation's maritime environment and to promptly share actionable intelligence with naval ships at sea. Additionally, the country's naval ships are equipped with certain modern systems, such as AIS,

ECDIS, GPS, Radar, as well as other key systems onboard. Also, the navy relies on intelligence information from the Multinational Maritime Coordination Centre (MMCC) Zone F with modern systems as well, established by the Economic Community of West African States (ECOWAS) to ultimately mitigate maritime crime activities within the GoG (Broohm et al., 2020). All these ICT-based systems are susceptible to cyberattacks. It is therefore essential that maritime cyber security awareness of personnel is raised and skills imparted in order for them to avoid high impact mistakes while using the internet as well as ICT devices including systems onboard. Thus, assessing the level of maritime cyber security awareness of personnel at the MOCs, MMCC Zone F as well as those on board ships is very crucial in protecting the Ghana Navy from attacks of cybercriminals.

1.3. Research aim and objectives

The aim of this research is to assess the level of awareness of maritime cyber security in navies of the GoG countries, with a focus on Ghana Navy. Furthermore, the research is aimed at determining if the navy is prepared to handle cyberattacks.
The study will seek to address the following objectives:

- To assess the current state of maritime cyber security awareness in the Ghana Navy.
- To ascertain the level of preparedness of the Ghana Navy to deal with cyberattacks.
- To propose an effective maritime cyber security framework for protecting Ghana Navy.

1.4. Research questions

The research will seek to answer the following questions:

- What is the state of maritime cyber security awareness in the Ghana Navy?
- How prepared is the Ghana Navy to mitigate or prevent cyberattacks?

- Is there any maritime cyber security framework that guides the operations of the navy and what are its basic principles?

1.5. Significance of the research

The findings of the study are projected to contribute to security practices and serve as a theoretical or knowledge-building venture for the Ghana Navy, West Africa (WA) sub-region, and Africa at large. The results of this research can be used to develop a framework for the training of operators at MOCs, the Fleet, MMCC Zone F, and the entire navy's workforce. Further, the research is expected to make an impact on policy regarding maritime cyber security in the Ghana Navy and the maritime industry at large. In addition to the aforementioned, the study would help narrow the gap in the literature regarding maritime cyber security awareness of navies in the GoG states, the WA sub-region, and Africa in general. Also, the findings of this research have the potential to bring about significant social change by giving the Ghana Navy a more objective assessment of the existing level of awareness of maritime cyber security, which will allow for more effective training on that.

1.6 Expected results

The collection and analysis of data from correct sources would enable the researcher to come up with a maritime cyber security framework for the Ghana Navy. Further, it is expected that the results will help raise the needed awareness of maritime cyber security in the Ghana Navy and the GoG countries at large. Also, it is expected that the results of the study will help know how well the Ghana Navy is prepared for maritime cyber attacks.

1.7 Key assumptions and potential limitations

The research survey questionnaire would mainly be conducted within the Ghana Navy and it is envisaged that key participants would be available to support willingly in achieving the aim of the study. Also, with respect to the interview that will be conducted to help with the qualitative analysis aspect of the study, participants would

be selected based on their background in cyber security. However, the lack of or insufficient scholarly data on cyberattack incidents in the GoG or Africa as a whole posed as limitation. Furthermore, the lack of data on cyber incidents against navies pose as limitation to the researcher, this is because majority of navies have neither open nor official dissemination of accident reports including cyber security attacks.

1.8 Composition of the dissertation

The dissertation was organised into five chapters as illustrated in Figure 1:

- Chapter 1: Introduction to the research: This focused on the background to the research, statement of problem, aims and research objectives, research questions, significance of the study, expected results, key assumptions and limitations.
- Chapter 2: Literature Review: It focussed on extensive overview of maritime security threats in the GoG. Furthermore, it examined some cyber security incidents in the maritime industry. Also, it looked at human element as a weakness for cyberattacks.
- Chapter 3. Research Methodology. It presents the research methodology and methods that will be used in the study.
- Chapter 4: Research findings and results discussions.
- Chapter 5: It covered the conclusion and recommendations based on findings of the study.

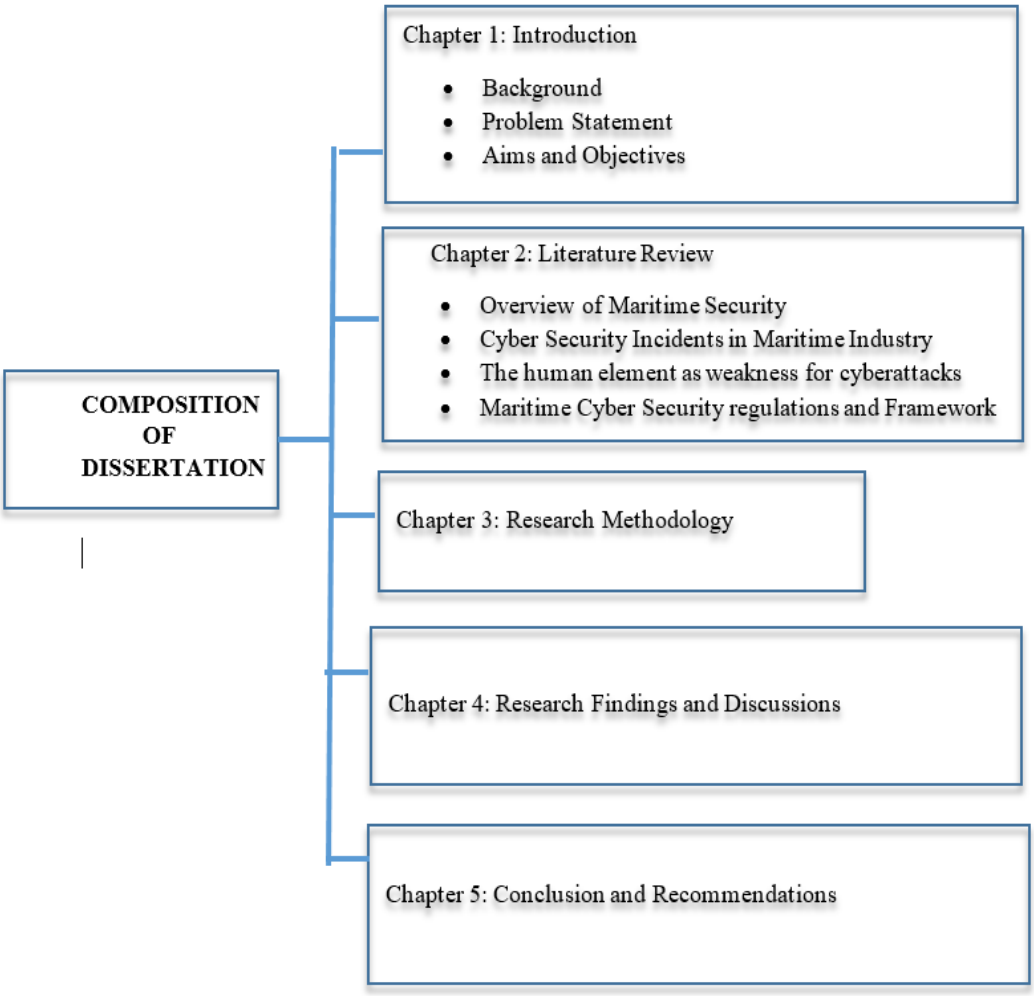


Figure 1. Composition of the Dissertation.

Source (Created by the Author)

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter presents discussions on maritime cyber security in the GoG. The relevance of the chapter in the study was to explain thematic areas relevant to the study of maritime cyber security in the GoG. This enabled the study to review relevant discussions on the research questions. The outcome of the thematic areas, therefore, enabled the study to achieve the study objectives. The presentation of the chapter was based on these themes. The overview of maritime security threats in the GoG, maritime cyber incidents in the maritime domain, maritime cyber security regulation and framework. In the broader context of the concept, maritime cyber security has negatively affected the security of the world's maritime domain. This is because this is an emerging threat and the maritime industry is not fully prepared in terms of awareness, training, policies to mention a few.

2.2 Overview of maritime security threats in the Gulf of Guinea

The GoG is an arm of the Atlantic Ocean located along the Western and Central African coasts. Geographically, it's the Atlantic coast stretching about 3,240 nautical miles (nm) which is approximately 6,000 km from Senegal to Angola (Okafor-Yarwood & Belhabib, 2020; Dalaklis, 2019). This coast comprises of states including Angola, Benin, Cameroon, Cote d'Ivoire, Democratic Republic of Congo (DRC), Equatorial Guinea, Gabon, Ghana, Liberia, Nigeria, Republic of Congo, Sao Tome and Principe, Senegal, Sierra Leone, and Togo. The GoG is of immense strategic importance as it serves as a critical shipping route to the world for virtually all of its littoral countries, including the landlocked countries of Mali, Burkina Faso, Chad, Niger, and the Central African Republic which depend on access to the sea for import and export of goods and services from and to major global markets (Bourmaud et al., 2021; Suh, 2017).

According to Dalaklis (2019), the GoG's strategic shipping routes and huge resources have increased economic activities and unfortunately also, attracted criminal activities such as piracy, armed robbery at sea, illegal bunkering, illegal unreported unregulated (IUU) fishing, smuggling, drug trafficking, maritime cyber security, among others, which constitutes maritime security threats. It is imperative to note that these threats ultimately impact negatively the economic development of the entire region. This is evident on the fact that, there is a growing need for enhanced maritime security cooperation in the GoG and the collective participation of countries like Nigeria, Ghana, Cote D'Ivoire including the rest of the GoG countries is required in this regard to increase awareness among the population (Ibaba, 2020).

The GoG environment is not immune to the radical ability of modern digital communications and computing leading to all forms of cyber security-related issues. In order to gain the advantages of modern technology, those operating in the maritime industry must also become aware of and develop strategies to handle the inevitable cyber security issues that modern computing systems bring with them (Fitton et al., 2015). The increase in cyber attack-related activities globally raises critical security concerns amongst the maritime community and navies in the GoG are no exception. This is because cyber attacks interrupt the flow of goods and services which impacts negatively on the global economy. It is imperative to note that about 90% of the volume of global trade is transported through the sea (United Nations Conference on Trade and Development [UNCTAD], 2019; Kaluza et al., 2010). Thus, any break in the transportation chain occasioned by acts such as cyber attacks has dire security implications on global trade.

Lately, maritime security threats in the GoG have received the needed attention. For example, the economic organizations such as the Economic Community of West African States (ECOWAS), the Economic Community of Central African States (ECCAS), the Gulf of Guinea Commission (GGC) and the Maritime Organization of

West and Central African States (MOWCA) continue to devise ways to suppress acts of all forms of security including maritime cyber security in the GoG. This was made evident in the promulgation of the Yaoundé Code of Conduct concerning the repression of security-related activities in the maritime domain in West and Central Africa (Mansaray, 2017).

An overview of the maritime security threats in the GoG revealed that, cybercriminal activities could enhance other crimes such as piracy, arms and drug smuggling, and human trafficking among others to fund their operations. This situation creates an environment where criminals find themselves cooperating to achieve different ends (Shane & Magnuson, 2016). Therefore, the maritime security threats in the GoG are highlighted as follows:

2.2.1 Piracy

Pirate activities occur in the GoG because West Africa has many active ports involved in both regional and international trade, and most often than not vessels not only transit through the region but sail into the ports to either load or unload products (Bueger & Edmunds, 2020; Aboh & Ahmed, 2018; Hasan & Hassan, 2016). Therefore, that provides a wider opportunity for the pirates to attack ships that are either on transit, or berthed or anchored.

Similarly, pirates have been reported to have hacked into a cargo management system of an unnamed shipping company in March 2016 and identified where on the targeted vessel the valuable cargo was located (Hand, 2016). This enabled them to make a very fast and efficient raid on a vessel, going right to the container of interest. The author further asserts that piracy over the period has had an effect on economies all across the world. Similarly, a German-owned container ship with 8,250 TEUs from Cyprus to Djibouti apparently had its navigation systems compromised by hackers for 10 hours in February 2017 (Blake, 2017). The report indicated that the ship's entire IT system was completely compromised until IT experts were brought

on board to restore the systems. The aforementioned instances demonstrate the extent to which modern-day pirates utilize hacking in the maritime industry and cause the industry huge sums of money.

Likewise, a research report by Safety4Sea, revealed that pirate gangs in the Niger Delta for instance generate approximately $5 million per year in direct income through theft and hostage-taking (Safety4Sea, 2021). This loss and many others shows the extent to which the industry loses money. Figure 2 shows the summary of reported piracy incidents in four (4) GoG countries in 2018.

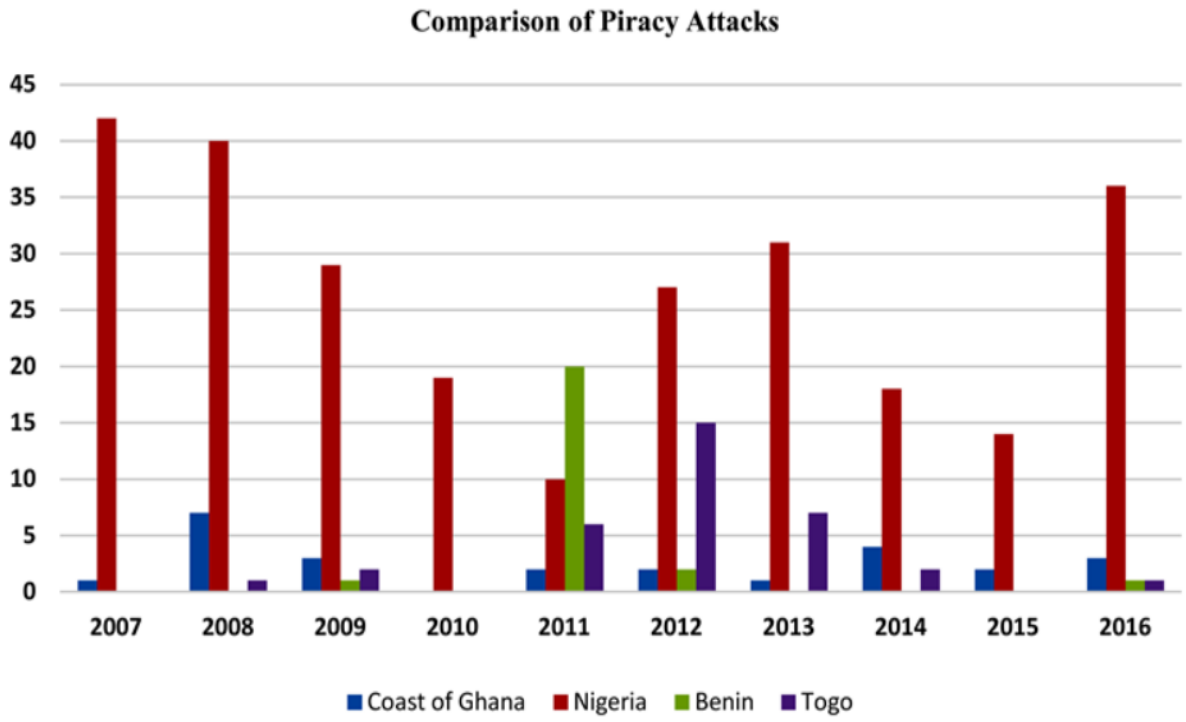


Figure 2. A summary of reported piracy incidents in four (4) GoG countries.

Source (Ofosu-Boateng, 2018)

2.2.2 Armed robbery

One key aspect when considering the impact of the use of digital technologies is their ability to create dynamic connections between different locations in real-time leading to enhance criminal activities interconnected. Armed robbery against vessels at sea is a modern-day day challenge of the maritime and offshore industries because of the use of modern communication to share information (Aboh & Ahmed, 2018). Recent

incidents, especially on the West African coast, have reminded the shipping industry and the public in general about the violence and cruelty with which armed attacks are conducted, the dangers faced by those on board, as well as the significant losses that may occur both in terms of human life and property as a result of information sharing.

2.2.3 Human trafficking

Human trafficking is also another major maritime threat that lingers in the GoG.

Fitton et al. (2015) and Konrad et al. (2016) in their studies assert that developments in communication and information technology have altered the ways in which criminals collaborate across national borders and in the maritime environment. They further indicated that logistics and surveillance challenges for naval and other maritime stakeholders has made criminal actors to engage in human trafficking. Thus the GoG serves as a potential means to human trafficking. Trafficking in persons along with the links to organized crime and the significant human rights, economic, social, and political impacts are acknowledged as endangering human and national security (Abiodun & Dahiru, 2020). In most instances, criminals involved in the act along the GoG consider human trafficking as the lowest risk activity for criminal groups (Chapsos, 2016). Most forms of trafficking that take place in West Africa are men, women, and children trafficked for labor and domestic work; women and children trafficked for commercial sexual exploitation through online activities (Konrad et al., 2016).

2.2.4 Illicit Drug Trafficking

Communication being mainly dependent on IP-based systems, there is an increased risk of information breach by criminals to disrupt the monitoring of illicit drug smuggling along the GoG (Beseng & Malcolm, 2021). Information can be accessed, usurped or corrupted the complexity of the networks and the multilateral and joint operating environment also contribute to increasing the risk of information breach. When this is done, small boats are tool for the purpose of illicit drug smuggling,

especially small canoes, which have no documents aboard and which carry passengers without identity cards (Ukeje, 2015). That method of transport avoids any customs duty. In other empirically discussed overview of maritime security threats in the GoG, Chamberlain (2008) discussed security threats in maritime domain.

Kim (2019) argued that the adoption of some measures such as introduction of the International Shipping and Port Security Code, Proliferation Security Initiative (PSI), Container Security Initiative, and the Customs-Trade Partnership against Terrorism, have helped enhanced maritime security and led to the protection of shipping in general. Despite the argument advanced by the author, the shortfall of the article is the fact that the author did not consider maritime cyber attacks to be one of the organised crimes in the GoG region. This could be as a result of insufficient awareness on the subject matter. This study addressed this in subsequent themes.

2.3 Cyber attacks or incidents in the maritime domain

Although maritime environments and ships may seem like unusual targets for cyber-attacks, they are vulnerable due to the growing digitalization of the maritime environment and the increased use of industrial control systems (ICS), IT systems and OT systems. Cyber attacks are growing more common, and coordinated criminal networks and opposing states are increasingly targeting all parties in the digital value chain (Kesseler & Shepard, 2022). Figure 3 shows top-10 list of maritime cyber threats or attacks categorised under similar characteristics among the incidents and are ranked based on frequency and severity.

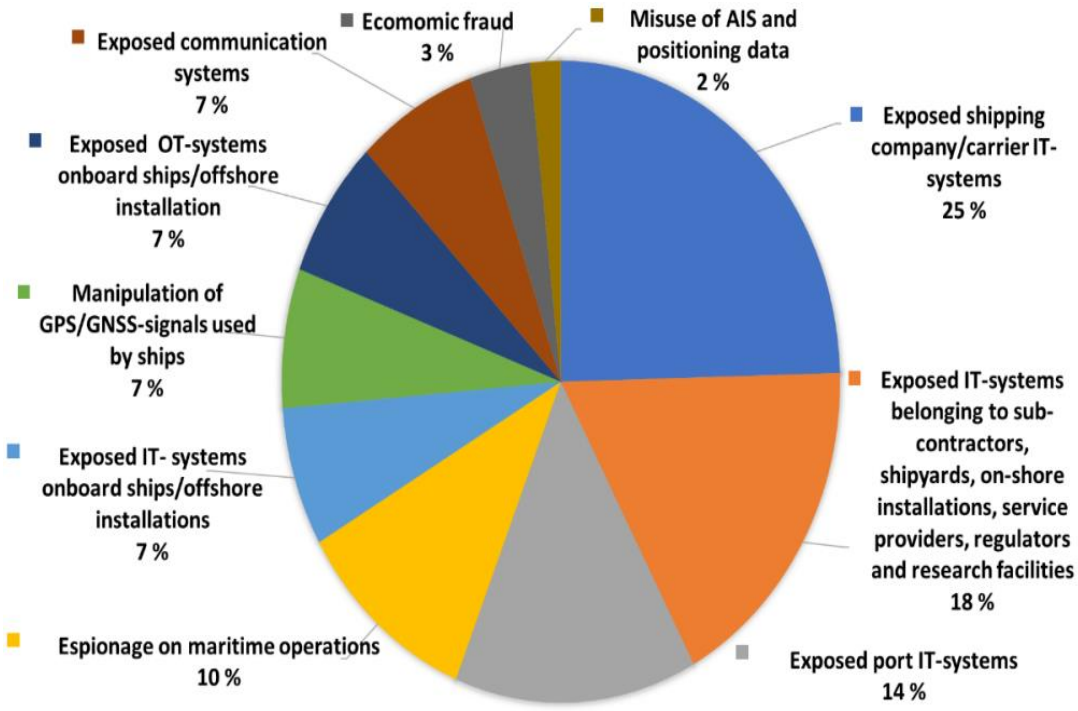


Figure 3. Top ten (10) cyber incidents based on categorization.

Source (Meland et al., 2021)

Most reports and literature in recent times, share a common goal, that is the frequency and severity of cyber attacks are increasing. According to Gehem et al., (2013), IBM in 2013 reported that the average business or organization experienced about 109 cyber incidents or attacks. The authors further indicated that in 2014, the same IBM in its Cyber security intelligence report indicated that over 95% of the attacks can be attributed to human errors, ranging from poor password protection including the usage of unsecured internet connection and others. In confirming to the recent increase in cyber attacks, Loomis (2021) in his study posit that reports of maritime cyberattacks increased by 400% in 2020, while attacks on port facilities or systems and shipboard technologies increased by 900% over the previous three years. Greenberg (2018) argues that after the NotPetya malware, a cyber attack spread from infected Ukrainian tax-preparation software called MeDoc, Maersk was

attacked and the company spent more than $300 million in repairs and remediation over the course of 10 days before it could resume normal operations.

Similarly, according to (Kesseler & Shepard, 2022) in October 2020, an advanced and powerful attack on the International Maritime Organization (IMO) was able to get past its dynamic cyber defences. Most likely, an old version of the Microsoft SharePoint Web server caused IMO's public website, intranet, and other services to be down for several days. Likewise, in 2017, Danish shipping company A.P. Moller-Maersk was the target of a ransomware assault, which became one of the most famous cyber events in the maritime industry. It is worth noting that all these attacks caused these companies huge sums of money to restore their systems back. This goes to shows how powerful cybercriminals have penetrated the maritime space.

It is necessary to mention that, 2020 and 2021 saw the most cyber attacks on the maritime industry and ransomware cyberattacks was on the increase. For instance, according to Kesseler and Shepard (2022), a Toll Group, an Australian transportation and logistics company in the maritime supply chain, was struck by ransomware in January 2020 and May 2020. In both situations, it affected their services. Similarly, In October 2021, ransomware propagated into Danao's Management Consultants' networks, a well-established IT firm serving the maritime industry since 1986. Danao's Maritime Software Suite encompasses chartering, payroll, crewing, analytics, document management, procurement, and online collaboration (Kesseler & Shepard, 2022).

Although the aforementioned reports or incidents are worth noting for the maritime industry, the authors of these reports fail to indicate what the contributing factors were and whether the human elements in those organizations contributed to these incidents or not or as a result of lack of awareness on the part of personnel or as result of exposed shipping company/carrier IT-systems or OT systems. All these were not demonstrated.

2.4 Human element as the weakest link in maritime cyber security attacks

To begin with, even though cyber vulnerabilities of information systems have been studied and written about a lot, there still exist some gaps, especially when it comes to cybersecurity awareness among humans and the management of information including communication technologies (Digrazia, 2018).

In recent times there has been a lot of progress in maritime technology, but the industry including navies still relies heavily on humans, therefore human error is understood to be an acknowledged danger in day-to-day activities (Barnett & Pekan, 2017). Hence, as a result of this, the connection between risk and safety has often become complex. Furthermore, insecure information technology (IT) systems result in substantial damages, and human action is largely associated all along the way with the loss. Likewise, human mistakes are to be blamed for a lot of the cybersecurity threats that happen in industries including the maritime industry (Webb et al., 2014). Furthermore, according to the most recent analysis on data breaches conducted by Verizon, 85 % of all data breaches are caused by human factor (Verizon, 2021).

Lately, organizations have demonstrated the need to raise their operatives or work security awareness and knowledge so as to practice cyber hygiene and not be manipulated by cybercriminals. For instance, in the studies of Boletsis et al., 2021and Meshkat et al., 2020, they assert the human factor continues to be the key most significant internal concerns that organizations face including the maritime industry with regards to their cyber security. Similarly, this claim is supported by data presented in the most recent BIMCO white paper on cyber security, which shows that human error is the primary source of security challenges for 52 percent of responding businesses (HIS Markit, 2020).

Conversely, the European Union Agency for Network and Information Security (2017) argues that although the human factor is seen as weakest link and blamed for

about 80 to 85% of cyber attacks, the human error can be mitigated by training and education, and the growth of a strong cyber safety culture. This will then allow humans to act as robust firewalls against maritime cyber attacks or incidents. Additionally, to reduce the risk posed by the human element in relation to cyber attacks, Berg (2013) argued that there is the need for adequate training to raise the awareness on maritime cyber security, the use of qualified personnel at the right places, and further the application of the good management policies in the maritime industry.

Consequently, it is therefore imperative, that the people who operate or take care of digital systems have the right knowledge and skills to make sure that their decisions and the decisions of others don't put the safety of activities in the maritime space at risk. This is encouraged even more by the Just culture according to IMO (2010). Also there is the need to for the maritime industry including navies to focus more on developing their personnel to act robust firewalls against maritime cyber security.

Similarly, Bauer and Bernroider (2017) indicate that the most effective way is to increase personnel or crew’s knowledge or awareness of cyberattacks and maritime cyber security is through information security training, which should be mandatory. That is the gap that is been presented in the maritime industry where personnel sufficient knowledge on this emerging threat, maritime cyber security.

Sequel to the above, the gap that is research sought to achieve is to find out the level of awareness of maritime cyber security in navies since they are key stakeholders in the maritime industry as well.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Introduction

This chapter will outline the methodology and approach that was used to perform the research. Further, it will explain how the approaches or methods were used to answer the research questions (RQ) mentioned in Chapter One. To help recap, this study focused on the following RQ areas:

- RQ1 What is the state of maritime cyber security awareness in the Ghana Navy?
- RQ2 How prepared is the Ghana Navy to mitigate or prevent cyberattacks?
- RQ3 Identify if there is any maritime cyber security framework that guides the operations of the navy and what are its basic principles?

3.2 Methodology of the Study

According to Danzin (2010), the methodology of a study relates to how it is planned to guarantee that data is collected in a way that provides accurate and reliable answers to the research questions. Because the method used in a study improves the validity and trustworthiness of the research's results and conclusions, research methodology is crucial (Kothari, 2004). Consequently, this research made use of both qualitative and quantitative methods (Figure 4), as derived from the triangulation viewpoint, which is an approach that also falls in line with the study of Johnson and Christensen (2019), who found it useful and implemented it into their research.

The quantitative method assisted the researcher to obtain respondents' perspectives on the level of awareness of maritime cyber security in the Ghana Navy, the importance of maritime cyber security knowledge, and how cyber resilient the Ghana Navy is. Qualitative research methods are focused and require in-depth analysis of

details of a particular area of study. The qualitative approach will be used to acquire an objective answer to the research question on how to establish an optimal maritime cyber framework for the navy. The quantitative will be employed because this method makes use of measurements and statistical analysis of data that are collected (Frankfort-Nachmias & Leon-Guerrero, 2018). Further, in quantitative research, it is possible to collect numerical data to generalise results across groups.

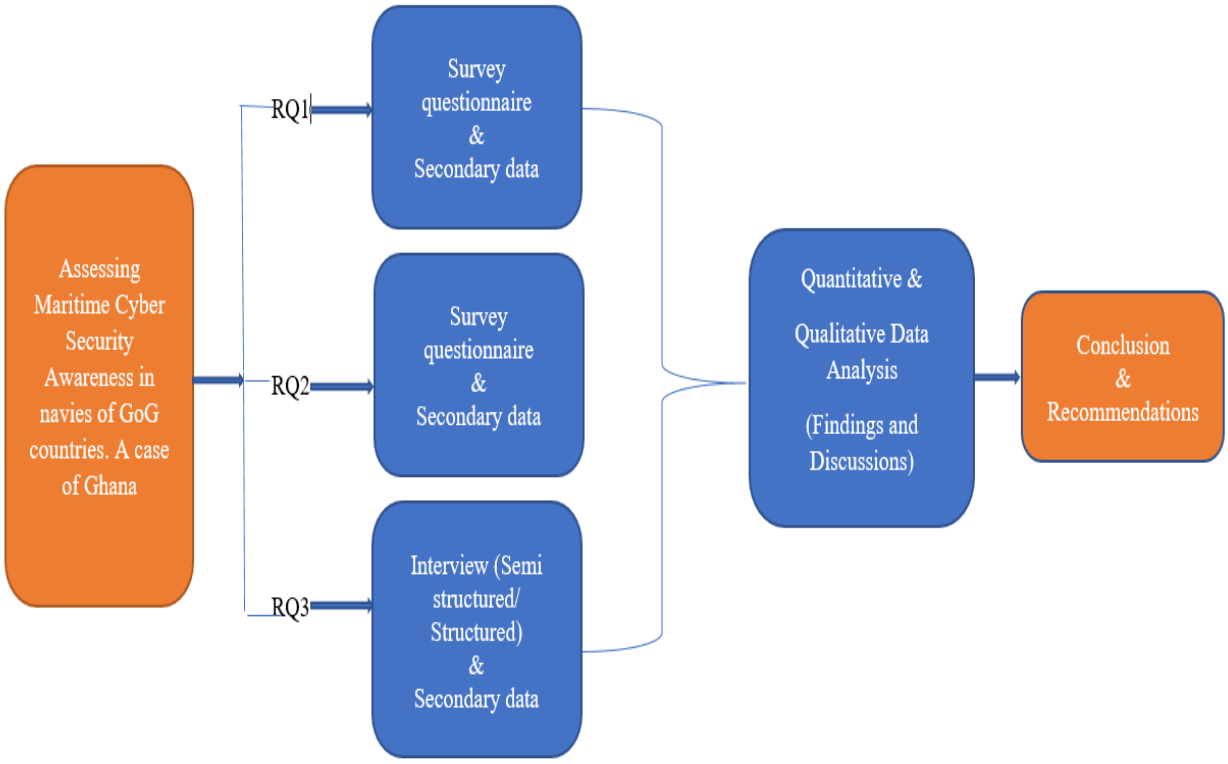


Figure 4. Summary of Research Approach/Structure.

Source: (Created by the author)

3.3 Study Area and Data Collection

The research was conducted with Ghana Navy as the epicentre of attention. To begin with, the areas that were focused on included the MOCs which are spread along Ghana's coast from the Western border to Aflao at the Eastern border. Other places where the MOCs are located include Burma Camp in the Greater Accra Region,

Tema also within Greater Accra and Sekondi in the Western Region. Further, the Ghana Navy Fleet and MMCC Zone F shore-based infrastructure also formed part of the study area. With respect to the data collection, Ghosh (1992) posits that data collection is a systematic process of assembling observations or measurements in research to attain a purpose. Both qualitative and quantitative approaches were employed in this research. A survey questionnaire was administered to participants to solicit information from them.

3.4 Data Sources

There are diverse methods used to collect data and these fall under two groups, that is primary and secondary data (Douglas, 2015). This research would collect both primary and secondary data. Researchers or scholars agree that the mark of a good case study is the adoption of different data sources, an approach that enhances the credibility of the data. Given that, this research would employ both primary and secondary data as a form of data triangulation to guarantee the credibility as well as the reliability of the information that will be obtained. A survey questionnaire was conducted within the Ghana Navy and participants were drawn from the Fleet, MOCs, and MMCC Zone F. With respect to the interviews, participants were drawn from different organizations across the world with backgrounds in cyber security

3.6 Data Analysis

The survey questionnaire was divided into four (4) sections; Section A focused on the respondent's background, examining issues like demographics, with Section B focusing on identification of the awareness in relation to maritime cyber security. Further, Section C focussed on the investigation of standard operating procedures and Section D looked at the preparation of the navy against maritime cyber attacks. The quantitative data was analyzed using Microsoft Excel and Statistical Package for the Social Sciences (SPSS) version 26 and also both descriptive and inferential statistics be used. Descriptive statistics include the data for age, gender, and level of education. On the other hand, principles of inferential statistics were used to

determine the level of awareness of maritime cyber security. The responses from the survey questionnaire were finally analysed to draw conclusions. QuestionPro software was used to administer the survey questionnaires and it was chosen due to its convenient organisation features including the ability to export data to other softwares for further study. Furthermore, information gathered from the interview helped to assess the need for a framework for maritime cyber security to guide the operations of navies.

3.6 Reliability and validity

This research's mixed-method approach yielded profound insights and details concerning the objectives of the research. With regards to the semi-structured interviews, the questions on the maritime cyber security framework were carefully crafted and validated by the Professor (supervisor) with extensive experience in the navy and maritime sector. For the quantitative part, large number of naval personnel (116) who participated lead to achieving a valid and reliable research outcome.

3.7 Sampling, selection of participants

A sample size was derived using the Cochran's formula (Cochran 1977). The sample size was determined based on proportion of individuals (84%) who had high level of awareness on cyber security in a previous study conducted in Ethiopia (Demissie Gizaw et al., 2018).

The formula is as stated below:

$$n = \frac{Z^2_{1-\frac{\alpha}{2}} P(1-P)}{e^2}$$

n - The sample size

z = 95% confidence interval (standard value 1.96).

e - The desired level of precision or level of acceptable error = 0.05

$$n = \frac{1.96^2[0.84(1-0.84)]}{0.05^2}$$

n = 3.8416×0.1344/0.0025, therefore, n = 206

Therefore, the sample size that was targeted for the quantitative aspect of the study was 206 with the assumptions of 95% confidence level and 5% precision. However, some of the respondents did not answer the online survey, hence, ended up with the arrival of respondents' feedback of 116.

3.8 Ethical Considerations

According to Creswell (2014), ethical consideration involves the protection of participants to guarantee the trust and integrity of the study as well as guard against misconduct that is likely to echo negatively on the participant's organization. Hence, this research complied with the WMU Research Ethics Committee standard. Participants' consent was sought and recorded before the survey questionnaire and the interviews were conducted. Hence, the confidentiality of the retrieved data was strictly maintained. Further, for the purpose of transparency and mutual trust, the purpose, essence, sequence of discussions, and intended uses of data were explained to participants. The information that was collected was kept secret and anonymous, and it was stored safely with a password and it would be deleted safely when the study is over.

3.9 Chapter Summary

In this chapter, the study methodology, detailing the tools and procedures employed to compile this dissertation and provides context for the data sources. Mixed method comprising quantitative and qualitative research were described and how the data of this study were collected. Furthermore, this chapter explained how the estimated sampling size was arrived at using Cochran's formula.

CHAPTER 4

FINDINGS AND DISCUSSIONS

4.1 Introduction

The previous chapters provided the basis and indicated the methodology that was used to conduct the research. The main findings of the research will be presented in this chapter, along with a discussion of how those findings compare to those of previous studies. The purpose of data analysis is to support the attainment of the study's objectives. The expected outcome of this chapter therefore includes a critical understanding of the current awareness level of maritime cyber security in the navy and how well prepared the navy is in relation to cyber attack threats. Consequently, the data analysis enabled the researcher to come up with a maritime cyber security framework for the navy. First part of chapter deals with quantitative data analysis and the later part will analyse the qualitative data and draw inferences from it.

4.2 Research Findings: Quantitative Analysis and Discussion

Survey questionnaires were sent to personnel of the Ghana Navy, both officers and ratings through QuestionPro online platform and in person on the field as well. The presentation of the research findings from the survey questionnaires was characterized into four sections. The sections or thematic areas comprise the demographic characteristics of respondents, maritime security awareness, assessing standard operating procedures, and preparations of the navy against maritime cyber attacks. The findings of the survey questionnaire helped the researcher to address the RQ1 and RQ2. The interview questions were also qualitatively analysed and discussed as well.

4.2.1 Demographic characteristics of respondents

A total of 116 respondents were sampled for the study. Most respondents representing 65 (56%) were between the ages of 31-40 years followed by those between 18-30 years 44 (37.9%), few respondents 4 (3.4%) were between the ages of

41-50 years and 3 respondents representing 2.7% were above 50 years. The significance of the data regarding the age of respondents lies in the fact that the researcher collected responses from personnel who had previous relevant work experience. The implication of the respondents' characteristics to the study was observed in respondents' responses which indicated understanding and situational awareness with regard to the level of maritime cyber security awareness. The substantial number of knowledgeable respondents lends credibility to the results of the study's data collection and, consequently, its findings as depicted in Table 1. With regards to the highest level of education attained, the results showed that majority of respondents 47 (40.5%) had SHS/SSS, 39 (33.6%) had first degree, 14 (12.1%) had Diploma/ HND and 8 (6.9%) had master's Degree as shown in Figure 5. With respect to gender, most respondents 109 (93.9%) were males whilst the remaining 7 (6.1%) were females. The demographic characteristics is as illustrated in Table 1.

Table 1: Demographic characteristics of respondent's (N=116). Source (Reseacher)

Variable	Frequency	%
Age (Yrs.)		
18-30	44	37.9
31-40	65	56.0
41-50	4	3.4
>50	3	2.7
Educational level		
Basic	8	6.9
SSS/SHS	47	40.5
HND/Diploma	14	12.1
First Degree	39	33.6
Master's Degree	8	6.9
Gender		
Male	109	93.9

Female	7	6.1

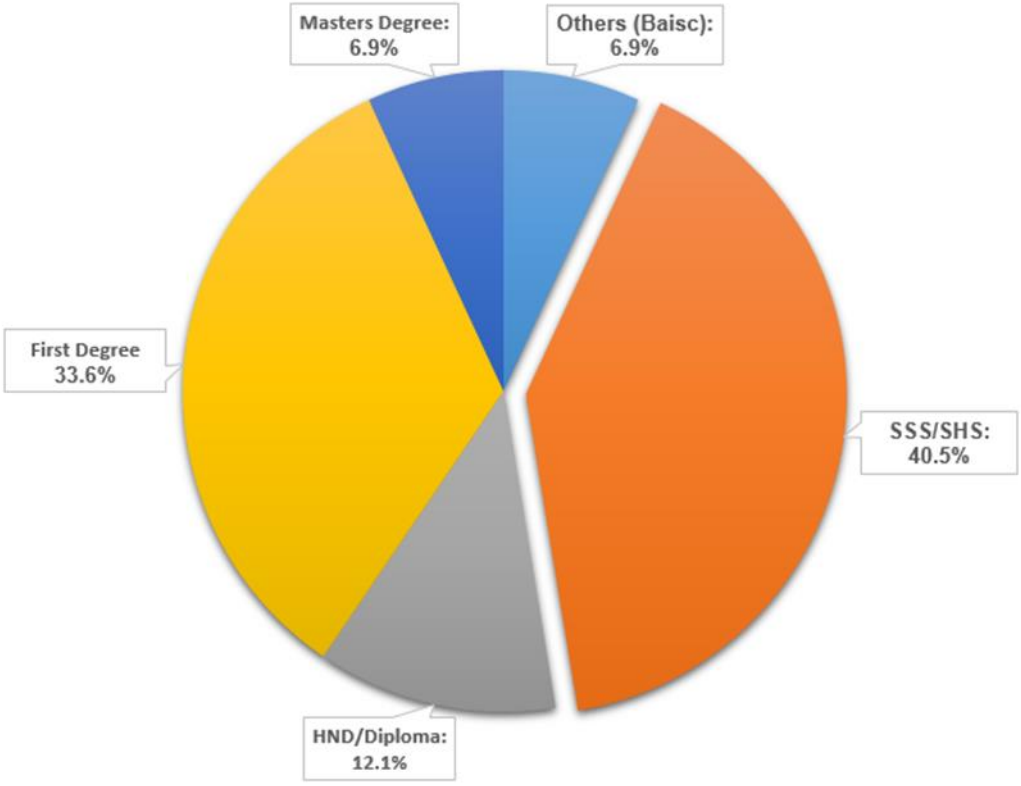


Figure 5. Respondents' level of Educational Distribution.

Source (Researcher)

The gender status or distribution was also analysed and it plays a key role with respect to awareness of maritime cyber security. The gender analysis carried out in this research is not restricted to the participation of females in the study alone, but instead allows for the collection of a broader spectrum of viewpoints in relation to the objectives of the study. Accentuating the earlier point, Hudson (2011) in his study noted that a broader spectrum of viewpoints provides reliable empirical data on the gendered nature of maritime security related issues, ideas, and practices to which maritime cyber security is no exception. Consequently, with respect to the findings,

male respondents were 109 out of 116 counts corresponding to 93.9% and 6.1% were females (Table 1). One could attribute the high per cent of male respondents to the male dominant nature of the military profession. The military is traditionally viewed as a man-dominated field, which goes to elucidate the overwhelmingly male percentage. However, the small proportion of females in the study shows that more women should be included in discussions about maritime security, including maritime cyber security in Ghana and the GoG at large.

4.2.2 Awareness of maritime cyber security

This section sought to obtain the respondents' awareness level of maritime cyber security. Respondents were first and foremost assessed to rate the threat levels that the variables presented to them pose to Ghana's maritime security in the survey questionnaire. The diverse responses with corresponding percentages obtained are illustrated in Figure 6. From the study findings, the respondents identified or rated IUU fishing and smuggling as high threats with 70.79% and 62.81% respectively as shown in Figure 6. However, respondents considered or rated maritime cyber attacks as least with score of 47.65%. The reason majority of the respondents assigned to the least rate of 47.65% was that they believed the other threats presented to them are day to day threats that they encounter at sea or hear on the media compared to the maritime cyber attack, hence the least score assigned.

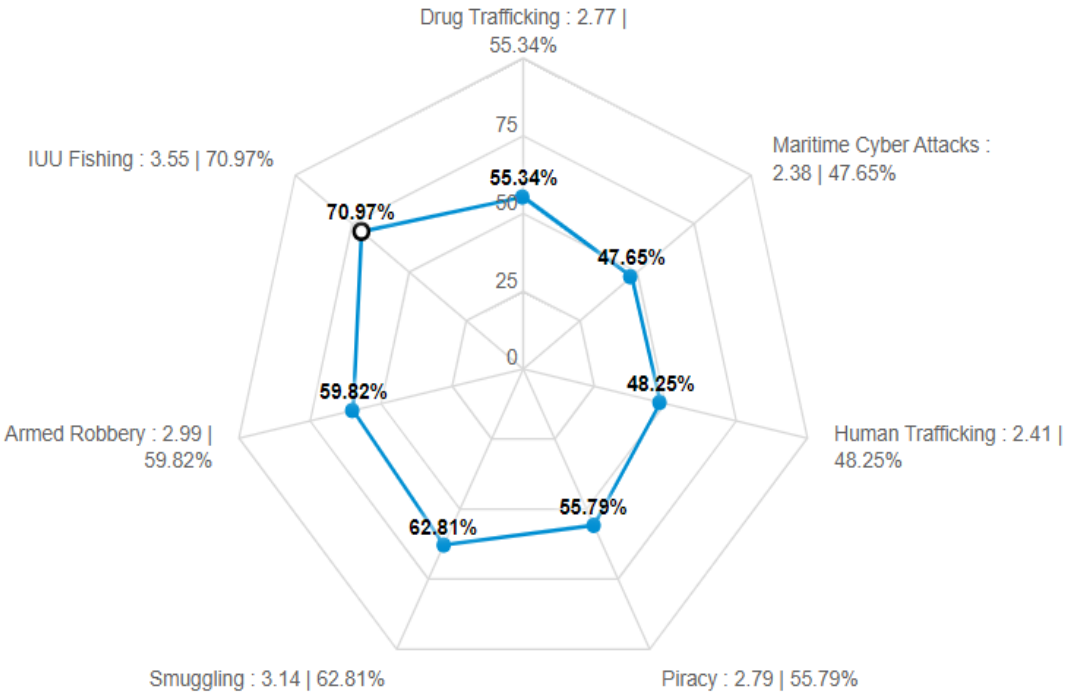


Figure 6. Maritime security threat perception in terms of awareness in the GoG. Source (Researcher)

Furthermore, the proportion of naval personnel with awareness on maritime cyber security was determined. Awareness was classified into two (2) as; low level of awareness and high level of awareness. Consequently, awareness on maritime cyber security was assessed by asking ten (10) questions. This was done by using a Likert scale with five (5) point ratings; “Very low”, Low “Average”, “High” and “Extremely high”. The respondents were allowed to choose only one response. A scoring technique was assigned to each rating. Extremely high was given the highest score of 5, high (4), average (3), low (2) and very low (1). The individual score was added and the sum was determined. Depending on the summative score of the questions, since there are ten questions that was used to access awareness, an individual score would fall between 10 and 50 with an average score of 30. Any respondents with a score below the average (<30) was classified as having low awareness, whilst those with scores above the median (>30) were classified as

having high awareness. Any individual with a score equal to the average (=30) was classified as having average awareness.

The results showed that the proportion of naval personnel with high level of awareness of maritime cyber security was 72/116 (62.1%) and those with low level of awareness was 44/116 (37.9%) (Figure 7). The findings from the aforementioned imply that the awareness level of maritime cyber security in the Ghana Navy is high considering that 72 out of the 116 respondents demonstrated a high level of awareness representing 62.1% on the subject matter compared to the 44 respondents that demonstrated low level of awareness representing 37.9%. However, this result of high awareness is in contrast to that of the study of Heering et al. (2021), where they assessed the level of awareness of maritime cyber security to be low among port authorities, government bodies and other maritime companies.

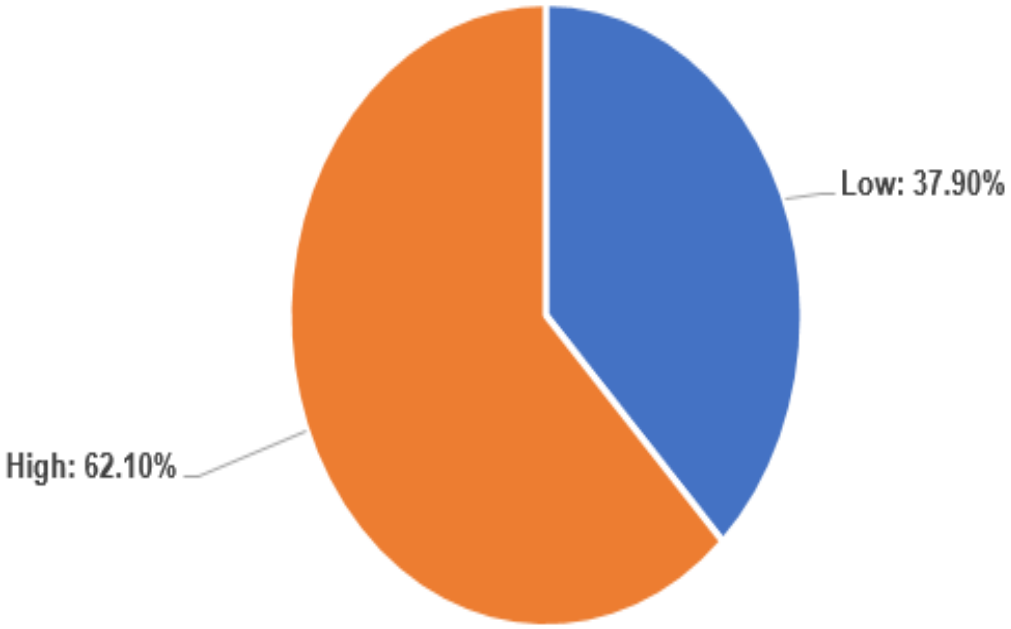


Figure 7: Proportion of naval personnel with awareness on maritime cyber security. Source (Researcher)

It is worth noting that, though the level of awareness in the navy was assessed to be high, one of the questions which sought to know if personnel had undergone official

training on maritime cyber security revealed interesting feedback. The results as demonstrated in Figure 8 indicated that 89% responded “No” while 7% of respondents indicated “Yes”. The remaining 4% indicated “Not Sure”. The inference that can be drawn here is that, there is the need for more maritime cyber security training to be factored into the training regime of the navy to help raise further awareness among personnel of the navy. The need for more training in enlightening further awareness is supported by the results of the question if respondents needed training on maritime cyber security. All the respondents indicated “Yes”, that they need training, and is this depicted in Appendix C. Training on awareness is very key since personnel or humans are perceived as the weak link in relation to maritime cyber security breaches (Safa & Maple, 2016). Therefore, the need for training of personnel or the human factor is consistent with studies by Heering et al. (2021), where they indicated that training of the human element would reduce the chances of cyber attacks since cyber criminals mostly target humans to achieve their end state.

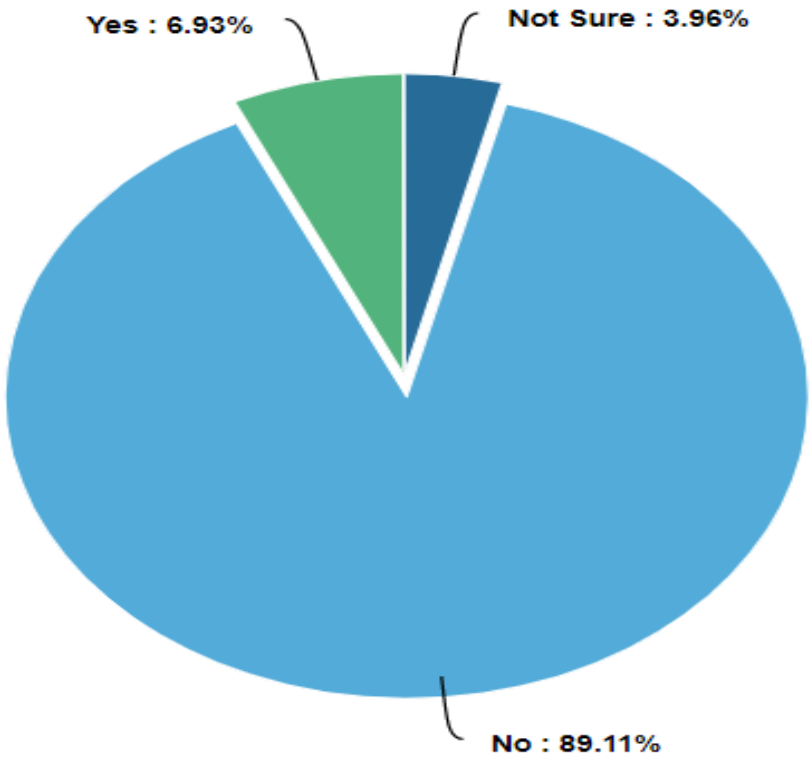


Figure 8. The results of respondents on formal training on maritime cyber security

Source (Researcher)

4.2.3 Association between demographic data and awareness of maritime cyber security

A bivariate analysis[2] was conducted to determine the association between demographic data and awareness on maritime cyber security. This was tested using 95% confidence level. The results showed that that the following demographic variables were significantly associated with awareness; Age ($\chi 2 = 3.752$, $p = 0.042$), educational level ($\chi 2 = 4.292$, $p = 0.018$). Gender of respondents did not significantly influence awareness on maritime cyber security at 5% level of significance ($p>0.05$) ($\chi 2 = 2.752$, $p = 0.174$) (Table 2).

Table 2: Association between demographic characteristics and Awareness. Source (Researcher)

	Awareness level n (%)			$\chi 2$	p-value
	Low	High	Total		
Age				3.752	0.042*
18-30	30 (68.2)	14 (19.4)	44 (37.9)		
31-40	11(25.0)	54 (75.2)	65 (56.0)		
41-50	2 (4.5)	2 (2.7)	4 (3.4)		
>50	1(2.3)	2 (2.7)	3 (2.7)		
Educational level				4.292	0.018*
Basic	6 (13.6)	2 (2.8)	8 (6.9)		
SSS/SHS	21(47.7)	26 (36.1)	47 (40.5)		
HND/Diploma	4 (9.1)	10 (13.9)	14 (12.1)		
First Degree	11(25.0)	28 (38.9)	39 (33.6)		
Master's Degree	2 (4.6)	6 (8.3)	8 (6.9)		
Gender					
Male	40 (90.9)	69 (94.5)	109 (93.9)	2.752	0.174
Female	4 (9.1)	3 (5.5)	7 (6.1)		

***Significant at p<0.05**

4.2.4 Multiple Logistic Regression of factors influencing Awareness

Multiple logistic regression analysis was conducted on all demographic characteristics that were found to be statistically significant or not at the bivariate level. These factors were; age, educational level and gender. The results show that

[2] It is one of the forms of statistical analysis, used to find out if there is a relationship between two sets of values.

with age, respondents who were between the ages of 31-40 years were approximately three times more likely to have a high level of awareness of maritime cyber security compared to those with age between 18-30 years (AOR=2.55; 95% CI=1.029-5.919, p=0.017). The logistic regression results further showed that respondents who had first degree level of education had an increased odd of having a high level of awareness of maritime cyber security compared to those with basic level of education (AOR= 1.82; 95% CI=1.174-5.728, p=0.025). Regarding gender, females were more likely to have a high level of awareness of maritime cyber security compared to their male counterparts although the association was not statistically significant (AOR= 1.28; 95% CI=0.782-4.719, p=0.285) (Table 3).

Table 3: Multiple Logistics regression of the factors associated with Awareness.
Source (Researcher)

Variable	**Awareness**		**COR (95%Cl)**	**AOR (95%CI)**	**p-value**
	Low	**High**			
Age (yrs)					
18-30	30 (68.2)	14 (19.4)	1.0 (ref)	1.0 (ref)	
31-40	11(25.0)	54 (75.2)	2.84 (1.231-5.629)	2.55 (1.029-5.919)	0.017*
41-50	2 (4.5)	2 (2.7)	0.81 (0.35-2.537)	0.92 (0.582-2.874)	0.149
>50	1(2.3)	2 (2.7)	0.72 (0.385-2.852)	0.65(0.291-3.728)	0.282
Educational level					
Basic	6 (13.6)	2 (2.8)	1.0 (ref)	1.0 (ref)	
SSS/SHS	21(47.7)	26 (36.1)	0.32 (0.201-2.345)	0.44(0.115-2.820)	0.163
HND/Diploma	4 (9.1)	10 (13.9)	0.12 (0.067-1.922)	0.27 (0.127-2.855)	0.284
First Degree	11(25.0)	28 (38.9)	2.92(1.229-5.387)	1.82(1.174-5.728)	0.025*
Master's Degree	2 (4.6)	6 (8.3)	0.48 (0.2827-1.643)	0.42(0.287-1.729)	0.181
Gender					
Male	40 (90.9)	69 (94.5)	1.0 (ref)	1.0 (ref)	
Female	4(9.1)	3(5.5)	1.34 (0.628-4.625)	1.28 (0.782-4.719)	0.285

*p<0.05, ref: reference

AOR: Adjusted Odds Ratio

COR: Crude odds Ratio

4.2.3 Assessing the preparedness of the navy against cyber attacks

To help assess the preparedness of the Navy against cyber attacks, a one sample T-test was used. Three main questions were asked in the survey questionnaires and scored were assigned to the answers that participants selected. After the feedback, a hypothesis was established to help establish this answer. The hypothesis was that; The Ghana Navy is prepared to deal with cyber attacks. The mean test value assigned was 3.5 and p-value of 0.05. If p less than 0.05, the null hypothesis will be rejected. After the SPSS was used to analysis the one sample t-test, it revealed that the mean difference was 1.85345 compared with the test value of 3.5. From results Table it implies that null hypothesis should be rejected, since the mean difference is lower from the test value, implying that the navy's preparation is not adequate. However, since the mean difference is not that much from the test value, in terms of percentage gives approximately 53%. It can be concluded that the navy's preparation against cyber attacks is average. Hence there is the need to invest in more cyber security solutions and training of personnel in that regard.

T-Test

[DataSet1]

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
PNMC	116	5.3534	2.19586	.20388

One-Sample Test

Test Value = 3.5

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
PNMC	9.091	115	.000	1.85345	1.4496	2.2573

Figure 10. Results of one sample t-test Source (Reseacher)

4.3 Research Findings: Qualitative Analysis and Discussion

The qualitative survey was aimed at focusing on RQ3. The feedback from the interviewees helped the researcher to develop a proposed maritime cyber security framework for the navy. Eight (8) interviews were conducted using semi structured questions; additionally, nine (9) structured questions on the same interview guide questions were sent through QuestionPro link generated for the intended interviewees to answer due to their busy schedule, not allowing for the interview. The recorded interviews took approximately 20 to 30 minutes. They were later transcribed, coded and finally analyzed with the MAXQDA Analytics Pro 2022, software. Subsequent paragraphs are the outcomes and discussions of the interview guide questions.

Q1. How important is maritime cyber security to the operations of navies in general?

This question was meant to ascertain the importance of maritime cyber security to the operations of navies in general. Here, all the respondents indicated that maritime cyber security is very important to the operations of the navies and security in general. For instance, Interviewee (INT) 3 indicated that:

> "*Maritime Cyber Security is very important in the operations of navies, because naval operations rely on navigational and surveillance systems. The integration of maritime transport systems into a digitized world through the use of GPS, ECDIS, Satellites, Radars, surveillance systems, and other shipboard security systems to mention a few. If they are not secured well, it can be vulnerable to cyber threats*".

In addition, most of the interviewees intimated that most navies have integrated systems that help them with communications, surveillance, and navigation of their platforms, and also assist with the operations of their shore-based installations, therefore there is the need for navies to take maritime cyber security very important

and factor it into their safety management system. On the contrary, others intimated that although important, maritime cyber attacks in recent times serve as very critical threat to the maritime sector because cyber security awareness is very low in terms of cyber security knowledge and skills. Consequently, navies are required to play a lead role in developing policies or frameworks for cyber security. Additionally, navies need to improve their cyber security awareness through information sharing, capacity building, and awareness raising by working together closely with other key maritime stakeholders to strengthen and keep their cyberspace secured from cyber threat challenges.

Further, three (3) main codes or themes were assigned using the MAXQDA Analytics Pro; Cyber threats, Role and Systems. These three (3) themes were the most frequent in the respondents' feedback. Approximately 65% of the respondents as part of their explanation intimated that maritime cyber security is important because of the existence of cyber threat, as illustrated in Figure 11. Further, 47% of the respondents agreed to its importance in relation to the systems employed in navies. The respondents believed that the systems employed by navies should be well secured or protected.

To confirm the importance of maritime cyber security to the maritime industry including navies, Hareide et al. (2018) explained that naval operations and maritime operations are not immune to cyber threats, since the maritime industry has embraced technology in their day to day operations, hence the need for education on the part of their personnel is paramount. Furthermore, the feedback from this question is consistent with the studies of Karamperidis et al. (2021) and Tam & Jones (2018), who indicated that maritime cyber security is indeed important for the protection or securing of maritime assets including shore-based surveillance installations against cyber threats, hence less knowledge on it could lead to cyber criminals attacks valuable systems of the maritime industry.

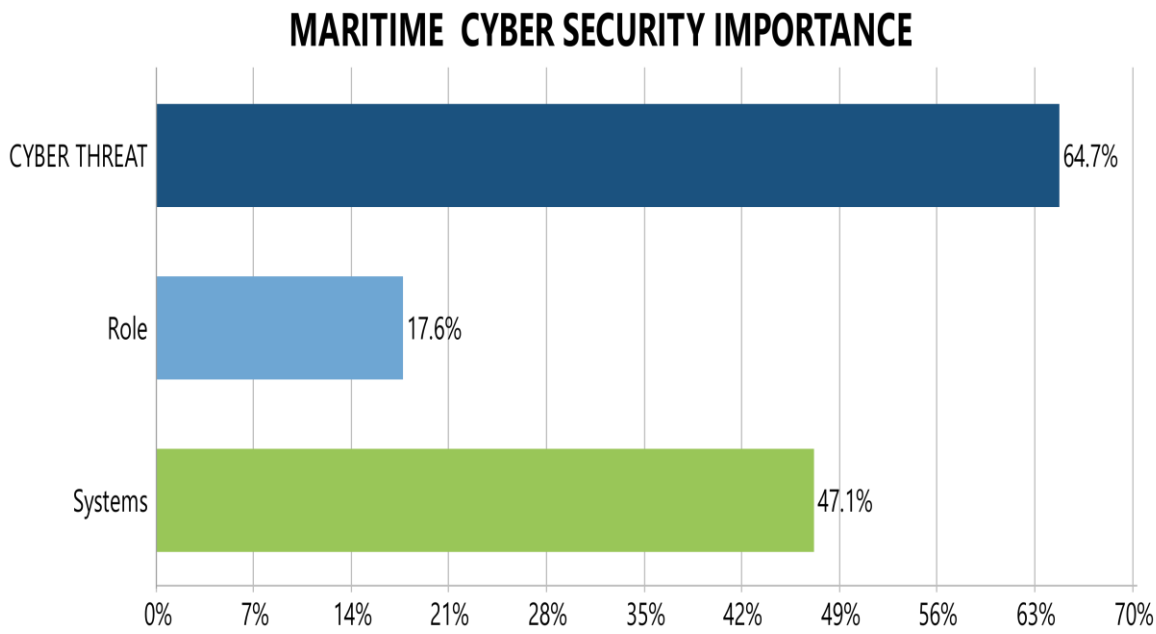


Figure 11. The three (3) themes assigned to the importance of maritime cyber security.

Source (Researcher)

Q2. What are some of the weak links with respect to maritime cyber security governance/management?

This inquiry was intended to determine the weak links with regard to maritime cyber security management. To analyze this question, four (4) main codes or themes were assigned using the MAXQDA Analytics Pro; Governance, Resources, Communication Systems and Human beings were the themes that recurred the most in the interviews. All the interviewees revealed that indeed there are weak links when it comes to maritime cyber security management. After the analysis, the result indicated that approximately 88% of the interviewees indicated that human beings form the weakest link when it comes to maritime cyber attacks by cybercriminals (Figure 12). For example, INT 1 explained that:

"No industry or organization is immune to cyber threats. The maritime industry including navies relies on ICT Base systems for their operations. The integration of cyber technologies into maritime or naval operations comes with major vulnerabilities. Primarily personnel in the maritime industry including that of navies lack education in maritime cyber security. This makes the human element or beings act as weak links for cybercriminals to take advantage of. For instance, the unacceptable use of personal USB sticks and connected devices of personnel that breach cyber security protocols."

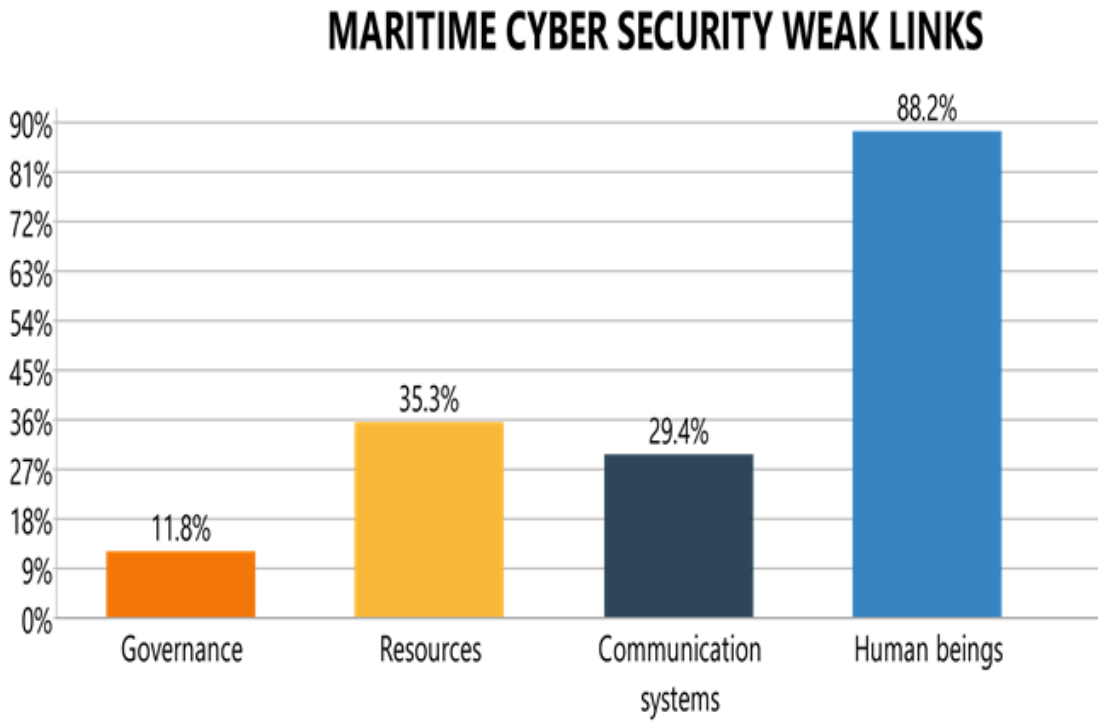


Figure 12: The four (4) themes assigned to maritime cyber security weak links.

Source (Researcher)

The 88% response on human beings or human element forming the weakest link is consistent with other studies such as Boletsis et al., 2021 and Meshkat et al., 2020, where their work revealed that although the safety and security issues have many facets or layers, the human factor continues to be one of the largest internal dangers to organizations' cybersecurity. Further, the aforementioned feedback from the

analysis is supported by the results of the recent white paper on cybersecurity published by BIMCO where 52% of respondents regarded humans as the greatest cyber security risk or vulnerability facing their organizations (HIS Markit, 2020). In addition to this, the most recent Verizon Data Breach study reveals the fact that the human element was involved in 85 % of all data breaches (Verizon, 2021).

Similarly, according to authors like Senarak (2021) and, Felsik and Zwolak (2020), the human factor interface continues to account for the majority of maritime accidents including maritime cyber attacks, therefore, making it the weakest link when it comes to cyber security. This is mainly due to the fact that personnel or crew lack adequate awareness in terms of training, knowledge, skill as well as experience when it comes to maritime cyber security. Hence, cybercriminals take advantage of their lack of awareness through emotional manipulation or social engineering.

Furthermore, 35.3% of the interviewees explained that resources serve as the weak link in maritime cyber security. Also, 29.4% generally intimated that a lack of good communication systems such as robust ICT infrastructures could act as weak links that the cybercriminals could prey on. This is consistent with the studies of Abdalrahman and Varol (2021), who revealed that security technology is only as good as its strong systems including communication systems. They also indicated that if the security networks of the systems including communication and surveillance systems and their softwares are not strong or patched well and up-to-date, it makes the connected devices serve as chief targets or weak links for cyber attackers. From the aforementioned, it is, therefore, necessary for organizations including navies to enhance the security of their connected systems or devices.

It is worth noting that, approximately 12% of the interviewees explained that governance also plays a role as a weak link in the architecture of maritime cyber security management. They emphasized that lack of governance such as policies, procedures, and good cyber hygiene practices to mention a few have not been fully

put in place for systems that are been used daily. The issue of governance is supported by Christou (2016), who indicated that there is still not overall governance for the framework on network and information security including maritime cyber security. The concept itself requires extensive explanation in order to convey information to the average sailor or rating in the navy. To this end, it is imperative that policies, procedures, and good cyber hygiene practices are made available and integrated into the training of naval officers and ratings.

Q3 What are your views on what an optimal framework would look like? or What would its essential components look like?

This question was meant to find out what an optimal framework looks like and it essential components or basic principles. The feedback that was generated from the interview enabled the researcher to assign five (5) themes using the MAXQDA Analytics Pro; namely Roles and Regulations, Sanctions, Training, Cybersecurity Plan, and NIST Framework as the components of a framework. Eighty-one per cent (81%) of the interviewees as demonstrated in Figure 13, explained that for an optimal framework, its component should constitute some elements of the NIST Cybersecurity Framework (CSF) or the NIST CSF should serve as a baseline for establishing organizations including navies' maritime cyber security framework. The elements of the NIST CSF include recover, identify, protect, respond and detect cyber security risks.

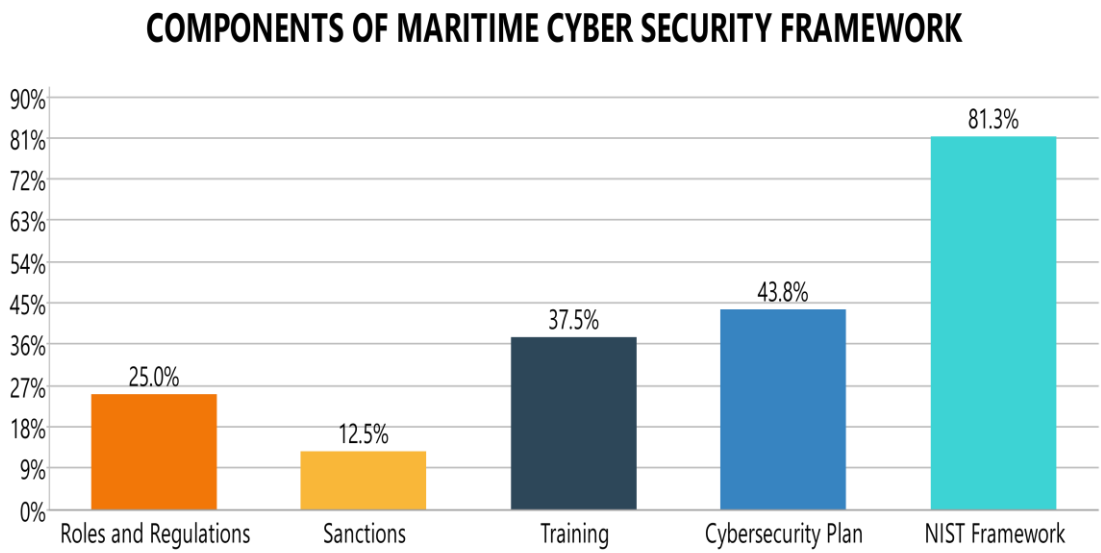


Figure 13. The five (5) themes assigned to components of maritime cyber security framework. Source (Researcher)

The feedback on the elements of the NIST Framework forming part of an optimal framework of an organization is in line with the study of Gordon et al. (2020) who revealed that organizations and government agencies including navies all over the world have widely embraced the NIST CSF in their security architecture. It is, in fact, worthy to note that, the NIST CSF has swiftly emerged as not just one of the most frequently approved methods, but also one of the most globally acknowledged frameworks overall, which supports cybersecurity risk management within organisations. It is therefore essential for Ghana Navy to adopt the elements of the NIST Cybersecurity framework as a basis for developing its maritime cyber security framework to guide its operations.

Similarly, the navy could also complement the NIST CSF with some elements of the ISO 27001, which is the international Standard for best practice Information Security Management Systems (ISMS) including maritime cyber security. The ISO 27001 is stringent and thorough in terms of its guidelines for ensuring data or systems are safe and secure in accordance with the tenets of CIA Model (El-Bably, 2021). The

possibility of the navy complementing the NIST CSF with ISO 27001 is supported b Sulistyowati et al. (2020) in their study revealed organization could implement some features of the NIST CSF together with other frameworks such the ISO 27001, and COBIT to mention a few.

Also, approximately 44% of the interviewees as part of their responses indicated the need for a Cyber Security Plan (CSP) to be part of the essential components of the maritime cyber framework. Having a CSP as part of the maritime cyber security framework undeniably will assist to handle the security vulnerabilities in the related security evaluations by instituting standard precautions tailored to decrease the chance of a security breach and the repercussions of potential risks. The CSP being part of the cyber security framework is supported by the study of Turk et al. (2022) who assert that CSP is critical in coming up with a systematic framework to address cybersecurity in the construction sector.

Besides the CSP, 37.5% of respondents also pointed out that training should form part of the components of a framework for maritime cyber security. With the training component there, it will aid to raise the awareness of all personnel in the organization or navy on cyber security and not just for the IT personnel alone. Additionally, 12.5% explained that sanctions should be part of the components of the framework. When sanctions are part of it, it will deter operators or uses of systems who flout the cyber security protocols.

4.4. Chapter Summary

This chapter presented the research finding and the discussions as well. It looked at both the qualitative and quantitative analysis of the findings in this study and the discussions deduced from them. It was quantitative analysis was done using SPSS and other statistical analysis to arrive at the discussion. It was revealed that the level of awareness of maritime cyber security was high. However, in terms of preparedness for cyber attacks, the preparedness was assessed to be average from the

single t-test conducted using hypothesis generated for that. Also, MAXQDA Analytics Pro was used to analyse the qualitative aspect of the study. It was revealed from the interviews conducted that the human element forms the weakest link in maritime cyber security management which was consistent with most available literatures. It was also noticed that the navy currently has no maritime cyber security framework available.

CHAPTER 5

CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The chapter presents the conclusion, limitations and some recommendations for decision-making and future research relating to maritime cyber security.

5.2 Conclusion

This study was sparked by the dangers that cyber attacks or threats pose to the maritime industry as a result of low or poor awareness on maritime cyber security and the lack of preparedness of the maritime industries including navies to mitigate this threat. Hence related publications concerning maritime security threats including maritime cyber security, cyber attacks in the maritime industry, human elements as weak links to maritime cyber security helped with the theoretical as aspect of the research. The study was aimed at assessing the level of awareness of maritime cyber security in navies of the GoG countries, with a focus on Ghana Navy. Furthermore, it aimed at determining if the navy is prepared to handle cyberattacks. Therefore, the study assessed maritime cyber security awareness in the Ghana Navy.

Further assessment was done with respect to the demographic data gathered such as age and educational background. Therefore, the objectives of the study were achieved by analyzing statistically the questionnaire data collected. It was revealed that the level of awareness of maritime cyber security in the Ghana Navy was assessed to be high. In terms of age, it was revealed that those in the age range of 31-40 years had a high level of awareness of maritime cyber security compared to the other age ranges. Additionally, the logistic regression results disclosed that respondents who had a first degree level of education had an increased odd of having a high level of awareness of maritime cyber security paralleled to those with basic level of education. However, when various maritime threats including maritime

cyber attacks were presented to participants to rate them, participants rated maritime cyber security the least.

In addition, the study sought to determine how the navy was prepared to deal with cyber attacks. It was revealed that the level of preparation was average after the single t-test was conducted. Hence, there is a need for investment in robust maritime cyber security solutions and effective training of personnel in relation to cyber security. To investigate if the Ghana Navy has any maritime cyber security framework guiding its operations, it was disclosed that there is currently no framework on maritime cyber security, however, the relevant departments have been tasked to generate one. The interview analysis results together with other relevant documents assisted the researcher to develop a proposed maritime cyber security framework illustrated in Figure 14 that will help the Ghana Navy in the interim. Appendix D recapitulates the details of the proposed framework. The study therefore supports the need to develop maritime cyber security and improve upon training of personnel on maritime cyber security. Furthermore, the study tends to agree with other literatures on human element being the weakest link in maritime cyber security.

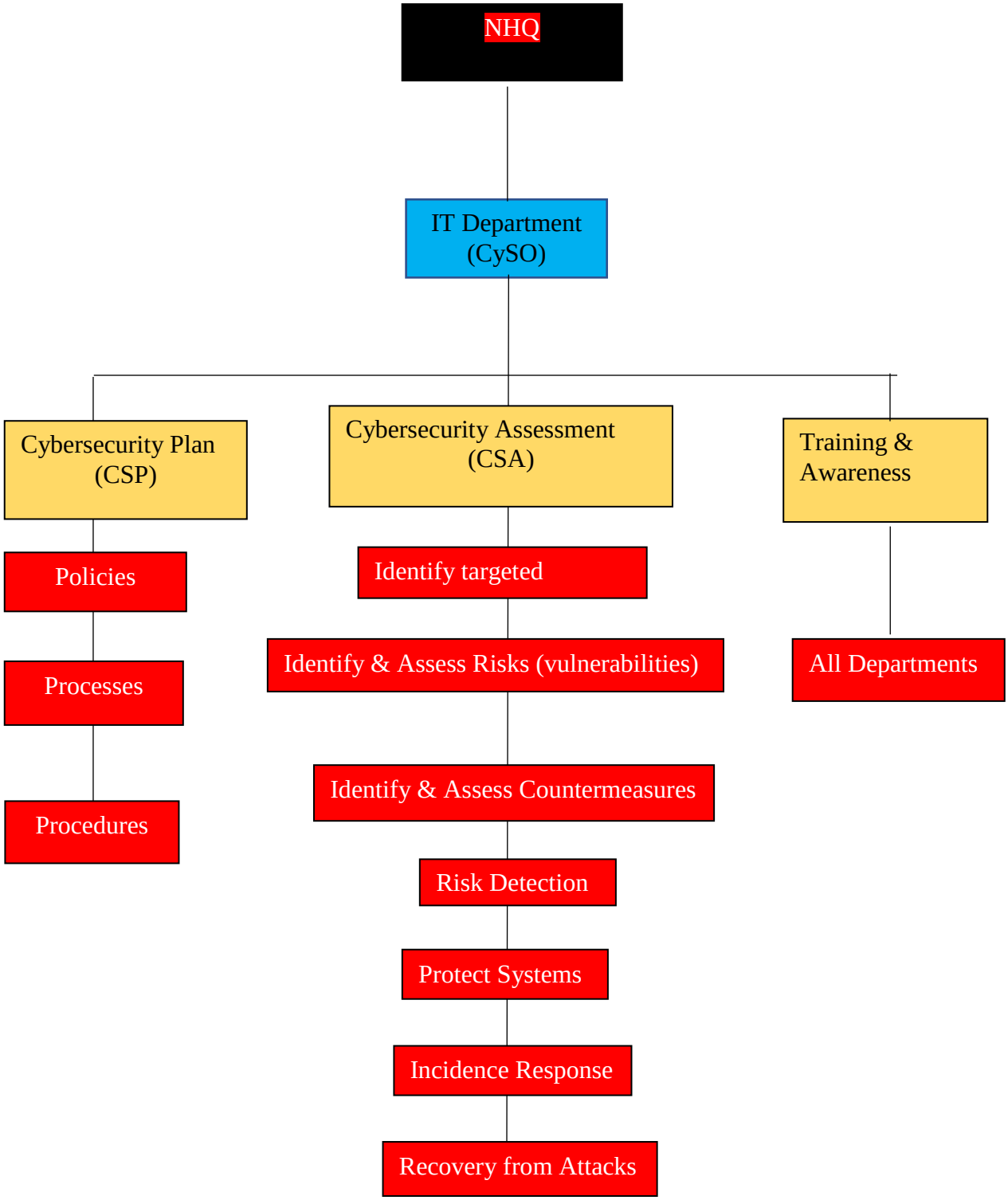


Figure 14. Proposed maritime cyber security framework structure.
Source (Created by Author)

5.2 Recommendations

Following the key analysis and subsequent discussions made, the recommendations can be expressed as a systematic approach and grouped into 3 main areas which could be integrated into the SMS of the navy (Dalaklis, 2017). The areas include Training, Equipment/Systems and Polices/Procedures.

5.2.1 Training

a. The Ghana Navy should design a maritime cyber security education and training and further incorporate this education and training in its training institutions to help raise the awareness of personnel on maritime cyber security.

b. The Ghana Navy should ensure that naval personnel receive the appropriate and adequate maritime cyber security skill and knowledge to man its integrated systems.

5.2.2 Policies/Procedures (Framework)

a. The navy should collaborate with other stakeholders like the Ghana Maritime Authority to come up with a robust framework on maritime cyber security in guiding its operations. Element of the NIST CSF and ISO 27001 should be factored when developing framework which will constitute among other things, the policies and procedures.

b. Since every framework has an output and input elements, the Ghana Navy should ensure that these outputs and inputs of the framework when developed are documented and frequently evaluated to serve as feedback mechanism for improvement.

5.2.3. Integrated Systems/ Equipment

The Ghana Navy should ensure integrated systems or ICT-based equipment are well secured through the use of softwares patches and up to date as well.

Additionally, the Navy should ensure that there are comprehensive recovery plans for the systems or equipment employed.

5.3. Limitations and future research

a. Out of the 116 respondents who showed their consent to participate in the survey, only 6 were female. Future researchers could increase the sample size and involve more or adequate female participation. This will go a long way to enable the researcher to draw comprehensive inferences on the level of awareness of maritime cyber security between males and females of the navy.

b. Lack of scholarly data on cyber attack incidents on navies in the GoG or Africa as a whole posed a limitation and hence delayed the researcher in gathering quality data for the literature review.

c. Furthermore, limitations were posed during the collection of data and responses from the questionnaire. It was observed that most of the personnel who initially had wanted to participate declined to participate because they were afraid of giving information regarding policies and procedures in connection to maritime cyber attacks, since they saw it as confidential and hence not willing to report.

d. Future researchers could investigate the type of maritime cyber security knowledge as well as skills training that the Navy could use to train personnel.

References

Abdalrahman, G. A., & Varol, H. (2019, June). Defending against cyber-attacks on the internet of things. In *2019 7th International Symposium on Digital Forensics and Security (ISDFS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ISDFS.2019.8757478

Abiodun, T. F., & Dahiru, M. Y. (2020). Maritime insecurity in the Gulf of Guinea (GoG) and the quest for security intelligence deployment in combating the menace. International Journal of Advanced Academic Research, 6(4), 79-99.

American Bureau of Shipping. (2016, February). Guidance Note on; The Application of Cybersecurity Principles to Marine and Offshore Operations. Volume 1. Retrieved from: https://safety4sea.com/wpcontent/uploads/2018/04/ABS-Cyber_Security-2016_02.pdf

Aboh, A. B., & Ahmed, N. (2018). Understanding West Africa Maritime Security Threats: A Critical Appraisal of the Development of Piracy and Armed Robbery at Sea in the Gulf of Guinea. *Socialscientia: Journal of Social Sciences and Humanities*, *3*(2).

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

Ani, U. D., He, H., & Tiwari, A. (2019). Human factor security: Evaluating the cybersecurity capacity of the industrial workforce. *Journal of Systems and Information Technology, Vol. 21 No. 1, pp. 2-35.* https://doi.org/10.1108/JSIT-02-2018-0028

Barnett, M. L., & Pekcan, C. H. (2017). The human element in shipping (pp. 1-10). Encyclopedia of Maritime and Offshore Engineering: Wiley Online.

Beseng, M., & Malcolm, J. A. (2021). Maritime security and the securitization of fisheries in the Gulf of Guinea: experiences from Cameroon. *Conflict, Security & Development*, *21*(5), 517-539.

Berg, H. P. (2013). Human factors and safety culture in maritime safety. TransNav, 7(3), 343-353. https://doi.org/10.12716/1001.07.03.04

BIMCO, CLIA, ICS, Intercargo, Intertanko, OCIMF and IUMI. (2017). Guidelines on Cyber Security onboard Ships. In: BIMCO (ed.) Version 2.0 ed. Bagsvaerd.

Blake, T. (2017). Hackers Took "Full Control" of Container Ship's Navigation Systems for 10 Hours. Retrieved from https://rntfnd.org/2017/11/25/hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-ihs-fairplay/

Boletsis, C., Halvorsrud, R., J B Pickering, S. P., & Surridge, M. (2021). Cybersecurity for SMEs: Introducing the human element into Socio-tehnical cybersecurity risk assessment. In Proceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications.

Broohm, D. A., Wang, G., & Gao, J. (2020). Maritime security: A new strategy for merchant shipping to avoid piracy in the Gulf of Guinea. *Open Journal of Social Sciences*, *8*(5), 392-410. https://doi.org/10.4236/jss.2020.85027

Bueger, C. (2015). What is maritime security? Marine Policy, 53, 159–164. https://doi.org/10.1016/j.marpol.2014.12.005

Bueger, C., & Edmunds, T. (2020). Blue crime: Conceptualising transnational organised crime at sea. *Marine Policy*, *119*, 104067.

Canepa, M., Ballini, F., Dalaklis, D., & Vakili, S. (2021). Assessing the effectiveness of cybersecurity training and raising awareness within the maritime domain. Paper presented at the *Proceedings of INTED2021 Conference*, (Vol.8, p. 9th). https://doi.org/ 10.21125/inted.2021.0726

Chapsos, I. (2016). Is Maritime Security a Traditional Security Challenge? In *Exploring the Security Landscape: Non-Traditional Security Challenges* (pp. 59-78). Springer, Cham.

Cochran, W. G. (1977). Sampling techniques. John Wiley & Sons.

Creswell, J. W. (2014). *A Concise Introduction to Mixed Methods Research*. SAGE publications. https://doi.org/60361063

Cronje J and Martin G. (2021). Experts warn of increasing cyber security threats for the African maritime industry. https://www.defenceweb.co.za/featured/experts-warn-of-increasing-cyber-security-threats-for-the-african-maritime-industry/

Dalaklis, D. & Maximo, M. (2022). International Agenda in Maritime Security. Project- Building National Maritime Security Policy. http://dx.doi.org/10.13140/RG.2.2.18948.60802

Dalaklis, D., Nikitakos, N., & Yaacob, R. (2021). Cyber security training strategy: dealing with maritime SCADA risks. http://dx.doi.org/10.21677/imla2021.05

Dalaklis, D. (2018). Exploring the issue of technology trends in the "Era of digitalization". In Proceedings of the World Maritime Day Parallel Event, Szczecin, Poland. https://doi.org/10.13140/RG.2.2.18767.79524

Dalaklis, D. (2019). Technology Deployment in Maritime Security: Emerging Issues. https://doi.org/10.13140/RG.2.2.27723.13605

Douglas, M. (2015). "Sources of Data". Retrieved from http://www.onlineetymologydictionary/data.Retrieved: 06 February 2022.

El-Bably, A. Y. (2021). Overview of the Impact of Human Error on Cybersecurity based on ISO/IEC 27001 Information Security Management. *Journal of Information Security and Cybercrimes Research*, *4*(1), 95-102. https://doi.org/10.26735/WLPW6121

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. https://eprints.lancs.ac.uk/id/eprint/72696

Ghosh, B. N. (1992). *Scientific Methods and Social Research*, Sterling Publishers Pvt. Ltd: New Delhi. https://www.worldcat.org/title/scientific-method-and-social-research/oclc/32113364

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity*, *6*(1), tyaa005. https://doi.org/10.1093/cybsec/tyaa005

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

Hasan, S. M., & Hassan, D. (2016). Current arrangements to combat piracy in the Gulf of Guinea Region: an evaluation. *J. Mar. L. & Com.*, *47*, 171.

Haque, A. B., Bhushan, B., & Dhiman, G. (2022). Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. *Expert Systems*, *39*(5), e12753.

Heering, D., Maennel, O. M., & Venables, A. N. (2021). Shortcomings in cybersecurity education for seafarers. In *Developments in Maritime Technology and Engineering* (pp. 49-61). CRC Press. https://doi.org/10.1201/9781003216582-6

IHS Markit. (2020). Safety at sea and BIMCO cyber security white paper. Retrieved from https://ihsmarkit.com/Info/0819/cyber-security-survey.html

Johnson, R. B., & Christensen, L. (2019). *Educational research: Quantitative, qualitative, and mixed approaches*. SAGE. https://www.vitalsource.com/products/educational-research-r-burke-johnson-larry-v9781544337821

Karamperidis, S., Kapalidis, C., & Watson, T. (2021). Maritime Cyber Security: A Global Challenge Tackled through Distinct Regional Approaches. *Journal of Marine Science and Engineering*, *9*(12), 1323. https://doi.org/10.3390/jmse9121323

Kessler, G. C., & Shepard, S. D. (2022). Maritime Cybersecurity-A Guide for Leaders and Managers (ed.). *Amazon. Distance to cyber risks. The reliable cyber-physical systems. Trust in others for cyber-defence*.

Kim, S. K. (2019). isps Code and Port & Cargo Container Security. In *Global Maritime Safety & Security Issues and East Asia* (pp. 196-227). Brill Nijhoff.

Kothari, C. (2004). *Research Methodology: Methods and Techniques (Second Revised Edion).* New Delhi: New Age International (P) Ltd. https://www.scirp.org/(S(lz5mqp453edsnp55rrgjct55))/reference/ReferencesPapers.aspx?ReferenceID=1285422

Konrad, R. A., Trapp, A. C., Palmbach, T. M., & Blom, J. S. (2017). Overcoming human trafficking via operations research and analytics: Opportunities for methods, models, and applications. *European Journal of Operational Research*, *259*(2), 733-745.

Lee, Y., Park, S., Lee, W., & Kang, J. (2017). Improving cyber security awareness in maritime transport: A way forward. *41*(8), 738-745. https://doi.org/10.5916/jkosme.2017.41.8.738

Mc Mahon, C. (2020). In defence of the human factor. *Frontiers in Psychology*, *11*, 1390. https://doi.org/10.3389/fpsyg.2020.01390

Meland, P. H., Bernsmed, K., Wille, E., Rødseth, Ø. J., & Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 15. https://doi.org/10.12716/1001.15.03.04

Meshkat, L., Miller, R. L., Hillsgrove, C., & King, J. (2020). Behavior modeling for cybersecurity. In Proceedings of the 2020 Annual Reliability and Maintainability Symposium.

Okonkwo, T. (2017). Maritime Boundaries Delimitation and Dispute Resolution in Africa. *Beijing Law Review, 8*, 55-78. https://doi.org 10.4236/blr.2017.81005

Okafor-Yarwood, I., & Belhabib, D. (2020). The duplicity of the European Union Common Fisheries Policy in third countries: Evidence from the Gulf of Guinea. *Ocean & Coastal Management*, *184*, 104953.

Pieterse, H. (2021). The cyber threat landscape in South Africa: A 10-year review. *The African Journal of Information and Communication*, *28*, 1-21. https://doi.org/10.23962/10539/32213

Progoulakis, I., Nikitakos, N., Dalaklis, D., & Yaacob, R. (2022). Cyber-physical security for ports infrastructure. Retrieved from https://commons.wmu.se/cgi/viewcontent.cgi?article=1008&context=lib_papers

Richardson, M. D., Lemoine, P. A., Stephens, W. E., & Waller, R. E. (2020). Planning for cyber security in schools: The human factor. *Educational Planning*, *27*(2), 23-39. https://files.eric.ed.gov/fulltext/EJ1252710.pdf

Safa, N. S., & Maple, C. (2016). Human errors in the information security realm and how to fix them. Computer Fraud and Security. https://doi.org/10.1016/S1361-3723(16)30073-2

Sanchez-Gonzalez, P. L., Díaz-Gutiérrez, D., Leo, T. J., & Núñez-Rivas, L. R. (2019). Toward digitalization of maritime transport? Sensors, 19(4), 926. https://doi.org/10.3390/s19040926

Siebels, D. I. R. K. (2020). Maritime Security in East and West Africa (Vol. 13). Springer International Publishing.

Tam, K., & Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, *18*(1), 129-163. https://doi.org/10.1007/s13437-019-00162-2

Tam, K., & Jones, K. D. (2018). Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping. *Journal of Cyber Policy*, *3*(2), 147-164. https://doi.org/10.1080/23738871.2018.1513053

Ukeje, C. (2015). The Abuja Declaration and the challenge of implementing a maritime security strategy in the Gulf of Guinea and the South Atlantic. *Journal of the Indian Ocean Region*, *11*(2), 220-235.

Verizon. (2021). 2021 data breach investigations report. Retrieved from https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2021- dbir-executive-brief.pdf

Zhang, X., & Ghorbani, A. A. (2021). Human factors in cybersecurity: Issues and challenges in big data. *Research Anthology on Privatizing and Securing Data*, 1695-1725. https://doi.org/10.4018/978-1-7998-8954-0.ch082

APPENDICES

Appendix 1

Survey Questionnaire

CONSENT FORM

Dear Participant,

Thank you for agreeing to participate in this research survey, which is carried out in connection with a Dissertation that will be written by the researcher, in partial fulfilment of the requirements for the degree of Master of Science in Maritime at the World Maritime University in Malmo, Sweden. The topic of the Dissertation is ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA.

The information provided by you in this survey will be used for research purposes and the results will form part of a dissertation, which will later be published online in WMU's digital repository (maritime commons) subject to final approval of the University and made available to the public. Your personal information will not be published. You may withdraw from the research at any time, and your personal data will be immediately deleted.

Anonymised research data will be archived on a secure virtual drive linked to a World Maritime University email address. All the data will be deleted as soon as the degree is awarded.

Your participation in the survey is highly appreciated.

Student's name	Kwadwo Forson-Adaboh
Specialization	Maritime Safety and Environmental Administration

Email address w2005014@wmu.se

I consent to my personal data, as outlined above, being used for this study. I understand that all personal data relating to participants is held and processed in the strictest confidence, and will be deleted at the end of the researcher's enrolment.

Name: ……

Signature: ……

Date: ……

Dear Participant

This survey questionnaire guide is developed to help the researcher gather data on ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA.

This research aims to assess the level of awareness of maritime cyber security in navies of the GoG countries and how prepared they are to handle cyberattacks, with a focus on the Ghana Navy.

The research is part of the requirement for the Master of Science in Maritime Affairs degree award, with a specialization in Maritime Safety and Environmental Administration. This survey questionnaire would take not more than 30 minutes of your time.

The information you will provide in this form is for academic purposes only and will therefore be treated with maximum confidentiality. The research data will be disposed of upon completion of the dissertation. Your participation is very much appreciated and will form part of the success and realization of the study.

Please should you have any inquiries on the aforementioned, kindly contact me via email at w2005014@wmu.se or via WhatsApp number +233243247276. Further,

be assured that your responses would be in compliance with the Data Privacy Act 2012.

Thank you for your attention, and I will be looking forward to your responses to the questionnaire. Kindly provide the responses where appropriate, tick or write.

Section A: Demographics

1. Age. ☐ 18 – 30 years ☐ 31 – 40 years ☐ above 40 years

2. Gender. ☐ Male ☐ Female

Unit: _____

Department: _____

3. Level of education.

☐ Masters

☐ First Degree

☐ HND

☐ SSS/SHS

☐ Others (Please Specify) _____

Section B: Assessing maritime cyber security awareness

4. Which of the following do you consider a threat to Ghana's maritime security?

	Very Low	1	2	3	4	5	Extremely
Drug Trafficking		☐	☐	☐	☐	☐	

Maritime Cyber attacks		☐	☐	☐	☐	☐	
Human Trafficking		☐	☐	☐	☐	☐	
Piracy		☐	☐	☐	☐	☐	
Smuggling		☐	☐	☐	☐	☐	
Armed Robbery		☐	☐	☐	☐	☐	
IUU fishing		☐	☐	☐	☐	☐	

Other (Please specify)

5. In your view, how would you rate the level of technology employed in the Ghana Navy with respect to Ghana's maritime security?

	1	2	3	4	5	
Very Low	☐	☐	☐	☐	☐	Extremely

6. How would you rate the threat of maritime cyber attacks in the Ghana Navy?

	1	2	3	4	5	
Very Low	☐	☐	☐	☐	☐	Extremely

Briefly explain your reason for the above selection. (Minimum of 50 words)

7. a. List any type of cyber attacks you know and rank them in a priority.

b. Which of the following types of cyber attacks in your view do you think the navy is likely to be vulnerable to?

Malware	☐
Phishing	☐
Man-in-Middle	☐
DoS & DDoS	☐

c. Are there any other cyber attacks not specified above? Kindly name them.

8. Have you or your unit been exposed to any form of cyber attack before?

☐ Not sure ☐ No ☐ Yes

If Yes, how many times and briefly describe the incident. (Minimum 50 words)

9. Have you heard of the term maritime cyber security?

☐ Not sure ☐ No ☐ Yes

If Yes, in your view, what does the term maritime cyber security mean?

10. How important is maritime cyber security to your daily job and activities? (Minimum 50 words)

11. Does the navy have available educational training regarding maritime cyber security and cyber best practices?

☐ Not sure ☐ No ☐ Yes

If Yes, describe the nature of the course. (Minimum 50 words)

12. a. Have you undergone any official training on maritime cyber security as naval personnel or operator?

☐ Not sure ☐ No ☐ Yes

b. If Yes, how many times?

c. If Yes, what was the duration of the training given?

13. Do you think you need further training on maritime cyber security

☐Not sure ☐ No ☐ Yes

Section C: Assessing Standard Operating Procedures

14. a. How often are the softwares in your unit updated?

	1	2	3	4	5	
Rarely	☐	☐	☐	☐	☐	Frequently

b. How often do you go online with the department's computers/systems?

	1	2	3	4	5	
Rarely	☐	☐	☐	☐	☐	Frequently

c. How often are you allowed to connect your personnel devices to the unit's computers/systems?

	1	2	3	4	5	
Rarely	☐	☐	☐	☐	☐	Frequently

Section D: Preparedness of the navy against cyber attacks.

15. When was the last time your department/platform carried out a cyber security assessment?

☐Not sure ☐No idea ☐Once a month
☐ More than once a month

16. Does the navy have any preventative measures established regarding maritime cyber Security?

☐ Not sure ☐ No ☐Yes

17. Are there any swift measures established by the navy in terms of recovery of systems should there be any maritime cyber attack.

☐ Not sure ☐ No ☐Yes

18. Is there any additional information you would like to share in relation to maritime cyber security?

Appendix 2

Personal Interview Guide

CONSENT FORM

Dear Participant,

Thank you for agreeing to participate in this interview, which is carried out in connection with a dissertation which will be written by the researcher, in partial fulfilment of the requirements for the degree of Master of Science in Maritime at the World Maritime University in Malmo, Sweden.

The topic of the dissertation is ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA.

The information provided by you in this interview will be used for research purposes and the results will form part of a dissertation, which will later be published online in WMU's digital repository (maritime commons) subject to final approval of the University and made available to the public. Your personal information will not be published. You may withdraw from the research at any time, and your personal data will be immediately deleted.

Anonymised research data will be archived on a secure virtual drive linked to a World Maritime University email address. All the data will be deleted as soon as the degree is awarded.

Your participation in the interview is highly appreciated.

Student's name	Kwadwo Forson-Adaboh
Specialization	Maritime Safety and Environmental Administration
Email address	w2005014@wmu.se

I consent to my personal data, as outlined above, being used for this study. I understand that all personal data relating to participants is held and processed in the strictest confidence, and will be deleted at the end of the researcher's enrolment.

Name: ……

Signature: ……

Date: ……

Dear Participant,

This interview guide is developed to assist the researcher to gather data on ASSESSING MARITIME CYBER SECURITY AWARENESS IN NAVIES OF THE GULF OF GUINEA COUNTRIES: A CASE STUDY OF GHANA.

The research aims to determine the level of awareness of maritime cyber security in navies of the GoG countries and how prepared they are to handle cyberattacks, with a focus on the Ghana Navy. It forms part of the requirement for the Master of Science in Maritime Affairs degree award, with a specialization in Maritime Safety and Environmental Administration.

This interview aims to determine how to establish an effective maritime cyber security regulatory framework for guiding the operations of the Ghana Navy. Your responses will be treated with utmost confidentiality and will be used only for academic purposes. Your participation is highly appreciated.

Name (optional): _____

Organization / Unit: _____

Position: _____

Number of years in position: _____

This interview will be centered around the following questions:

1. How important is maritime cyber security to the operations of navies in general?
2. What are some of the weak links with respect to maritime cyber security governance/management?
3. Is it necessary for navies to establish a regulatory framework for addressing maritime cyber security issues? Does the Ghana Navy have any maritime cyber security framework and what are its basic principles?

4. What are your views on what an optimal framework would look like? or What would its essential components look like?

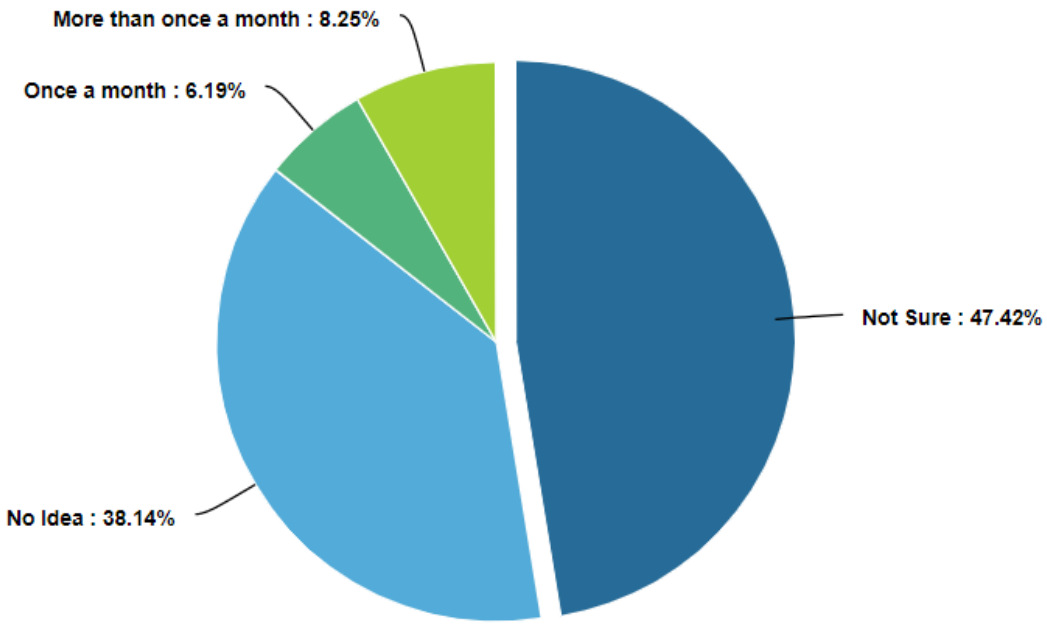
5. How should an effective regulatory framework be established in the governance/management of maritime cyber security?

Thank you!

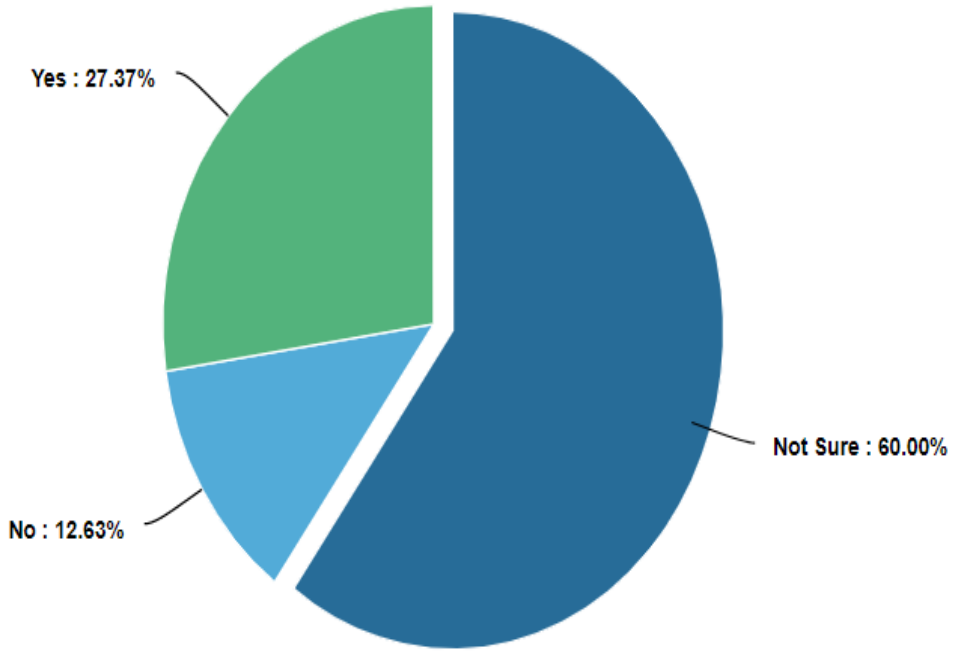
Appendix 3

Preparation of the navy against maritime cyber attacks

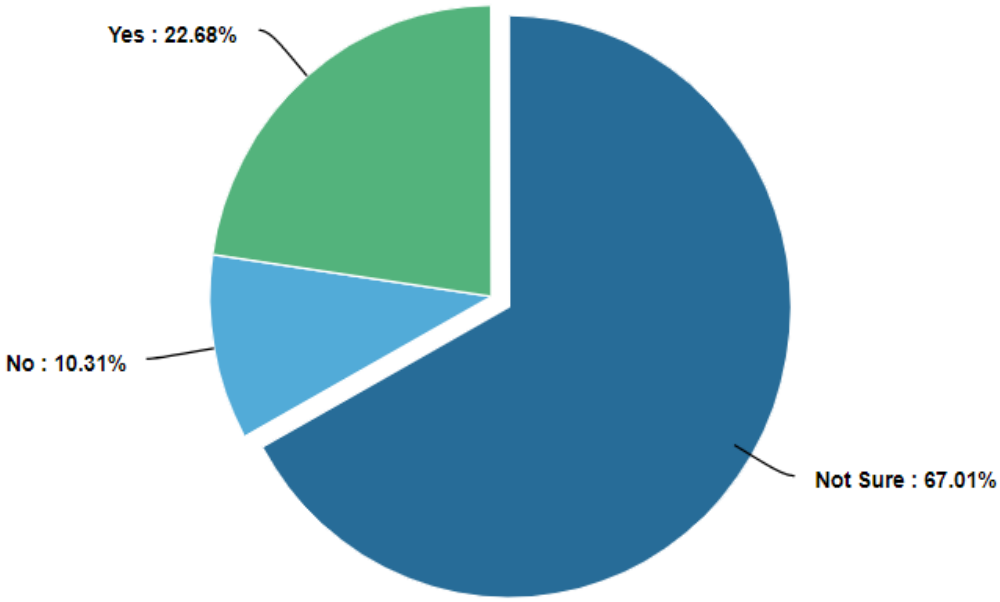
How often does your unit/department carry out maritime cyber security assessments?



Does the navy have any preventive measures established regarding maritime cyber security?



Are there any swift measures established by the navy in terms of recovery of systems should there be any maritime cyber attack?



Appendix 4

Appendix 5

T-Test

[DataSet1]

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
PNMC	116	5.3534	2.19586	.20388

One-Sample Test

Test Value = 3.5

	t	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
					Lower	Upper
PNMC	9.091	115	.000	1.85345	1.4496	2.2573