A MODEL ON THE ROLE OF TECHNOLOGY IN MARITIME SECURITY

by

Sudeeptho Ghosh

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfillment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

JANUARY, 2025

A MODEL ON THE ROLE OF TECHNOLOGY IN MARITIME SECURITY

by

Sudeeptho Ghosh

Supervised by

DR. BARUNAVA BANERJEE

APPROVED BY  Dr. Olesya Meskina

Dissertation chair

RECEIVED/APPROVED BY:

Admissions Director

Acknowledgements

My guide, Dr. Barunava Banerjee has been instrumental in shaping the direction of this research. I'm grateful for his precise inputs and critical course corrections which were vital in delivering a comprehensive and thorough research paper. My seniors Deputy Inspector General Manish Bahl, Deputy Inspector General Himanshu Nautiyal, Deputy Inspector General AK Satapathy, Commandant SN Samale, Commandant Kunal Kumar, Comdt (JG) Vikas Dhanker, Comdt (JG) Mandeep Singh, Comdt (JG) Awikshit Ghildiyal have enriched the dissertation with valuable inputs from their Headquarters and on field experience. They have been a perennial source of peer learning and brainstorming which helped me address many gaps regarding the various maritime security technologies available.

I would especially like to thank Comdt (JG) Anil Yadav and Comdt (JG) Naresh Kumar who are presently posted at United States Army Command and General Staff College, Fort Leavenworth and Defence Service Staff College, Wellignton respectively for helping me gather the data required for analysing the Impact of Technology in Maritime Security. I am thankful to the staff of Naval War College, for being supportive during the entire course of NSTMC, with the support of the library and TRIM facility.

I thank my family for their support and finally, Indian Coast Guard for giving me an opportunity to undergo the Doctorate in Business Administration Course and pursue research in an area that is relevant and current.

ABSTRACT

A MODEL ON THE ROLE OF TECHNOLOGY IN MARITIME SECURITY

Sudeeptho Ghosh
2025

A wide variety of goods, including raw materials, completed goods, and bulk materials, can be efficiently and affordably transported via maritime routes. In response to the shift in economic power brought about by "Globalisation" and the proliferation of trade-friendly policies, the shipping sector has been providing first-rate services to customers all over the world. The overarching goal of this research is to assess the maritime industry's susceptibility to maritime crimes, including piracy, armed robbery against ships, and maritime terrorism, by reviewing relevant legal instruments and conducting an internal evaluation. The approach applied in this research entails qualitative and quantitative data by interviewing the main maritime stakeholders such as the administrative officers, law enforcement, and the shipping companies, and using surveys and statistical testing. Questionnaires were administered to a diverse sample of maritime stakeholders: foreign navies, coast guards, and shipping companies, so as to achieve a cross-sectional view of the status of maritime security worldwide. According to the findings, all the participants agree that more should be done to improve maritime security and measures, but they are divided regarding International Maritime Organization (IMO) norms and standards. Certain areas face considerable problems in exchanging information, including data about security threats and the results of the analysis, in real-time, which is important for a timely reaction. Furthermore, measures like the “Ship Security Alarm System” (SSAS), “Automatic Identification System” (AIS) and “Vessel Traffic System” (VTS), although useful in effectiveness, are reduced by the differences in the development of facilities and training between regions thus, leading to inconsistency

in the measure taken. The study concludes that a contextually adaptive approach to maritime security, one that considers regional capabilities and specific threat levels, is essential for improving global maritime safety. Rather than a one-size-fits-all solution, the research suggests region-specific adaptations to IMO standards and improved coordination between administrative, enforcement, and operational stakeholders. This work is useful for policymakers and maritime agencies trying to improve their security measures and creates a basis for subsequent academic research on regional and technological developments of maritime security.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

Abbreviations	**Full Form**
IMO	International Maritime Organization
IOR	Indian Ocean Region
SSAS	Ship Security Alarm System
AIS	Automatic Identification System
VTS	Vessel Traffic System
MTSA	Marine Transportation Act
MARPOL 73/78	International Convention for Prevention of Pollution from ships, 1973. Modified in 1978
CSI	Container Security Initiative
C-TPAT	Customs and Trade Partnership Against Terrorism
OSC	Operation Safe Commerce
AEO	Authorised Economic Operator
FAST	Free and Secure Trade
SAGAR	Security for Growth for All in Region
SOLAS	Safety of Life at Sea
STAR	Secure Trade in The APEC Region
SEP	Secured Export Partnership
NVIC	Navigation Vessel Inspection Circular
AI	Artificial Intelligence
DF	Domestic Ferries
ICT	Information and Communication Technologies
ISPS	International Shipping and Port Facility Security
IOT	Internet of Things
UAVs	Unmanned Aerial Vehicles

EU	European Union
UNSC	United Nations Security Council
LAC	Line of Actual Control
SUA	Suppression of Unlawful Acts
SMN	Safety of Maritime Navigation
BCN	Biological, Chemical, And Nuclear
US	United States
ASEAN	Association of Southeast Asian Nations
SSP	Senior Superintendent of Police
PFSP	Port Facility Security Plan
BD	Big Data
OECMs	Other Effective Area-Based Conservation Measures
BBNJ	Biodiversity Beyond National Jurisdiction
IEL	Indian Extractions Limited,
CS	Computer Science
INSS	Indian National Strategy for Standardization
MASS	Maritime Autonomous Surface Ships
GIS	Geographic Information System
AIS	Annual Information Statement
FSA	Formal Safety Assessment
IACS	Indian Association for The Cultivation of Science
MOR	Military Operational Research
UNCLOS	United Nations Convention on The Law of The Sea
AFL-VA-ISN	Adaptive Fuzzy Logic Assisted Vulnerability Analysis of Intelligent Ship Networks
SIS	Ship Information System's
CSG	Cybersecurity Governance

SCM	Supply Chain Management
DT	Digital Transformation
LIDAR	Light Detection and Ranging
VTSs	Vessel Traffic Systems
CISE	Common Information Sharing Environment
C2	Command and Control
ECDIS	Electronic Charts Display Information Systems
SDG	Sustainable Development Goals
ENC	Electronic Navigational Charts
VGI	Volunteer Geographic Information
WIO	Western Indian Ocean
OT	Operational Technology
BCS	Bio Cyber Security
GNSS	Global Navigation Satellite System
FGD	Focus Group Discussions
SA	Situational Awareness
MMS	Maritime Monitoring System
SDR	Software-Defined Radio
PKI	Public Key Infrastructure
MIDS	Mahindra Defense System Limited
EEZ	Exclusive Economic Zone
IONS	Indian Ocean Naval Symposium
NSP	Net Security Provider
UAVs	Unmanned Aerial Vehicles
IBM	International Business Machines
LRIT	Long-Range Identification and Tracking
VDR	Vessel Data Recorder

AMVER	Automated Mutual-Assistance Vessel Rescue System
JASREP	Japanese Ship Reporting System
INDSAR	Indian (Maritime) Search and Rescue Computerized Ship Reporting System
J2EE	Java 2 Platform Enterprise Edition

CHAPTER I:

INTRODUCTION

1.1 Shipping

Shipping means carriage of products and things from point A to point B. This can take place by means of road transportation, through waterways, and even airways. The term Maritime defines trade and commerce activities carried with a water background which means that movement of goods and people over the water. Maritime involves connection of one country to some another part of itself or any other country through sea route and globally which relates to navigation, shipping, and Marine engineering (Alsawalqa and Venter, 2022).

1.2 Importance of Shipping.

This industry has a subterranean and umpteen repercussion on everyday life of preponderance of people. The term Maritime is derived from a Latin word ‘maritimus’ pertaining to – ‘of the sea’. Whales and dolphins are Maritime animals. The terms nautical and maritime are like day and night; former means related to ships only, the latter covers both ships and other stuff related to oceans. Maritime industry is like meat and potatoes for global economy whose evacuation will bring international trade to a standstill. Besides transportation Maritime industry includes other secondary activities like ship building, repair and maintenance of ships, port operations and Marine engineering. The branch of maritime defense comprises a clamant arm of national military defense. Looking through the members of EU it caters defending the national territory and integrity including defense of another national Maritime(Borg, Attard and Mallia Vella De Fremeaux, 2023).

1.3 Maritime security.

The protection of vessels on both an intrinsic and extrinsic level is referred to as maritime security. The topics covered are global, and some noteworthy ones include: defense against robbery, piracy, and terrorism; illegal trafficking[i] of products and individuals; illegal fishing and protection against marine pollution. In light of the current gravity of maritime security issues, Prime Minister Narendra Modi convened a high-level, public meeting of the United Nations Security Council to explore potential solutions. Prime leader Narendar Modi was the first Indian prime leader to chair an open discussion hosted by the United Nations, and the activities were held by video conference. The 2021 debate conference was attended by several notable figures, including Russian President Vladimir Putin and US Secretary of State Antony Blinken (Kristensen and Korda, 2022).

It reset the centrality of maritime security that interpolates to guard the marine ecosystems, increase the economic growth and arrest human security. In addition to the world's oceans, maritime security includes domestic domains such as rivers, ports, territorial waterways, and regional seas. A leading-edge incident in which two crew members were killed in a satirical drone assault on an Israeli-controlled ship in the North Arabian Sea near Oman serves as an example of the meaning. Given that India has a roughly 7000-kilometer coastline, maritime security becomes even more crucial in this regard. Balakrishnan Nair et al. (2023) and physical lowery in the marine region have been eclipsed by technical browbeating as a result of technological growth. Transportation of people and products within India is mostly accomplished by maritime routes, as the Indian Ocean plays a significant role in the country's trade. As a result, protecting SLOC (Sea Lens of Communication) is a top priority in India in the twenty-first century.

1.4 Growing presence of China in IOR.

China in specific has over the recent past become a key player among the Indianger the South Asian region. Presently they are most considerably a security threat to the Indian interest. It has been done before and one of the events happened in 2019 when Chinese research vessel Shiyan 1 was sunk near Andaman and Nicobar Islands. Again on August, 2020 while there was tension escalation at the LAC at eastern Ladakh; another Chinese vessel Yuan Wang entered into the Indian Jackie zone of the Indian Ocean (H, 2020)

Speaking during a 2019 speech, the retired Chief of Indian Navy, Admiral Karambir Singh noted that the country needs to put a lot of emphasis and resources into its maritime security conceptualization and management in the area to address both traditional and modern challenges. In the light of above statement present project has been undertaken by the scholar. The researcher, who was formerly a member of the Indian Navy, is well-versed in the fact that India's foreign policy currently revolves upon maritime security. India is a country that does not care to meddle into people's issues unless when forced to. The SAGAR's vision was unveiled by Prime Minister Narendar Modi when he embarked on the Mauritius trip in 2015. Improving economic and security links between India and its naval neighbours while also assisting them in building their security capacity is the project's principal objective. Ajit Doval was the only one who could handle this inflow.

The main focus of this session was conversation over security in Indian Ocean Region. The vision of PM Narendar Modi has been elaborated by Indo Pacific oceans Fellow (2016) initiative that focuses on 7 pillars of maritime security, which have been illustrated in diagram underneath:

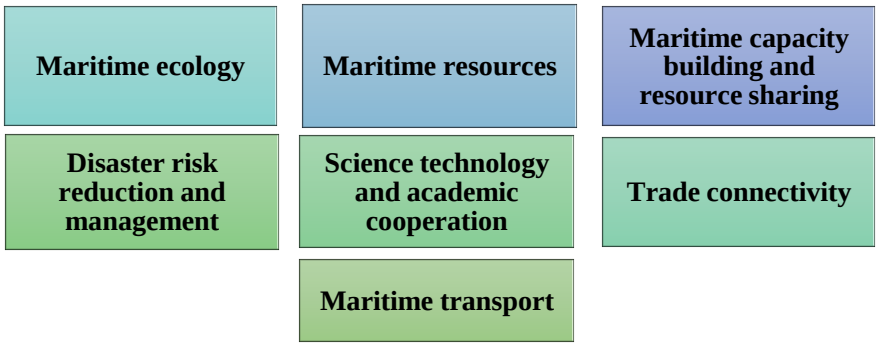


Figure 1.1: Seven pillars of Maritime security

1.5 Importance of Shipping Industry.

Since ancient times, shipping has been one of the most cost-effective modes of transportation, and it is currently the most popular one[ii](Mitsatsos, 2005). Shipping is one industry that has made globalization a reality (Boutilier, 2005). According to statistical data 90% of total world trade is on the shoulder of approximate 50,000 ships that are registered in 150 different countries and managed by around millions of officers(Chamberlain, 2008). Human intention to explore the uncharted waters of the world and reach new dimensions of success and trade have led to proficient shipping techniques and equipment's, state of the art ships and, Hi-Tech technology used in Maritime industry. All this has led to posthaste growth of maritime industry and it is going to aggrandize in future poring its share in the process of globalization[iii]. DeSimone (2008) The international character of shipping industry can be attributed to two factors - shipping holds the responsibility of carrying almost everything possibly that can be thought of, and this happens in supervision of crew that harbor this field from stem to stern of the globe[13]. But every boon has a tailed bane.

Maritime development has mushroomed associated perils like piracy, terrorism, and robbery; and many others which have been listed underneath:

(a) Piracy

(b) Stowaway

(c) Illegal Migration

(d) Narcotics

(e) Smuggling of Arms and Ammunition

(f) High-jacking

The scholar's questionnaire covers all these bases when it comes to marine dangers, and the project is built on the fundamentals of managing and preventing these major challenges and risks. While we do touch on other topics, the ones that get the most interest are maritime terrorism, armed robbery, and piracy.

1.6 Functions of international Maritime Organization.

IMO specifically has an important role of protecting the sea environment and its involvement in the issues regardin securing the maritime environment is equally important. In order to fight terrorism, piracy as well as marine crimes, the IMO has devised several measures such as coming up with the security measures for ships and the ISPS Code. It has also amended the SOLAS 74 and is responsible for the MARPOL 73/78 which is convention on the prevention of pollution of the sea by oil. Of course, the IMO has an anti-piracy program and encourages the ratification of the convention for the "Suppression of Unlawful Acts against the Safety of Maritime Navigation" (SUA) of 98.

1.7 After math of 9/11.

The humdrum of 9/11 that occurred in New York City in September 2011 raised a chill down the spine of the entire global community(Sklet, 2006). The security agency is tight-lipped as they had no reply and reaction about what had happened. The means and resources through which weapon and terrorist reached their destination was beyond imagination. The footprints of 9/11 reached the maritime sector also that persuaded the International Maritime Organization take following amendments:

(a) Assurance of secured shipping

(b) Making quintessential amelioration in chapter 11 of SOLAS by coalescing port facilities and shipping in control of maritime governance

(c) Approbation of ISPS code

- **Effective marine security management by shipping companies:**

The research scope is restricted to shipping businesses that operate commercial ships because the primary emphasis of this study is maritime security of merchant shipping. There are two types of marine security threats concerning the aforementioned companies: direct and indirect (Moseley, 2009). Examples of direct threats include terrorism, piracy, marine armed robbery, transnational organized crime, and illicit trafficking. Indirect dangers include things like corporate devices (such unlawful access to vessel identifying information) and biological, chemical, and nuclear (BCN) weapons. Since the majority of laws pertaining to shipping companies that aim to mitigate the aforementioned risks are of an international nature, the study's geographic scope is unrestricted by any territorial framework and includes businesses worldwide (SADOVAYA, 2015).

- **Risk-based and security models in ports and shipping:**

Numerous frameworks have been developed, either through the act of voluntary adoption or due to legislation, to enhance marine and port security after the September 2001 terrorist attacks and the increasing concern of international passenger and cargoes transport security. At higher stage at national levels a second level of security measures have been activated of which the most important one is supported by US. The Statutory and optional ISPS rules of the Marine Transportation Act (MTSA) of 2002 was among the first set of measures that the United States engaged on (DHS, 2003). To address specific marine activities, additional layered security systems were then developed. These

programs fall under this category: “Container Security Initiative” (CSI), “Customs and Trade Partnership against Terrorism” (C-TPAT), “Secure Freight Initiative” (SFA), Mega-port initiative, 24-hour Advanced Manifest Rule (referred to as the 24 hour rule) and Operation Safe Commerce (OSC). All these and many others were later incorporated into the United States Safe Port Act with only a slight modification of the 24 hours’ time limit. Other national policies are the 24-hour bans in Canada and Mexico, and the Swedish Stair-sec.

Additionally, the EC has taken action in accordance with Directive 2005/65/EC, which extends security from the ship-port interface to the extent of the port facility, Regulation 884/2005, which outlines the procedures for Commission inspections on maritime security, and EC Regulation 725/2004, which increases the security of ships and port facilities. Because of this, one of the programs that has to be thoroughly examined is the “Authorised Economic Operator” (AEO) program, which was incorporated into the EU Custom Security effort on January 1, 2008, and might be viewed as the EU's response to the US C-TAPAT program. Other regional initiatives include “US-Canada-Mexico Free and Secure Trade” (FAST) project, “Secure Trade in the APEC Region” (STAR) for the Asia Pacific, and the ASEAN/Japan Maritime Transport Security. To prevent transnational crimes like sabotage, tampering, and the smuggling of terrorists or items associated with terrorists during the transportation of commodities from New Zealand to the United States, a bilateral custom security agreement known as the Secured Export Partnership (SIP) was established.

Due to the complexity of the present marine security architecture, a large portion of the literature has concentrated on the ex-ante costs of compliance and the prescriptive specifics of the measures being implemented. Nevertheless, models for supply chain and physical security risk assessment and management have received little attention. Examine

how the current frameworks for risk assessment and management have been developed, implemented, and are applicable to port and marine security. We specifically look at how security-risk assessment is now done and show how supply chain security and physical security are related.

- **The Maritime Security Risk Approach of Today:**

The US Coast Guard's recommended security recommendations for facilities, "NAVIGATION VESSEL INSPECTION CIRCULAR" (NVIC) No. 11-02, are an excellent example of a system safety-based maritime security risk model. This circular provides a five-phase summary of the risk-based approach to security assessment and management.

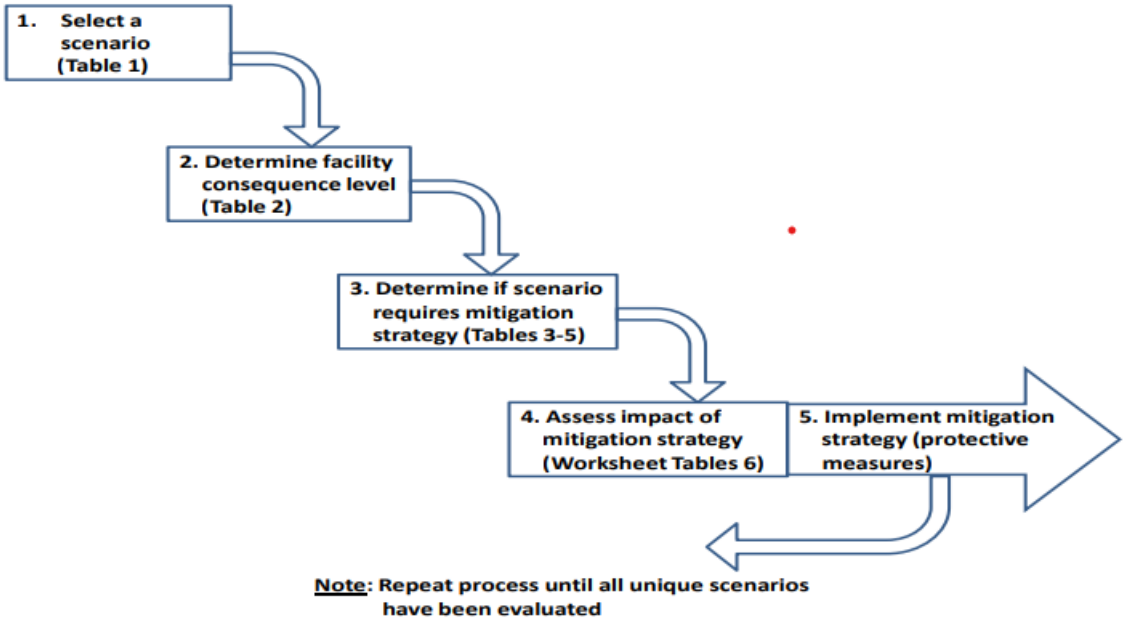


Figure 1.2: The NVIC risk assessment model

Step-1. The first step in the risk evaluation process is choosing an attack scenario, which examines potential threats to the vehicle (such as a ship or truck), cargo or passengers, a facility (such as a port), equipment, and/or operations (such as cargo handling). It also considers capability, opportunity, vulnerability, and consequences. Such

scenarios have to conform to those, which are being designed in the framework of the RS of MS for formal assessment, for example, to the ISPS Code for the SSP or the PFSP.

Step-2. The idea found in the security risk evaluation is to obtain the right level of significance for this type of activity that various assessments are based upon.

Step-3. refers to the evaluation of vulnerabilities using the following four criteria: The factors include; facility hardness, availability, accessibility, and organic security. The MARSEC levels based on ISPS provisions may be compared with the grading risk of NVIC scenario within the scope of ISPS Code.

Step-4. is concerned with risk minimisation. This may be accomplished by figuring out the scenario's position according to the consequence level and vulnerability assessment score, as indicated in table 4.

- **Artificial intelligence (AI) and Big Data (BD) in the marine sector:**

In almost all organisations, BD and AI are critical components of analytical and decision-making processes (Brouer, Karsten and Pisinger, 2016; Liang and Liu, 2018). Recently, a plethora of research has focused on the intersection of AI and BD. Nevertheless, there are academics who have noted that BD is often seen as a marketing ploy (d'Amore, Baggio and Valdani, 2015). Large volumes of data are often referred to as BD. Because of the recent increase in data volume, experts have been actively assessing new BD analysis methodologies (Franks, 2012). Today, the term "AI" incorporates a subset of these methods. In the beginning, AI research sought to simulate human decision-making by employing robots to process vast amounts of data. Ten years ago, AI couldn't have done everything that it can now. For instance, advanced AI systems have created autonomous ships, which have a lower mistake rate than ships handled by humans and can function independently without human intervention. Over time, AI is

starting to change the way the maritime industry does things. Research on BD and AI applications has so expanded substantially since 2012 (Liang and Liu, 2018).

Due to the lack of study on the use of BD in the marine industry, there is a knowledge vacuum despite the fact that both BD and AI have significant impacts on maritime business (Yang et al., 2019; Mirović et al., 2018). Marine operations with support of AI and BD has potential to improve financially and environmentally the industry (Sanchez-Gonzalez *et al.*, 2019) Further, it is indicated that approximately 80% of the total trade in the world takes place in the marine industry (UNCTAD., 2018) and the industry's size presents several difficulties (Brouer, Karsten and Pisinger, 2016) in addition to constantly changing regulatory requirements (Lee, Kwon and Ruan, 2019). Some of these issues are addressed by AI and BD at present and offer potentially practical solutions. For example, a ship owning company can electronically manage and control the operation of a particular vessels to improve the operation of the vessels with data on performances and navigation (Mirović, Miličević and Obradović, 2018). The industry produces a wealth of data that, if used wisely, may lower costs, lessen environmental effects, and improve maritime safety. As far as we are aware, only two review studies on BD and two on digitisation have been carried out in a maritime setting (Sanchez-Gonzalez et al., 2019; Fruth & Teuteberg, 2017). The examined investigations reported in this analysis are superior to previous reviews based on the quality and origin of the analysed research that employ AI and BD in the marine environment. For instance, Yang et al. (2019) zymarked literature that solely relies on data from automated identification systems (AIS). As opposed to the typical approach of the current study, (Mirović, Miličević and Obradović, 2018). probable did not select the literature methodically and which could have led to biassed outcomes. (Fruth and Teuteberg, 2017) and (Sanchez-Gonzalez *et al.*, 2019) Commonalities: Both used BD search for keywords

Digitalisation was targeted but Apple aimed at this while Google searched for it generally. While (Fruth and Teuteberg, 2017) omitted AI in the classification of marine sector; the literature identification process is largely unmapped and can hardly be replicated. However, the current study's methodology for conducting a literature search was distinct from that of the typical review studies in that it was transparent, dependable, and reproducible. This study reviews published publications on BD and AI in marine environments to determine what the field may entail and where its advances could go next. As a result, we outline four research goals. The first is to prove that the maritime sector is a legitimate area of research for BD and AI. The second step is to catalogue the publications, journals, papers, institutions, and writers that make up the academic community's cooperative writing network. The third is discovering and studying the underlying research clusters is the process of identifying the conceptual map of BD and AI research in the marine industry. The last goal is to determine and characterize the Field/ Area of Further Research (Munim *et al.*, 2020).

- **The Effects of AI Applications on Maritime Logistics:**

At the moment, AI has a significant place in both research and application. The technology known as AI enables computers to simulate human thought processes. It is possible to program computers to have extraordinary math, sorting, and searching abilities. However, there are a lot of things that computers cannot do, including speak our own language, think creatively, or decide what to do next. AI is unique in these respects; it looks for the algorithms that are required to satisfy these requirements (Millington, I., & Funge, 2009). Over time, AI has altered its ecological structure pattern. One of the well-known ways to solve social and corporate problems is now within reach, thanks to advancements in AI. Since organisations started using information technology in managing their processes, then the next phase to embrace is AI (AI). AI is being

increasingly required in many industries to assist with data-driven decision making. (Liang and Liu, 2018) This technique allows for the mining of large datasets for information, which can be useful for tasks like picture identification and anomaly detection. Due of the vast scope of network and planning issues, many traditional businesses, including the marine sector, rely more on intuition than statistics (Brouer, Karsten and Pisinger, 2017). Maritime logistics is one of the major sub sectors in the logistics sector. UNCTAD data suggest that in 2018, 11 plus million metric tonnes of dry and containerised bulk were shipped by sea, which the organization argues makes maritime transport "central to the global economy" (Sirimanne *et al.*, 2019). Therefore, acquisition and availability of reliable, efficient and faster means of transport is essential. At the same time, the expansion of the volume of data and further development of digitisation are now opening up new opportunities for the sector. With the use of ingenious information extraction techniques, data collected aboard ships may become available. Initially, AI research tended to use a lot of data to mimic human decision-making. AI can nowadays accomplish tasks which would earlier had been impossible to even imagine. Ships operated by AI, that is, ships that do not require human interference, have a lower error margin than manned ships. Such extensions can also be designed by highly advanced AI systems. Not only has AI persisted in permeating the marine industry, but it has also revolutionised the standard operating procedures. So, following 2012, a lot of studies were carried out on the topic of artificial intelligence and big data applications in the marine sector (Liang and Liu, 2018).

- **The Sustainable Ocean Governance Integrated Approach:**

In this context, Daniela Diz uses the ecosystem approach as an example of an integrated perspective to challenge the compartmentalised approach that underpins ocean governance and management in practice when addressing area-based management tools.

She notes that some of the area-based management tools like the marine protected areas and other OECMs may be regarded to be implementing the ecosystem approach due to their need for inter-sectoral cooperation. Diz looks at the legally binding provisions and measures of the 1992 Convention on Biological Diversity in terms of their application of biologically representative, linked area-based management systems. According to her, area-based management methods are essential for facilitating cross-sectoral implementation and guaranteeing equitable and successful management of ocean space.

From an integrated perspective, this article analyzed how the parent UNCLOS and the BBNJ Agreement relate to other sources of IEL. This research work is split into two parts. In Part I, the legal connection between the BBNJ and the CS regime beyond 200 nautical miles is first examined and runs until the end of the third INSS. The second part looks at the link between the proposed inclusion and application of the environmental impact assessment principle in the new draft text for the intended BBNJ Agreement and other area based management instruments and processes and other interrelated principles such as the strategic environment assessment (Borg, Attard and Mallia Vella De Fremeaux, 2023).

- **Ship personnel' effects on maritime safety:**

More than three quarters of the global trade occurs through ocean borne transport (For instance, European Union, 2009). The shipping industry is one of the most cutthroat in the world, with strict profit and efficiency standards, yet it is also one of the most multicultural and multilingual. (Hanzu-Pazara & Arsenie, 2010; Ljung, 2010) This has resulted in an increasingly international ship crew and a globalised labour market for sailors. For European and Japanese sailors, the shift in the labour market has been especially significant. They are accustomed to stable and controlled work environments, which are no longer the case (Lane, 1997). Today's crews are generally multicultural, and

language is an essential component of this (Silos *et al.*, 2012). Approximately 70–80% of the commercial fleet worldwide is made up of ethnic crews (Magramo, 2009; Pyne, 2005). Multiethnic crews, which may not share a common language, have raised concerns about the competency of ship personnel. There have been major shifts in ownership as a result of globalisation in the marine industry, which is driving expansion abroad. Ideally, this may also result in professional crews of all grades and countries receiving more structured training (Lane, 1999). Whether this is the case remains subject of controversy. Is there a greater exposure of a society and a greater differentiation of degrees and credentials for having more agents? Even on large carriers, major concerns become significant since technical progress has decreased the total number of personnel from 40 to 50 to 20 to 25 (Of *et al.*, 2013).

- **Improving marine safety: An in-depth analysis of the prospects and difficulties facing the domestic ferry industry:**

The role of the passenger ferry and the potential for economic activities have been discussed in the literature (Greig, M., & Ronald, 2005; Kotowska, 2015; Mendas, 2015), including how domestic ferries (DF) support modal transport and provide lifeline services to communities living in remote areas unconnected to any transport network (Kabran, E. G., & Eguavoen, 2019; Nurwahyudy, 2014). Despite a substantial decline in the international ferry sector due to the recent mayhem of the COVID-19 pandemic, the DF sector has proven resilient, ensuring sustainable operations(Baird, 2000). Hence, there has been supported continuous safe operations and boosted local tourism and other economic activities (Lee and Leung, 2022) Thus, coastal ferries are considered a well-organized mode of transportation in various social, economic, and environmental respects (Park *et al.*, 2018). Understanding the diverse operations of domestic ferries necessitates

a comprehensive view of the three primary ferry services outlined by Bruzzone (Bruzzone, 2012).

Among these, you can find three distinct kinds of ferry services: (a) water taxis, which are tiny boats that run on demand and go along predetermined routes over relatively small bodies of water; (b) passenger ferries- larger vessels, possessing more speed and passenger capacity than water taxis, that operate on a fixed route with a time-based schedule, and (c) automobile ferries- commonly known as ro-ro ferries, which transport passengers as well as vehicles, generally used on longer routes with fixed schedules. Moreover, ferry services are served in several ways, either through state-owned operations or via private stakeholder operators (Baird, 2012). Water-borne transportation is attaining significance as a viable solution to combat the escalating pollution and congestion challenges in cities, also seamlessly integrating into the multimodal transport network (Cheemakurthy and Garme, 2022).

There is an ongoing discussion regarding the extent to which prominence advancement in ship design, regulation, technology, and risk management systems have contributed to a 70 % drop in shipping accidents and losses over the past decade (Global., 2021). Nonetheless, DF accidents are not uncommon and can lead to a number of fatalities (Fenstad, Dahl and Kongsvik, 2016) and catastrophic consequences that can be overwhelming to society. The tragedies of Doña Paz (Philippines, 1987), Al Salam Boccaccio (Red Sea, 2001), Prince Ashika (Tonga, 2009), and Sewol (South Korea, 2014) have traumatized areas the world over, with massive socioeconomic impacts.

Despite covering shorter distances than other maritime transport industries, DF is more susceptible because of its intricate operations, limited capacity to handle crises, and poor infrastructure. Because of this, a single event might have disastrous results, highlighting the necessity for the DF sector to give sustainability and marine safety-first

priority. This situation underscores the need for sustainable and safety-oriented DF operations. “The International Maritime Organization” (IMO) is central to maritime safety IMO (2021), and the SOLAS regulations do not extend to ferries engaged in domestic voyages Consequently, these vessels are often referred to as non-SOLAS, or non-convention, vessels. Operating on domestic or inland routes, they are exempt from SOLAS compliance, presenting unique challenges, particularly in developing countries, where 97 % of known ferry fatalities occur in domestic operations. This contrast highlights the pressing need for concerted efforts to enhance maritime safety in the DF sector. While the IMO primarily focuses on international shipping safety, it recognizes the importance of extending its focus to non-convention vessels like domestic ferries.

The complexity of the DF operations means that the emphasis on the safety of these operations is even more important. Environmental conditions and traffic patterns put DF operations at risk, to begin with In addition, vessel scale and type used for DF operations differ quite significantly, making the safety environment even that much more challenging (Wisdom, T., & Kamanga, 2002). In some of the developing nations, such small boats lack proper registration or even distinctive names; thus, the loophole in regard to safety of vessels against accidents. Thus, it is essential to manage or escalate DF to international safety standards as a way of promoting safe maritime environment (Baig, Lagdami and Mejia Jr., 2024).

- **A Review of Cybersecurity Issues, Solutions, and Prospects for Maritime Autonomous Surface Ships.**

With the application of advanced technologies enabled by information processing technology, cybernetics, and navigation systems, MASS or Maritime Autonomous Surface Ships essentially constitute a revolution in the transport by sea (Kavallieratos, Diamantopoulou and Katsikas, 2020). These fully autonomous ships, thanks to their

complex self-sustainability, hold the key to revolutionizing classic marine activity due to their enhanced tender self-power that can be controllable through enhanced sensors and machine learning capacity (S. Aslam, M. P. Michaelides, 2020). When these technologies eventually reach the forefront of research and production, it will be crucial to comprehend their technical features and practical applications while also meeting new challenges like cyber threat protection, industry standard compliance, and regulatory compliance. Only then will they be able to adapt safely to the maritime environment (Hareide *et al.*, 2018). By making use of the MASS arrangement there are huge improvements in the realms of economies, operation efficiency, safety and security and all these improvements have the potentiality to transform the marine operations (Zarzuelo, Soeane and Bermúdez, 2020). However, to implement autonomous systems in the maritime sector, several other challenges come along, particularly in the areas of cybersecurity integrity, and regulation (Skjong *et al.*, 2016) its usefulness and the necessity of tackling new cybersecurity issues (S. Tan, J. M. Guerrero, P. Xie, R. Han, 2020). Research underlying the safe and long-term capacity of integrating autonomous vessels into the marine sector need to address security processes, measures, and viewpoints (Ali et al., 2021; Kumar et al., 2023).

Advancements in marines to bring digital electronics integration, significant uplift in operating facilities and environment with enhanced efficiency is the future of ship operating (Ali *et al.*, 2022). By replacing traditional sources, modern electric propulsion systems improve maneuverability while lowering carbon emissions and noise (Ali et al., 2023; Abbas et al., 2022). MASS can now make choices on its own, interpret data in real time, and perform predictive analysis due to the process simultaneous integration of complex sensors, “information and communication technologies” (ICT) and complicated control systems prompted by digitalization. (Farah *et al.*, 2022). In this research, the

interrelation between electrification and digitisation impacts on MASS, its operational consequences, technological advancements, and innovative application for smart marine transport are studied. With special emphasis made toward the close connection between electrification and digitisation, it is possible to gain a deep insight into the emergence of autonomous surface ships within the marine industry (Sadiq *et al.*, 2021).

Through commanding greater economic returns, lower impact on the environment and higher efficiency when it comes to marine propulsion, MASS company with power electronics propulsion systems is revolutionizing the industry. Kavallieratos et al. (2020) Electrification requires power electronics because they allow easy incorporation of renewable energy technologies and help to optimize energy conversions while enabling the movement of electricity in diverse forms. The increase in system stability and control, reduction in carbon emissions, and the enhancing flexibility effects of electrification are achieved by substituting electric propulsion systems controlled by state-of-art power electronics with conventional combustion engines (Sadiq *et al.*, 2021).

Focusing on the next step of the development of MASS as an electrified platform this work is expected to shed light on the scientific advancements, practical applications as well as initial environmental impacts of the marine industry's transition to sustainable and innovative approaches. To enhance its operating and navigation features and to introduce a shift from traditional processes to embrace technological advancement, MASS is at the moment in the process of transformation referred to as digitisation. This shows how some of the contemporary technology basics of MASS buildings such as GIS, navigation or AIS are integrated (Wang *et al.*, 2020). Focusing on the next step of the development of MASS as an electrified platform this work is expected to shed light on the scientific advancements, practical applications as well as initial environmental impacts of the marine industry's transition to sustainable and innovative approaches. To

enhance its operating and navigation features and to introduce a shift from traditional processes to embrace technological advancement, MASS is at the moment in the process of transformation referred to as digitisation. This shows how some of the contemporary technology basics of MASS buildings such as GIS, navigation or AIS are integrated (D. Bothur, Zheng and Valli, 2017). MASS is strategic in the intelligent and Technologically advanced marine vessel due to AIS GIS integration that enables accurate navigation and promotes automated decision making.

However, there are issues brought about by the Internet of Things' (IoT) and “information and communication technology's” (ICT) quick advancements, which must be carefully considered for MASS to continue developing (Kavallieratos et al., 2020; Qiao et al., 2021). Notwithstanding the advantages of ICT and IoT technologies in marine transportation, surface vessel autonomy has brought up a number of cybersecurity issues that require careful consideration. As a result, this study carefully investigates the complex cybersecurity problems related to MASS. Ships are more vulnerable to cyberattacks that jeopardise the security, functioning, stability, and integrity of their data as a result of their increased reliance on communication technologies.

The mass and the ships are in grave danger from a number of threats, including illegal access, data theft, and manipulations of the navigation system (Androjna *et al.*, 2020). This paper focuses on unpacking these vulnerabilities with an emphasis on the potential for attacker ingress points and their implications for MAJOR’s ability to operate in a secure and safe fashion. By identifying these cybersecurity weaknesses, the assessment contributes to the understanding of what it takes to build MASS’s immunity to a new breed of cyber threats (Tabish and Chaur-Luh, 2024).

- **Maritime Safety and Human Factors Management: A Review of Potential Dangers and Solutions for Ships' Engine Rooms**

Since more than 70 per cent value of global exchange and almost 80 per cent volume of world trade go through seas with supervision of seaport globally, maritime conveyance is vital in international trade as well as global affluence. This paper shows that the international maritime sector has a large impact on the global economy and its growth. Crews are central to operations of the shipments companies mainly involve in maintenance of ships and ensuring that the shipment is well done (Zhong and Meng, 2019). Sailing remains a crucial part of commerce, even though the profession is widely recognized as one of the risksiest in the world. Unquestionably, an effective measure to increase the chances of ships' safety and their crews is high qualifications of sailors.

The STCW organisation aims at minimizing"]); Grape marine accidents which are often as a result of negligence. Sailors are thus physically challenged, working in a physically demanding line of work in a high-risk environment to add to the fact that there are certain health risks inherent in the work that sailors undertake and which are not applicable to other forms of employment. They face multiple challenges to their state of mental health apart from physical pressure and psychological demands that crews are known to face at sea (Jepsen *et al.*, 2016).

They face difficult working circumstances while on board (Hjarnoe and Leppin, 2013). Long-term absences from home might have a negative impact on their health (Baygi *et al.*, 2017). Their lives and wellbeing are in peril in terms of what they come across every day like chemical products and sunshine not to mention what they put into their systems; cigarettes and some types of foods. Consequently, knowledge of these concerns can enhance the health and safety welfare within the marine industry of businesses and people going about their operations (Jensen *et al.*, 2006). However, sailing enjoys the reputation of one of the deadliest jobs since approximately 20% of work-

related accidents on the global level are associated with maritime activities and 1% results in death.

Approximately 4.7 times as many fatal accidents occurred in the shipping sector as in the construction sector, and 21 times as many workers died in these accidents (Roberts *et al.*, 2014). The exposure of seafarers to several dangerous conditions exists when operating the ship to execute its tasks and various activities including cargo, ballast, bunker, repair and maintenance, hot work, and enclosed space work which are usually carried out singly and at considerable distance from the shore (Ahn and Kurt, 2020). The number of marine accidents has not reduced significantly despite the conduct of rigorous inspections on ships and placing of detained or suspended ships out of operations (Cantarelli *et al.*, 2018). Accidents involving sliding, tripping, hitting or being struck by objects, falling on a board, or falling from a height are among the leading causes of injuries and fatalities in the industrial sector (Zhong and Meng, 2019). An accident often occurs due to an error or due to a failure of all protective measures, protection mechanisms or protection walls. The performance of adequate and effective corrective and preventative actions is required whereby shipping stakeholders will easily determine causes of accidents and prevent the reoccurrence of maritime disasters with an overall aim of enhancing the safety of maritime transportation (Roberts *et al.*, 2014). Of the 4104 accident incidences that were examined throughout the investigations, human activity was responsible for 65.8% of them, whilst system or equipment failure was responsible for 20% (Chowdhury *et al.*, 2024).

Ship security study using quantitative risk analysis to find efficient risk control solutions:

For earlier pirate incidents were closer to the SOMALIAN coast, the 2008 seizing of the 333-metre long tanker Sirius Star, at 400 miles offshore was unique (Kraska, J.,

Wilson, 2008). According to the BMP for protection against Somalia-based piracy which include attack on vessels in the "Arabian Sea", the "Northern Indian Ocean" and the "Gulf of Aden" affecting all the sub-sectors of shipping (BIMCO *et al.*, 2011). In order to combat piracy, the UN Security Council has urged for countries in charge of ports, flags, and coastal areas to support counter-piracy efforts off the Somali coast for both pirates and their victims (Kraska, J., Wilson, 2008). Furthermore, the Security Council has provided a number of decisions concerning piracy of ships, and these most important are numbers 1816, 1846 and 1851. These resolutions offer the international community unprecedented opportunity to address marine threats (Chalk, 2010).

The code development process started two months after the assaults, and the final release was just thirteen months later (Wengelin, 2012). The development process was characterised by the necessity of creating a defective product rather than nothing at all because of this short turnaround time (Mitropoulos, 2004). Consequently, this code recommends a far lower degree of ship security evaluation than, say, such probabilistic risk assessment for ship safety. The FSA ("Formal Safety Assessment for Ship and Risk-Based Ship Design"), SOLAS Regulation 17 (Alternative design and arrangement), and military threat assessment for navy ships are a few ship design domains that use advanced techniques and instruments for risk assessment. The imperfections and constraints of the code show that marine security requires more research and development in the future (Liwång, Ringsberg and Norsell, 2013).

- **Ship security management:**

Since the 1960's the IMO has created risk-based strategies. Probabilistic regulations in general and risk-based regulations in specific where first implemented in 1974 starting with SOLAS74 regulation of damage stability. In 1997, the IMO gave its nod for the Formal Safety Assessment which is a risk-based regulation mechanism

(Skjong, 2009). Therefore, even if quantitative risk-based methods have not yet been created for all areas of safety, they are well established in the marine safety field. Ship safety techniques are more advanced than ship security techniques. Following the terrorist assault on the cruise liner Achille Lauro in 1986, the IMO created and approved the first security protocols. However, only the United States, Canada, and the United Kingdom required these precautions. Accordingly, the ISPS code is the first rule that might have an impact on ship security initiatives, and the IMO has designated it as a first step in this regard (Mitropoulos, 2004). According to the IACS, the general industry standards and class criteria should be considered a minimal step to ensure a ship's safety and security.

The instruments utilised in the current study are shown in Figure 1 and are derived from military force protection, probability risk analysis, risk-based ship design, and military operational research (MOR). These tools are utilised to conduct the analysis and utilise the existing techniques to structurally display, analyse, and assess risk.

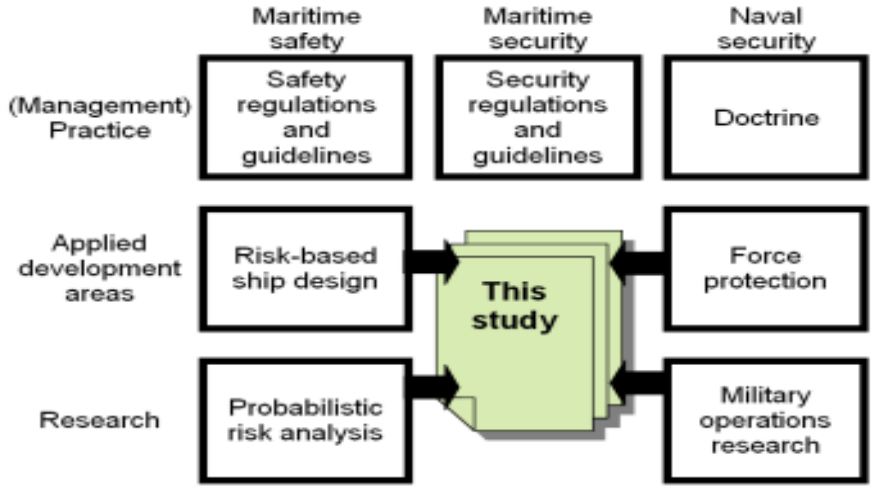


Figure 1.3: Ship Security Management

Figure 1.3 describes the analysis method for the study's methodological schematic. Based on research and development from related fields of maritime safety as

well as naval security we identify tools that may be suggested with regard to minimize potential subjectivity in management of maritime security, owing to a dearth of literature in the discussed area.

According to the research, risk is determined by the likelihood and impact of a danger. Simplified instances of this function are as follows:

risk = consequence × probability.

But in general, the analysis must be able to evaluate many consequence types, and the definition must then be tailored for that particular mix of consequences (Liwång, Ringsberg and Norsell, 2013).

1.8 Overview of the Research Problem.

Maritime security is protection of sea vessels of all kinds both on a domestic level and internationally, there are many threats like piracy terrorism trafficking of people and resources Ellis fishing pollution of water bodies etc. that are posing several problems and difficulties in the maritime industry. Shipping industry is one of the oldest kinds of and most common event today remember how India was discovered by Vasco da Gama while he was on a ship that old is the history of maritime indulgence. Preventive efforts to stop any illegal or immoral behaviour in the sea are part of maritime security, which also includes reactive measures to defend the maritime domain from threats both domestically and internationally as well as legal actions. Events such as the discovery of a Chinese marine vehicle in the Andaman and Nicobar Seas highlight how crucial maritime security is to India. This present work is an effort to find out the importance of maritime industry and the threats it is facing due to armed robbery a detailed explanation of these along with how technology can be used to combat this problem have been discussed in the dissertation. Technology is one thing which has helped to solve many problems in marketing of areas and how it can be fruitful for the maritime industry is the goal that the

project aims to achieve(Nik Nor Suhaida Ali, Anas Afandi Ahmad Apandi and Laila Suriya Ahmad Apandi, 2016a).

1.9 Research aim.

The dominant objective with which current study will be practiced is to investigate and optimize solutions that can lead to better Maritime security on grounds of current technologies available. Future recommendations of new technology that might bring in higher degree of security will also be attempted.

After taking a detailed look on the available technologies available in various countries that pertain to protect Maritime security this present study targets to examine current technologies open to Maritime industry and responsible for security of our country India. Also, evaluation of available solutions for optimizing current problems in hand and recommendation for future will be attempted in this study.

1.10 Research questions.

This dissertation takes a sincere attempt to improving current understanding of maritime security and technology's involvement in it. The dissertation will advance with the aid of a qualitative methodology. In order to collect opinions about the marine sector and various facets of maritime security, three sets of questionnaires will be created and sent to the following groups of people:

(a) Administrative officers that will include officials responsible for overall administration and legal aspects.

(b) Officers responsible for enforcing National Maritime legislation in their respective Maritime zones like - coast guard, Navy, Maritime security agency, Marine police etc.

(c) Cast and crew present at the ship that include ship masters, shipping organizations and companies, shipping associations etc.

CHAPTER II:

REVIEW OF LITERATURE

2.1 Introduction

This chapter is an overview of maritime security along with some definitions, fragility of sector and major obstacles like piracy/ robbery and waterborne terrorism. It also reveals remedial measures that are available in international instrument form to ascertain security of people and products.

2.2 An Overview and Definitions

General definitions of maritime security. It includes definitions and few literature reviews from related field:

a) States that many times security is all the measures combined together undertaken by owners and operators and involve port facilities and all related Marine organizations with the common objective to protect against any hostility with legitimate operations(Graham, 2014) .

b) Steven M. Jones (2006). Advocates that maritime security refers to the feeling where a shipping company or vessel feels safeguarded against any act of piracy/ terrorism or associated crime(Leach, 2011).

Shipping is one of the most economical and affordable means of transport of goods and high-time leisurely entertainment for people with big fat money. But has already stated that every virtuous possession has associated drawbacks; the same applies here. Maritime vessels and boats have been used for long for illegal transport of weapons, narcotics, illicit materials, terrorists as stowaways(Leach, 2011) etc. In one notorious case, Indian customs officials seized ballistic missiles at Kandla Port; in another, Italian customs officials seized about 8,000 assault rifles and automatic weapons packed into three shipping containers at the port of Gioia Tauro in 2004. Politicians and media

moguls use situations like this to their advantage because of the shipping industry's significant role in the commercial market (Kasperson *et al.*, 2003).

The major area of concern of this dissertation is armed robbery that occurs in waters of Indian Ocean and South East Asia. Literature review of a few recent research papers and documents has been briefed underneath to bring to limelight the seriousness of this situation.

2.3 Previous Studies

a) **Liss 2003.** A nerve-wrecking incidence occurred in maritime history in 1998 in southeast Asia. Ship named Cheung Son was attacked little beyond West coast of a Taiwan port by a Chinese custom vessel. The captain had no choice and had to allow-in intruders dressed in Chinese officers' uniform and armed with guns to control the vessel. Pirates made their blood run cold for 10 days after which all 23 Chinese crew members were bulldozed to death and their carcass was disposed of in water. The pirated vessel was later traded for 36,000 US dollar inside the premises of China. The second owner repeatedly sold the same vessel to a party from Singapore for 300,000 US dollars. The dead bodies were alarmed to Chinese police through a fisherman. The pirates repeatedly indulged in such behavior, and when they got arrested, one of them admitted in the court of law that they were directed that each gang member was to extirpate minimum 1 crew member(Liss, 2003).

b) **Treves (2009).** The cost of Somalia is much vulnerable to piracy attacks that has attracted the attention of Security Council of UN. Security Council resolution 1816 of 2000 and other similar have added more value to current narrow international law rules on piracy in a way which is kosher and permitted on high seas. The security council resolutions have been adopted to Somali transitional

government authorization and framed so that they are not considered as advocating customary law. One of the red-letter philosophy to adopt this fabric is to eschew bickering regarding Somali territorial sea. The captured individuals were given a very barbarous and diabolical treatment by the seizing states because usage of force against pirates has been approved as an exception to exclusive right of flag state (Treves, 2009). Present research was undertaken to advocate the safe keeping of all person involved.

c) **Nath (2023).** This research is related to "Palash Logistics" a famous third-party logistics company providing delivery solutions to a colossal online retail company in India. The paper opens consulting an external management consultant and his important role as a ray of light during the deep dark issues the company had to face at certain times(Nath, 2023). Although the success story relates more towards the management aspects of the company, yet it can be suggested that adoption of novel maritime techniques in the cargo ships will further add feathers of success to its cap.

d) **Captain Himadri Das (2021).** The research conducted reported increase in incidences of armed robbery in Asia where the number was around 100 in 2020. Talking particularly about India the ballgame of armed robbery was 5 in 2019 waxed to 9 in 2020. Nine of these incidents were documented in Indian states of Gujarat and Andhra Pradesh (Kakinada). Other areas considered as hotspots are Kochi, Haldia, and Visakhapatnam, and in 2020 Alang from Gujarat became the new hotspot. In three of the four cases reported from Gujarat, 17 mobsters were apprehended, and in one case, stolen property was recovered. The arrests were made by coast guards at sea in one plight while by Marine police in other two. The kleptomaniacs were valorous in one incident to board a tanker under tow

from an Indian fishing vessel. It was observed that armed robbery is related to monsoons and some cases reported in this season is least (only 1, Kakinada). The highest number of cases were reported in February 2020 (5) cases.

The enfeeblement in number of robbery cases was also attributed to Covid-19 related lockdown which continued from March till May 2020[1]. Whichever is closer—India's contiguous zone twenty-four nautical miles or the international maritime border line—determines the maritime boundaries of coastal seas (Jones, 2006) 30. The scope of armed robbery includes internal territory waters and its suppression would be a great step to enhance coastal security.

Shipping industry is a kind of ancient and economical form of transport, highly flexible and at the same time vulnerable in its approach. The latest fad in international relations is the term Maritime security which includes safeguarding all biotic and abiotic components present on board ship. Any ship in the open sea has to encounter domestic ships and foreign national ships. Thus there are many kinds of booby traps and clogs while ship is on sail. It has to overcome these to make sure that the people and the cargo reach their ultimate destination.

2.4 Major Threats in Maritime Security.

Maritime security major threats (Defence, 2020) include following-

a) **Piracy and armed robbery.** Pirates in form of groups and with wearing configurations having different kind of boats rob bigger ships and sailors
b) **Illegal trade.** Illegal trade of drugs/ firearms/ technology is very customary because of the drop back that all large containers that aboard a ship cannot be scrutinized.

[1] Das, Himadri. "Armed robbery at sea in India: Trends and Imperatives". 2021. www.maritimeindia.org

c) **Human trafficking.** Displacement of felonious evacuees and poaching of individuals across borders

d) **Environmental deterioration.** Inevitable accidents like tanker spills or blast of ship in any water body causes conspicuous environmental dilapidation

e) **Stowaways.** Clandestine movement of a person in a container without the knowledge of ship owner or master of vessel

f) **Container crime.** Carrying any furtive material including human trafficking inside the container from one place to another.

g) **Maritime terrorism.** Uses of armed revolution in sea for a dangerous and higher cause like using a ship as a floating bomb in the middle of ocean; meant to attack a passenger or merchant ship

h) **Cyber-attack.** Maritime operations are vulnerable to attack by hackers

i) **Anti- ship missiles.** These comprise long range and powerful weapons used by military and if they miss their target or hit the wrong target causes immense damage

j) **Water borne improvised explosive device.** Primary usage is targeting warships and merchant ships; incidences have occurred in Red sea and Gulf of Aden. It involves usage of speed boats containing individuals firing small arms(IRS, 2020).

k) **Sea mines.** They are used to procrastinate access to key ports. Despite of being well defined there have happened incidences when they can break free and drift into shipping lanes.

2.5 Need for Maritime Security2.

Maritime security is a quintessential aspect for each country and it is concerned with stopping piracy at sea to give a runaround to sub-rosa migration and weapon movement. In context of India the two important aspects of maritime security include:

a) **National security.** The 7000 km long coastline of India is well protected in the light of advanced technology and number of physical threats from International waters is much under control.

b) **Trade security**. The security of maritime channels is of paramount importance since the exchange of economically useful products has relied heavily on the transport lens of the Indian Ocean. The escalating Chinese influence in the Indian Ocean poses a serious danger, and the appearance of Chinese survey ships in Indian waters should not be disregarded.

c) **Indian Context**. Three tier system of Indian coastal security operates at three different levels of hierarchy which has been diagrammatically represented underneath:

Figure 2.1: Three tier system of coastal security of India

[2] https://www.stratfor.com/analysis/southeast-asias-treacherous-waters

2.6 Legal Framework.

Man is not stagnant, he is movable. He should move around for personal growth and otherwise and so should move things necessary for survival of man. Movement of man and goods through sea route is one of the ancient trade routes ever known. Now some fast shipping methods even include movement through the Airways. Both Airways and waterways have strict and constringent security checks, rules, and guidelines, that need to be followed while any cargo or individual travels through either of the route. Despite of everything being taken care of the 9/11 attack of 2001 was one of the most astonishing and overwhelming incidences in one of the super powers of the world US. While the maritime industry was still struggling with the issues of piracy this act of terrorism certainly lead to intensive re-thinking of fostering top-notch securities in the maritime(Beckman and Page, 2014) sector. As a result of a reorganization of the 1974 International Convention for "Safety of Life at Sea" (SOLAS), "International Ship and Port Facility Security" (ISPS) code was developed after "International Maritime Organization" (IMO) approved a maritime security instrument in 2002. Not only did 1982 “United Nations Convention on the Law of the Sea” (UNCLOS) handle these further revisions, but it also addressed “suppression of unlawful acts” against "safety of marine navigation" (SUA). (Ali and Sidhu, 2023)

The aforementioned organisations are divided into two branches: criminal law (UNCLOS and SUA) and regulatory law (SOLAS and ISPS). As shown in the diagram below:

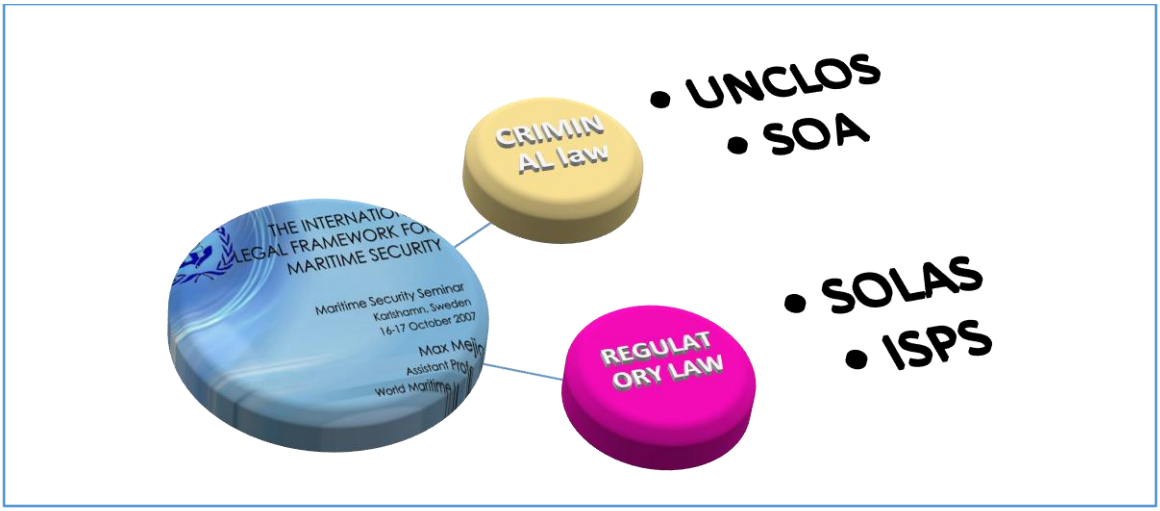


Figure 2.2: Two branches of law in the international legal framework for maritime security.

2.7 Importance of Technology in Enhancing Maritime Security

Lan *et al.* (2024) The imminent arrival of autonomous ships may pave the way for improvements in transportation efficiency, safety, security, and environmental impacts. Intelligent ship networks differ from traditional ships in that they can automatically recognize risks, make intelligent decisions, and have situational awareness. The increasing significance of marine information management and network security is a direct result of the fact that this area presents a threat to the stability of nations and societies as a whole owing to reasons like the variety and complexity of marine information types, the difficulties in collecting relevant data, and similar issues. This research presents "Adaptive Fuzzy Logic Assisted Vulnerability Analysis of Intelligent Ship Networks" (AFL-VA-ISN) for use in autonomous ships' information management and intrusion detection systems in a variety of scenario settings. To achieve this goal, it investigates ship systems and artificial intelligence technologies while also finding various vulnerabilities. The combination of artificial intelligence and fuzzy logic has resulted in a paradigm that intelligent ship networks can use to deal with imprecision and ambiguity in decision-making. To identify anomalies in risk data, One possible use of the

Ship Information System's collaborative control architecture is suggested in this paper. The main goal of this research is to ensure the security of networks used by intelligent ships. This was achieved by implanting nodes that could build self-execution protection organisations and by using multi-sensor nodes to analyse data, which included information about hostile attacks. In comparison to its predecessors, the proposed AFL-VA-ISN model outperforms in a number of critical measures, including data transmission rate (up 99.2%), attack detection rate (up 98.5%), risk assessment rate (up 97.5%), access control rate (up 96.3%), and network latency rate (up 11.4%).

Simola et al. (2024) Marine ecosystems and industries necessitate better, more unified cybersecurity regulations. In the marine industry, there is currently no standard cybersecurity method that can control the entire supply chain, even in crowded port areas and fairways. We need a more uniform approach to cyber threat prevention throughout Western port terminals and harbour areas. Cybersecurity for operational technology in the harbour region is understood to be rooted in more conventional knowledge of what is needed. The physical security service routines of randomly inspecting vehicles and people and performing customs functions on cargo and passenger transit are insufficient for ensuring the overall safety of the marine ecosystem. The traditional physical threats of yesteryear have evolved into hybrids. Hybrid attacks pose a distinct risk to everyday harbour activities, potentially causing long-lasting damage and jeopardising overall business continuity management efforts. Cyber danger elements in the maritime realm must be prevented at all costs. In terms of cyber security regulation, the study offers transnational and EU-level evaluations. Because of the importance of surveying member states' cyber security requirements, the results reveal where to focus and direct a maritime domain. This research is part of “cybersecurity governance” (CSG) of operational

technologies in smart energy networks research program in Finland. A standard model for operational technology cybersecurity governance is the goal of the project.

Koh et al. (2024) To survive and thrive in the face of the digital acceleration and disruptive technologies brought about by COVID-19, the marine crew must be trained and equipped with critical knowledge. Using the knowledge-based view and the "business logistic management framework," this study aimed to give a framework that would aid executives in maritime transport in identifying and ranking important knowledge domains and sub-domains both today and in the future. Digitalisation, personnel development, sustainability, marine business, and "supply chain management" (SCM) are the five domains and 23 sub-domains of knowledge that were formed after the study was reviewed. Using the approach of the fuzzy analytic hierarchy process, surveys were administered to shipping company management in Singapore. Based on the findings, the following information is crucial: digitalisation, maritime business, human development, sustainability, and supply chain management. In sum, the findings of this study have improved the competency and knowledge framework for executives in maritime shipping, aided studies examining the relationship between technology and knowledge management, and provided direction for educational initiatives.

Scarlat, Ioanid and Andrei (2023b) Marine ports are an integral link in the logistical network that includes the whole shipping industry and shipbuilding facilities, which are all undergoing an intricate "digital transformation" (DT). This study intends to outline the history of maritime transport and logistics as it relates to "information technology" (IT), identify the key features of each generation that has had an impact on these fields, and finally, suggest a future autonomous vessel port management system. The importance of "geographic information systems" (GIS) is highlighted, as it enables

electronic route optimization, which helps ships find new routes to deliver goods more efficiently and economically, and it provides location precision through the use of onboard and ashore GIS-based sensors, such as electro-optics, remote sensing, and LIDAR. Eventually, digitisation in shipping will lead to ships that are completely autonomous, safe, and dependable. The ship might achieve full autonomy with the help of adjacent AI-controlled systems that can navigate and manage it. These systems would include sensing and analytical tools, situational awareness, planning, and control capabilities. Future "Vessel Traffic Systems" (VTSs) will require new approaches and software. By eliminating the need for human intervention, the ideal systems will be able to autonomously gather and interpret data with great accuracy, feed it into decision-making systems, and propose evasive manoeuvres in dangerous situations. Modern technology has introduced new dangers to seaports and maritime trade, such as spoofing, data manipulation, and cyber-attacks. Any party with a stake in seaport logistics or maritime transport should pay close attention to the results.

Paladin et al. (2022) Utilizing cutting-edge “information and communication technology” (ICT) The two most critical elements in ensuring a high level of vessel traffic monitoring and maritime safety are tools and encouraging global cooperation among maritime authorities. Consequently, marine surveillance initiatives and regional and worldwide integrations rely on a "Common Information Sharing Environment" (CISE) that is cooperative, cost-effective, and interoperable. A network of maritime authorities working together on issues like environmental protection, border control, rescue missions at sea, and efficient data transfer and economic exchange through various interoperable systems utilising modern technologies makes up CISE. The CISE network core functioning is greatly improved by adopting a Big Data architecture that holds, organises, and distributes data to marine users. There is a growing need for this

processing due to the vast amounts of data being collected from diverse sources. This research delves into the benefits of the Data Lake architecture, counting its procedures, methodologies, instruments, and applications, to enhance marine surveillance and safety across the CISE network. Inside this section, you will find the components of the participating "command and control" (C2) systems that achieved interoperability and deployment. Finally, we examine the EU project EFFECTOR as an example; this initiative seeks to demonstrate how data-driven solutions may enhance marine situational awareness for tactical and strategic operations.

USLUER (2022) Safe navigation at sea is just one area where high technology and its wares have an impact on people's lives. In time, modern electronic technologies emerged as a viable substitute for the long-established, widely-recognized traditional approaches to maritime safety. If you're transporting goods by sea, you should invest in electronic technologies because they're more reliable and secure than traditional ways. Bridge electronic systems and the infrastructures that support them are compatible with high-tech goods as well. Without question, the most prominent instances of this are AIS, “electronic chart display information systems” (ECDIS), and “electronic navigational charts” (ENC). Such bridges and ancillary systems reduce likelihood of human mistakes and increase navigational safety on both domestic and international waters. Technology advancements in marine bridge navigation systems have had a beneficial impact on shipping, as discussed in this research.

Moroni et al. (2022) The UN's “Sustainable Development Goals” (SDG) prioritise the protection and sustainable utilisation of the world's aquatic environments and their resources for the advantage of generations to come. These goals have strong representation from the marine and maritime domains. Also, navigational safety is an issue, particularly near coastlines. Currently, there are operational services that rely on

cutting-edge technologies, such as in situ monitoring networks and remote sensing, to help with environmental preservation efforts through navigation and control. The potential of crowdsensing, however, remains untapped. To combat this, the authors of this study introduce a crowdsensing-based software that enhances maritime safety and awareness. As we plan to expand our environmental monitoring systems and frameworks in the future, this app can be easily incorporated. Maritime safety and security, crowd-sensing, citizen science, oil spill, pollution, and volunteer geographic information (VGI) are some of the index terms.

Bronk and Dewitte (2020) The problem of cybersecurity in the international marine system is the focus of this study. Trade across large bodies of water is made possible by the marine system, which consists of interconnected facilities. Both the challenge of preventing attacks on marine traffic and how cyberattacks alter this equation are addressed here. The writers investigate the nature of cyberattacks on ships, ports, and other marine infrastructure, as well as the measures used to prevent such attacks.

Munim et al. (2020) explored the application of artificial intelligence and big data in the maritime industry through a bibliometric study of 279 articles published in 214 scholarly publications by 842 researchers. They extracted bibliographic data from the Web of Science database and performed analysis using R's Bibliometric function. They identified the most important publications, writers, and organizations by analyzing citation data. Digital transformation in applications of big data from AIS, energy efficiency, the marine sector, and predictive analytics were the four major categories of studies found by bibliographic coupling. Extraction of future research issues was a result of their thorough analysis of these clusters. Additionally, they showcase author-level and institution-level research collaborative networks.

Bothur, Zheng and Valli (2017) The tide has not turned against cyberattacks on maritime infrastructure, so now is the moment to bring attention to the issue. The study examines various methods for securing shipborne systems and the vulnerabilities that exist inside them. There are a number of systems that are seriously faulty, including IT networks and industrial control systems, electronic chart display information systems, automated identification systems, and very small aperture terminals. Procedures and technological fixes are detailed in the countermeasures, which are in line with the "Defence-in-depth" idea. The marine industry is vulnerable to cyber threats because of its linked nature. Offshore platforms, submarines, and ships can all have Internet access by satellite. It paves the way for survival services, navigation, and communication in geographically isolated areas. Safer and more efficient processes and machinery may be controlled remotely, and new technologies are developed and used due to commercial pressure. The new standard of "smart" shipping will be made possible by these innovations, which include sensor fusion, AR, and AI. By 2035, completely autonomous ships without human crews will reportedly be plying international waters. Future research might build on this study to better understand the hazards and safeguard the maritime community from cyber threats.

Hayes (2016) Cybersecurity in the modern era is dynamic, ever-changing to address new threats. The United States maritime industry is susceptible to cyberattacks much like any other organisation. At this moment, neither the United States marine community nor national security is in danger from any significant cyber-attack. However, concerns about maritime cyber-attacks are justified in light of recent efforts to disrupt the industry's flow. Concerning cybersecurity in the maritime sector, the US has serious deficiencies. The effect of cyber threats on American national security is investigated in this thesis by comparing and contrasting US ports and policies with EU ones. Without

cyber resilience, the marine community would be ill-prepared to withstand and recover from a catastrophic cyberattack on the US. The United States' cyber resiliency and regular port operations depend on the international maritime community working together to resolve these concerns and preserve maritime superiority.

2.8 Definitions and Concepts of Maritime Security

Bueger, Edmunds and McCabe (2020) There has been an upsurge in global efforts to strengthen maritime security capacity. Additional research is needed in this area, both as a distinct field and as a model to inform reforms in other areas' security sectors and capacity-building initiatives. An early analysis of this area of study is this article. Their primary area of empirical study is the WIO, or Western Indian Ocean. Here, in reaction to Somali piracy, international entities have undertaken a slew of capacity-building initiatives. In doing so, they document the extensive range of capacity-building projects in the region and examine the ways in which maritime capacity-building has included novel elements that extend and refine the traditional definition of capacity-building. The authors conclude that studies on international security and development should devote more time and energy to the maritime domain, and they think about how lessons learnt from maritime capacity-building might be useful in other areas of international policy.

Germond and Mazaris (2019) It is widely acknowledged that coastal areas are more susceptible to the impacts of environmental change. In this light, researchers have focused extensively on the possible local, regional, and worldwide effects on society, the economy, and public health. Official strategy papers use the acquired knowledge to raise awareness and suggest and implement management and mitigation strategies to lessen risks to humans and the environment. Maritime crime rates, human security, and the social vulnerability of coastal towns have all been the subject of research. Although everyone agrees that we need a better grasp of how climate change is influencing

maritime security concerns, whether or not this body of information has informed policy is an open question. The link between social vulnerabilities, climate change, and maritime criminality is further explained in this paper, which synthesizes previous facts and understanding. Moreover, they investigate how much the maritime aspect of environmental change security is taken into consideration in official papers. There is a growing body of official rhetoric thatal connects climate change with marine security, but our research shows that official policy documents at the national and regional levels fail to address many of the academic community's concerns. Improving global ocean governance requires informing stakeholders and decision-makers about the potential linkages between climate change and maritime security.

Kanehara (2019) delves into maritime security by reevaluating the differences between the utilization of weapons in law implementation and utilized of force that is forbidden by international law. Due to the present strong inclination to comprehend marine security broadly, distinguishing between utilized of lawfully banned force and utilized of arms accompanying law enforcement is challenging but critically vital. Based on the premise that the type of force or weapons employed in an act or measure is, in principle, determined by the nature of the act or measure itself, this study first examines the debate around the use of force as defined in Article 2, Paragraph 4 of the United Nations Charter. The applicable case law will be presented subsequently, and then the non-prohibited use of weapons will be discussed. Examining the applicable sections of UNCLOS, It could be inferred that there are two separate types of weapon use: the first is the use of force, which is explicitly outlawed by international law, and the second is the use of arms, which is explicitly authorised by international law in relation to the administration of maritime law. Based on an analysis of current academic literature and Japanese legislation, this study concludes that the lines between security or military

legislation and law enforcement are blurry when it comes to maritime security. Law enforcement actions at sea are expected to take on more responsibilities than ever before to prevent the circumstances from getting worse. Accordingly, the key, according to this study, is to make sure that such weaponry doesn't fundamentally undermine the long-standing notion of the ban on force.

Chapsos and Malcolm (2017) Examining the Indonesian state's understanding and utilisation of maritime security, this article takes a look at President Widodo's stated goal of transforming his country back into a maritime nation. As the first step in a multi-stakeholder effort to assess potential ways to enhance Indonesia's maritime security capability, a Training Needs Analysis was conducted on key state maritime security players in the country. In covering the findings of this investigation, the report accomplishes its goal. The research shows that important maritime players in Indonesian state have different ideas about what maritime security is. It also claims that these players are ready to broaden their view of maritime security from a limited conceptualisation that focusses only on military threats and state defence. As a whole, Indonesia's strategy for maritime security reflects the emerging field of marine security studies' conceptual tendencies. The study finds that Indonesia could implement a more thorough maritime security agenda if the country maintains its current focus on the maritime domain in strategy and policy and places a premium on forming partnerships within and between non-state actors and the state. This study presents two prerequisites that, if supported, would lend credence to the human security lens as a useful tool for developing a more all-encompassing strategy for maritime security; further discussion of this topic is needed.

Germond, (2015) Despite the increasing amount of research devoted to various areas of maritime security, experts have disregarded the geopolitical dimension, which is discussed in this paper. The primary objective is to establish a shared understanding of

what "geopolitics" and "maritime security" mean. After a conceptual introduction to the geopolitical aspect of maritime security, the paper examines three real-world instances of 2014 maritime security geo-strategies. The findings show that geopolitical and geographical factors have an indirect and direct impact on maritime security goals and interests of nations and international organisations, even though this connection is only implicitly recognised in official documents. We invite academics and professionals with an interest in marine security to delve more into this aspect.

Bueger (2015) A relatively new term in field of international politics is maritime security. Some major players have refocused their efforts to incorporate maritime security as part of their mandate, or have begun to do so. The phrase "maritime security" highlights emerging threats and calls for collective action to counter them. Nevertheless, a universally accepted notion of maritime security remains elusive. When there is no universal agreement on a course of action, the use of buzzwords facilitates worldwide coordination. But these also confront the ever-present danger of hidden political strife and conflicts. There needs to be consensus-building techniques because there isn't a globally agreed-upon concept of maritime security. These three frameworks are put out in this study. The interconnectedness of maritime security with related ideas like blue economy, resilience, sea power, and marine safety provides a useful framework for first comprehension. Second, the securitization framework enables research into the origins of maritime dangers and the competing political claims that accompany them, illuminating hidden agendas and philosophies. Third, research into the actions of entities claiming to strengthen maritime security can be facilitated by security practice theory. All things considered; these models make it possible to draw a picture of maritime security.

2.9 Technology and Its Role in National Defense and Security

Shrestha (2024) Nepal has not yet adequately utilized technology to protect its national interests, despite its continual susceptibility to significant geopolitical influences. This research shows how states have used scientific technology to protect themselves and pursue their interests during difficult times. Investing in innovation and research is crucial for a nation's existence, as this report highlights. From a historical, geopolitical, and technological vantage point, this paper analyses the profound impact of tech on military strategy and tactics during conflict. This study looks at essential points in history when innovations like the bow and arrow, RADAR, proximity fuse, gunpowder, cryptography, and computer malware gave societies a significant leg up in protecting themselves. In addition, the study delves into the interconnected nature of scientific inquiry, new product development, and GDP expansion. It exemplifies how a nation's defensive capabilities and inventive ecosystems are strengthened by investments in science, which in turn drives economic growth. The overarching goal of this research is to survey all the ways science has bolstered national defense and prosperity. The research emphasizes the need for nations to adapt, interact, and utilize scientific developments to protect their interests in a world that is becoming more complicated by analyzing the association between strategy, innovation, and global dynamics. Nepalese politicians, military brass, and scientists can better navigate the complex terrain of national safe guardianship if they have a deeper appreciation for science's historical and contemporary roles in national defense. This will help guarantee a safe and prosperous future for Nepal.

Sarjito (2024) This research delves into the intricacies of improving national security through the formulation of defence management strategic policies, with a particular emphasis on how technical progress, changes in geopolitics, and tactics for dealing with non-traditional security threats have an impact. This context highlights how

international security threats are changing over time, calling for new ways of thinking beyond traditional military tactics. Defence management tactics are analysed in this study about technological breakthroughs including cybersecurity measures, machine learning, and artificial intelligence. Additionally, it seeks to comprehend how changes in global politics affect policies concerning national defence, stressing the necessity of plans that are both flexible and prospective. Studies also look at ways to deal with economic, environmental, and health security concerns, which aren't typically associated with conventional security issues. Literature reviews and case study analyses are examples of qualitative research approaches that make use of secondary material. Technological advancements improve threat detection, decision-making, and defence capabilities, according to the findings. Defence priorities, which impact strategy formation and foreign alliances, must be continually reevaluated due to geopolitical shifts. Integrated methods spanning economic, environmental, and health realms are crucial for effective tactics for dealing with atypical challenges. Finally, in order to ensure national resilience and mitigate complex security threats, a thorough and flexible defence policy framework is necessary.

Nurul Fadilah, (2024) An essential part of being a state citizen is standing up for the state, or maintaining national resilience. It is imperative that all citizens, and particularly the youth who will shape the nation's destiny, embrace and internalize the mindset of patriotism. According to the Constitution of 1945, “every citizen has the right and obligation to participate in efforts to defend the State” (Article 27, part 3). To evaluate and identify research works, this study uses the literature review approach, which is methodical, explicit, and reproducible. The study's overarching goal is to instil in students a sense of civic duty and patriotism, with a particular emphasis on the next generation's duty to protect the nation. Based on what we've covered so far, it's clear that

the government offers citizenship education to its citizens—and particularly the youth of the country—to fulfil the 1945 Constitution's provisions for national defence. Citizenship education will help future generations of Indonesians comprehend, evaluate, and respond to issues affecting their community, country, and state. Moreover, it must be compatible with the nation's objectives and ideals, as stated in the preamble to Constitution of 1945, and sustainable. It is believed that all Indonesians, particularly in this technology age, can be made aware of the importance of protecting the state or national security. For the simple reason that many outside dangers in our technology age are easy to ignore.

Pratiwi and Tarigan (2023)In this age of ever-increasing globalisation, technological advancement is a cornerstone that is constantly altering people's outlook on life. Furthermore, attempts to expand Indonesia's digital economy also include cyber security as a key cornerstone. The objective of this research is to weigh the pros and cons of technological progress on the integrity of Indonesia's national security. Quality descriptive research was the approach chosen. To counteract the potentially detrimental effects of technological progress on Indonesia's defence and security system, this report laid out some measures to be adopted. Increasing cyber defence capabilities, bolstering security and data protection, diversifying and improving human resources, collaborating with the private sector and universities, and implementing a rigorous supervision and control system can help mitigate the negative effects of technological advancements. To ensure that Indonesia's defence and security capabilities are robust, adaptable, and strong going forward, some of these measures must be put into place with unwavering dedication and effort.

Bibby and Dehe (2018) Companies are confused about what Industry 4.0 has in store for them since they have not yet completely grasped its complicated features. In this research, we build an evaluation framework for gauging the extent to which three aspects

of Industry 4.0—Factory of the Future, People and Culture, and Strategy—have been put into service. The eight components that make up the primary dimension known as the "Factory of the Future" are as follows: sensors, e-value chains, manufacturing execution systems, cloud computing, additive manufacturing, IoT and cyber-physical systems, big data, automation, and autonomous robots. The model is developed, tested, and validated by a defence manufacturing business; twelve other partners are also reported on in the research. They discovered that the core firm had a higher Industry 4.0 maturity level (59.35) than the average for the sector (55.58). This study adds to what is already known by doing an analysis of critical participants in the defence supply chain and then experimentally developing a model for the entire system.

Galinec, Možnik and Guberina (2017) Cybersecurity is an umbrella term for many different approaches, methods, and ideas that are all inextricably linked to information and "operational technology" (OT) security. One notable feature of cybersecurity is its involvement of offensive information technology attacks against adversaries. Both consumers and security professionals are confused by the phrase "cybersecurity" when used interchangeably with information security and technology security, which fails to highlight the important distinctions between the three fields. The researchers aim to define cybersecurity and describe the associations between cyber defence, operational technology security, information security, and other relevant domains and practices that are important to the national cybersecurity strategy. Security leaders should use the term cybersecurity exclusively to describe defensive security measures that use IT and/or OT environments and systems. The case study provides an example of “Republic of Croatia's National Cybersecurity Strategy” and Action Plan, which are presented and analyzed in detail. Acknowledging organizational issues with the

strategy's implementation and increasing awareness of the issue's societal importance are its principal goals.

2.10 Current Technologies in Maritime Security

Longo et al. (2023)Navigational situational awareness relies on some tools, one of which is the operation of radar equipment. Computerized instruments and their indications are becoming increasingly important to operators due to the growing demand for constantly running logistics and tighter shipment deadlines. Consequently, contemporary ships are more like a cyber-physical system, with computers and sensors continually coordinating and communicating with one another. One of the ship's most vulnerable security systems is the radar system, and in this work, we explore new risks to it. First, they go into depth about certain new attacks that can corrupt radar data, which could have disastrous effects on the crew's awareness of their surroundings or possibly their safety. Then, without modifying the target ship's setup, they introduce a detecting system that aims to identify irregularities in the radar video stream. Last but not least, they launch the assaults in a simulated setting to test their detection system. The assaults are doable, relatively simple to execute, and difficult to detect, according to the experimental data. They also demonstrate the efficacy of the suggested detection method.

Michaela Barnett, Issah Samori, Brandon Griffin (2023)The new areas of “bio cyber security” (BCS) and “cyber biosecurity” (CBS) have been extensively covered in the literature. The following are included: policy, generic applications, mission awareness, and definition. Particular BCS/CBS vulnerabilities with maritime theaters—that is, commercial and military endeavours focused on the ocean and littoral—are a subject that has gotten little attention. Future maritime-specific BCS/CBS attacks pose a significant threat to bioeconomies and military alike, threatening to diminish their capacity for activity. This is especially true when the aforementioned weaknesses are

used to attack transportation and personnel, hence causing logistical disruptions. This research takes a look at the increasing importance of CBS/BCS in the maritime domain, potential weak spots in maritime environments that could be used for BCS attacks, potential future attacks, defences, and preemptive positioning strategies, as well as relevance of CBS/BCS in international policy and how they differ in application. To inspire constructive action in this area, this study seeks to expedite and simplify the debate of BCS.

Ben Farah et al. (2022) offers a classification system for cyberattacks based on the most up-to-date standards in the maritime industry. A thorough classification of the ship's parts has been carried out, and the study of the most important port services has been supplemented. Due to its status as a vulnerable component of numerous marine infrastructures, "Global Navigation Satellite System" (GNSS) has been the focus of much research into potential cyber threats. New studies show that the extensive use of new enabling technologies, like IoT and Big Data, is driving the alarming growth of cybercrime. But there's no denying the compelling trend towards more integrated systems, which is producing substantial economic value through easing the way for autonomous vessel operations, increasing the use of smart ports, decreasing the need for human labor, and dramatically improving fuel efficiency and service quality. Lastly, they have outlined some of the more tangible difficulties and potential directions for future study.

Muhdar, Hamzah and Sofilda (2022) A country that is an archipelago and has several rear exits has transportation security as a top strategic concern. Investments by global corporations rely heavily on ports and shipping channels. Stakeholder expectations and the effect of secure maritime transport on Indonesia's GDP growth are the foci of this research. This inquiry made use of both quantitative and qualitative methodologies. The

quantitative method relied on Input-Output analysis, whereas the qualitative method relied on NVivo for the conduct and analysis of "Focus Group Discussions" (FGD). The quantitative method revealed a movement of 21.99 billion IDR in GDP and a rise of 0.13 billion IDR in worker income. An additional 79,072 workers were added to the workforce, and labour income increased by 860.31 billion IDR, all as a result of changes in the other 53 sectors. The qualitative research showed that, among all the stakeholders, Stakeholder Synergy made the biggest impact in improving the ecosystem for maritime transport security. A governmental policy's multiplier effect on all revenue and employment sectors is inevitable.

ÇETİN and KÖSEOĞLU (2020) The unfettered movement of commodities across maritime communication routes is jeopardized by some dangers, including piracy and terrorist strikes. Any dangers encountered in international and territorial waters that interrupt this flow could have a negative influence on the global economy. The study's overarching goal is to catalogue all the security issues confronting the marine sector, from those that originate in the water itself to those that endanger long-term maritime economic viability and those that call for concerted action on a global scale to ensure peace and safety, those that pertain to the protection of maritime areas vital to the global trade of goods, and those that are more traditional. It also seeks to categorise marine security threat subjects in light of global security strategy advancements and rising security problems, with an eye on how these factors affect maritime economics. The ever-increasing complexity of marine security issues is a major reason why there is no universally accepted definition of this concept. It is believed that a comprehensive strategy would be most suitable to deal with the subject, given its extensive and unexpected structure that cannot be contained under The ISPS Code. Aiming to provide

academic guidance to decision-makers, this study attempted to categorise dangers within the realm of maritime security.

Mraković and Vojinović (2019) An all-encompassing cyber security management strategy is required due to the increasing complexity, digitisation, and automation of systems in the maritime industry. Online, there is an ever-increasing number of ship-to-shore networked technologies that necessitate heightened security measures. Cybersecurity has recently emerged as a key issue in maritime computing. Death, theft of ships or critical data, and other serious consequences can result from cyber incidents in the maritime industry. From a cyber security standpoint, this report addresses critical issues in the maritime industry and offers recommendations for resolving or reducing them.

Germond and Ha (2019) In terms of political and governance priorities, environmental change and maritime security are at the top of the list for nations and international institutions right now. The real interconnections and dependencies between the two problems, however, have received very little attention from either academics or practitioners. Using "International Maritime Organization" (IMO) as an example, this study is the first of its kind to employ a corpus linguistic approach to uncover the lack of a narrative connecting the effects of environmental change with the incidence of maritime crime, even though there are some correlations in practice. Nonetheless, narrative connections between environmental change and migration maritime security were discovered, suggesting an indirect relationship between two. The study finishes by discussing what these results mean for future studies and real-world applications. Researchers in this field should reevaluate their present narrative in light of the connections between climate change's effects on human and non-human systems, as well as on maritime security.

2.11 Global Overview of Maritime Security Technologies

Islam (2024) Examining the ethical aspects of maritime security in light of the fast-paced evolution of technology, this article delves into the possibilities and threats posed by new tools for maritime security operations. Privacy invasion, disproportionate force, and the loss of human discretion and responsibility are some of the possible dangers associated with technology abuse. Ensuring the proper and moral application of technology in marine security requires a balanced perspective that considers the benefits and drawbacks of technological advances. Additionally, there needs to be strong governance and international collaboration. A literature survey of academic papers, policy papers, and pertinent case studies on maritime security makes up the research technique. Technologies such as cyber threats, unmanned maritime systems, and surveillance capabilities are evaluated for their ethical consequences using concepts such as proportionality, necessity, transparency, accountability, and human rights. The article highlights the importance of teaching maritime security personnel ethical principles and encouraging them to make responsible decisions. It suggests using case studies and simulations to test how well these principles work in practice. This study adds to continuing conversation on maritime security ethics by arguing for a proactive strategy that strikes a balance between technological possibilities and ethical principles. It provides a blueprint for making the oceans a place where people can freely travel while still feeling secure and having their rights honoured.

Palbar Misas et al. (2024) The marine industry is becoming automated due to technological advancements and will continue to do so in the future as it aspires to have completely autonomous vessels. The way ships are currently operated depends on a combination of human intervention, human decision-making, and automated systems. The use of onboard mariners may become obsolete as the number of remotely operable

vessels increases thanks to autonomy. Because these operations are taking place at great distances, mariners face additional operational hazards, such as the possibility of diminished "Situational Awareness" (SA) and cyber threats. Maritime activities rely on SA, and this study will go over the benefits and drawbacks of SA in distant operations. The second part of this study will be an examination of the education and preparation that sailors might require to operate in such a distant environment. Finally, with the coming of remote operations, it is vital to understand the current and future expertise of sailors in handling higher risk operations, such as port arrival/departure and heavy traffic.

Alqurashi et al. (2023) There is a growing need for dependable maritime communication technology due to the increasing number of oceanic operations, as water makes up 71% of the Earth's surface. Networks on land, in the air, and in space are all part of the current maritime communication systems. To provide a comprehensive review of the many maritime communication methods, this study also details recent developments in some marine technology. The study begins by providing an overview of the various methods utilised for maritime communications in optical and “radio frequency” (RF) bands. After that, they go over the models for marine communications radio resource management, coverage, capacity, modulation, and coding, as well as RF and optical band channels. The research continues by outlining some potential future applications of marine networks, including IoS and the S2U Internet of Things. Last but not least, they point out some intriguing unanswered questions and propose some avenues for further study in maritime communication, such as expanding internet access to the ocean floor, developing on-board applications for terahertz and visible light signals, and developing data-driven models for optical and radio marine propagation.

Wirawan (2022) The return of Indonesia to its maritime roots is central to President Jokowi's "World Maritime Axis" agenda. Indonesia, the largest archipelago in

the world and a country ideally situated between the "Indian and Pacific Oceans," is perfect for this. An international trade route that powers the global economy passes between the two oceans. In terms of geopolitics and geo-economics, Indonesia's location between the two oceans is advantageous. Threats and challenges to Indonesia arise from the maritime realm because its territory comprises the world's busiest shipping lanes, Malacca Strait and Singapore Strait. If Indonesia wants to contribute to global economic stability through the trade of diverse commodities along regional and national waterways, it must guarantee marine security in these areas. Since no one nation can effectively address marine security challenges that cut across international borders and affect other countries' sovereignty, defence diplomacy has emerged as a key component of Indonesia's maritime security strategy. Gradually enhancing defence capabilities is possible through the implementation of defence diplomacy in response to disruptions to maritime security. Within the context of "World Maritime Axis", Exploring the impact of maritime security on Indonesia's defence mediation, this study use content analysis to conduct a qualitative investigation. Defence diplomacy and marine security policy are topics he brings up while discussing this.

Akpan et al. (2022) There has been a meteoric rise in the frequency and severity of cyberattacks, and as a consequence, companies have suffered enormous monetary losses due to recovery costs, regulatory fines, and collateral damages like trust and reputation. When it comes to cybersecurity attacks on operational technology, the maritime industry is experiencing a 900% surge as it enters the digital era. This is even though the sector was previously assumed to be risk-free because ships at sea are geographically and technologically isolated from land. While there is some research happening in this area, cybersecurity in the maritime sector has not been thoroughly examined. Therefore, to shed light on security issues and concerns, this report offers a

thorough examination of the cybersecurity landscape in the maritime sector. At the outset, it delves into the systems accessible on ships that might be the object of an assault, the weaknesses in those systems, the potential outcomes of an attack, and real-life incidents. In the next section, potential preventative measures against these attacks are outlined and evaluated. At last, we talk about some of the difficulties and unanswered questions that remain for further study.

Freire et al. (2022) The aim of a strategic area known as "marine Domain Awareness" (MDA) is to help coastal nations keep tabs on their marine resources and EEZ. Within this framework, a "Maritime Monitoring System" (MMS) seeks to actively monitor maritime operations, both military and civilian, utilizing sensing devices like radars, optronics, "Automated Identification Systems" (AISs), and IoT, among others. The cybersecurity and scalability of such a diverse system provide significant obstacles to rolling out a nationwide MMS. This study investigates blockchain technology as a potential solution to these problems by enhancing MMS cybersecurity and guaranteeing the availability, validity, and integrity of pertinent navigation data. They suggest an open-source blockchain technology called Hyper Ledger Fabric, which is strong, flexible, and efficient, and they use it to construct a permissioned blockchain solution prototype. In order to assess how well this strategy works, a real experiment is carried out. A cheap AIS receiver built on a Raspberry Pi that receives data from sensors through "Software-Defined Radio" (SDR) technology is linked to the prototype. They created an easily deployable dockized blockchain client to decrease scalability attrition. Also, to lower implementation and maintenance costs, they ascertained the client's ideal hardware configuration through substantial experimentation. The outcomes demonstrate the practicality and efficacy of our approach within the framework of an MMS utilising AIS

data, while also providing a quantitative assessment of the overhead associated with blockchain technology and its impact on "Quality of Service" (QoS).

Frøystad, Bernsmed and Meland (2017) The world's most vital distribution of goods is handled by ships that ply their seas. Ships are becoming more and more like interconnected floating computers, which means they are more vulnerable to unwelcome cyber activities, as they evolve from separate pieces of empty metal vessels. Using a Public Key Infrastructure (PKI) architecture, this research demonstrates how the marine industry can safeguard digital communication. Here we are talking about emerging services that rely on datalinks between ships, ships and shores, and where both deliberate and accidental cyber threats can do serious damage to cargo, personnel, ships, and the environment. Due to design considerations of domain specific characteristics, bandwidth is limited and ships may experience lengthy periods of unavailability. Significant motivators have also included cost-effectiveness and global applicability. They describe the proposed PKI's design and how it can be operated in a global marine setting, and they give design goals that came from workshops and surveys that involved stakeholders in the maritime domain.

2.12 Technologies in Indian Maritime Security

Current Technological Landscape in India’s Maritime Security

Scarlat, Ioanid and Andrei (2023a) Marine ports are an integral link in the logistical network that includes the whole shipping industry and shipbuilding facilities, which are all undergoing an intricate DT. This study intends to outline the history of maritime transport and logistics as it relates to IT, identify the key features of each generation that has had an impact on these fields (e.g., intelligent sensor and IoT usage, position monitoring through geospatial technologies and databases, intelligence-based decisions), and finally, suggest a future autonomous vessel port management system. The

importance of GIS is highlighted, as it enables electronic route optimization, which helps ships find new routes to deliver goods more efficiently and economically, and it provides location precision through the utilization of onboard and ashore GIS-based sensors, such as remote sensing, electro-optics, and LiDAR. Eventually, digitization in shipping will lead to ships that are completely autonomous, safe, and dependable. The ship might achieve full autonomy with the help of adjacent AI-controlled systems that can navigate and manage it. These systems would include sensing and situational awareness, analytical tools, planning, and control capabilities. We need new methods and software for future VTSs. The ideal systems will be fully autonomous, collecting and interpreting data with pinpoint accuracy without any human input whatsoever. feed it into decision-making systems, and propose evasive manoeuvres in dangerous situations. Modern technology has introduced new dangers to seaports and maritime trade, such as spoofing, data manipulation, and cyber-attacks. Any party with a stake in seaport logistics or maritime transport should pay close attention to the results.

Zhang et al. (2022)Several nations and areas have investigated potential e-navigation test beds since the e-navigation plan was proposed. Nevertheless, navigation data comes from a variety of sources, and there are challenges to integrating data from all of these sources into a cohesive whole for study and use. Users frequently encounter challenges while attempting to access the necessary detailed navigational data. The goals of this research are to enhance the navigation safety guarantee, make shipping transportation organizations better at port operations, facilitate the sharing of navigation and safety information, create a platform for managing maritime data security based on e-navigation architecture, safeguard the marine environment, and increase monitoring of the marine environment. Consequently, this research presents a four-tiered system design utilizing “Java 2 Platform Enterprise Edition” (J2EE) technology. It creates a combined

platform for storing, analyzing, and managing maritime data. We need new methods and software for future VTSs. The ideal systems will be fully autonomous, collecting and interpreting data with pinpoint accuracy without any human input whatsoever. this platform may supply ships with comprehensive data resource services for navigation. This research delves into the system architecture and data interchange mode of a marine data security management platform, outlining its design, development, and demonstration operating schemes.

When faced with threats from the air, sea, and land, every country strives to beef up its defence capabilities. To avoid unforeseen dangers, naval force capacity and coastal security are paramount in maritime security. The purpose of these naval operations is to defend against potential attacks in the future (Bueger, 2015). The government's defence system also includes working to shape a maritime environment that is favourable to the country. Ocean security is an integral part of India's strategy to build up its marine forces and ensure they can continue to meet the country's demands for maritime security. With a strong presence on all three coasts of the Indian Ocean, India is showing its interest in the maritime sector, which is vital for trade, transportation, and the sea wealth through fishing and other activities. It demonstrates India's rise to become an international force in the nautical arena. India has taken many steps to strengthen maritime security, including:

- India's financing of the Bangladesh Air Force.
- Building a port in Myanmar to ship weapons
- Collaborative patrols and training exercises with the nations of Indonesia, Malaysia, Indonesia, and Singapore
- Collaboration and infrastructure facilities with Australia

- Collaborating with vital ports and islands such as Andaman Nicobar and Cocos in Australia, Diego Garcia in the US, and Réunion Island in France
- Facilities for operations in conjunction with the Maldives and Sri Lanka
- Obtaining authorization to use maritime communication facilities with Mauritius and Madagascar
- As a whole, India has great relationships. Authorization to use Oman's ports, joint exploration of India's oil reserves with the UAE, and submarine drills in Iran.

This growing influence of India on the subcontinent can be attributed to the aforementioned projects and activities. The country's amiable and cooperative ties with its neighbors were a direct outcome of these initiatives. It's also evidence of India's neighbourly friendliness and cooperative practices.

There are three branches of the Indian military that protect the country's coastlines: the Coast Guard, the Navy, and the Coastal Police (Patel, Malik and Nunes, 2016). various tiers. Coastal and marine security is the domain of the Indian Nodal Agency. They ought to highlight the Indian navy's strengths if they are discussing Indian maritime security. The Coast Guard and naval forces of India play a key role in maintaining maritime security. Vikramadhithya and other recently commissioned warships and submarines contribute to the nation's rise to international prominence (PTI, 2021). Due to their ability to detect enemy attacks in real time, submarines play a crucial role. Indian naval vessels such as the Arihant, Shish Umar, Sindhu Ghosh, etc., are constantly guarding the safety of Indian waters. The Indian Navy's elite commando squad, Marine Commandos, or "MARCOS," is renowned for its exceptional performance in maritime operations and missions. As an observer member of Indian Ocean Commission, India has been instrumental in fostering ocean cooperation, which has been useful in establishing such partnerships with countries like the Seychelles, Mauritius, and

Madagascar. One aspect of India's maritime security concerns is the development of warships in collaboration with private enterprises, such as “Mahindra Defence System Limited” (MDS) and Seagull Maritime Security, among others. Private yards also benefit from this trend.

(Joy, 2021) The study offers a concise overview of the strengths and weaknesses of India's marine security apparatus. One of the major concerns with the current international system is maritime security. The necessity for marine security is heightened by the fact that India is bordered by three bodies of water on three sides. There are numerous dangers that ships and maritime operations need to be safeguarded from, including piracy, robbery, illegal individuals, pollution, goods trafficking, and unlawful fishing. Many plans and programs have been developed to strengthen maritime security by international organizations and various states, India among them. Examining the function of marine security in power maximization is the primary goal of this article. The report also takes a look at India's marine security and how it's doing.

Premarathna (2021) Marine security is a catch-all phrase used by security agendas to categorise marine domain challenges, many of which are connected to national security. The idea of maritime security has grown trite in the realm of international affairs in recent years. The importance of marine security has been reemphasised or included in the missions of numerous powerful organisations. As a new development in security theory, non-traditional security concerns are given special attention. The energy and economic channels of the world now mostly pass via IOR. The strategic importance of Sri Lanka's position is high as well. The Indian Ocean region is home to a plethora of conventional and unconventional dangers to regional stability. For example, illegal fishing without a license IUU, climate change, terrorism, armed robberies at sea, human trafficking, drugs, wildlife, and weaponry. Ultimately, this research aims to uncover and

analyze the challenges associated with maintaining maritime security in the contemporary context of Sri Lanka and the Indian Ocean. The primary question that needs answering in this study is how maritime security concerns in Indian Ocean relate to modern Sri Lanka. This study used a qualitative methodology that combined primary and secondary sources of information. Thirty individuals from various professional backgrounds (including academia, the military, and government) were surveyed to gather primary data. The study identifies several issues that currently threaten the security of the Indian Ocean. These include the following: the militarisation of strategic chokepoints in the ocean, a lack of maritime awareness (MDA), growing naval rivalry between some littoral governments and important marine users, and need to seal off illegal actors while still allowing free navigation along the ocean's communication lanes. Today, Sri Lanka faces some concerns, including climate change, environmental degradation, maritime terrorism, unchecked extraction of marine resources, and illicit trafficking of weapons and drugs. Based on the research, the modern Indian Ocean region and Sri Lanka primarily face non-traditional maritime security problems. In addition, while looking at the region's effects on environmental and political security, as well as economic and military security, the most concerning ones are the effects on political and environmental security.

Strengths and Limitations of India’s Maritime Security Systems

Karunya (2024)Maritime security has become an increasingly critical aspect of national and regional stability due to the strategic importance of the seas in global trade, resource management, and geopolitical dynamics. For India, which is located along major sea routes and has a vast coastline, confirming maritime security is crucial not only for protecting its economic interests but also for maintaining regional peace. In recent years, the Government of India has significantly ramped up its efforts to bolster maritime security through a series of strategic initiatives. These measures aim to address a wide

range of challenges, from safeguarding the coastline against threats and confirming the safety of maritime trade routes to enhancing the nation's naval capabilities and fostering international maritime cooperation. The initiatives undertaken by India reflect a comprehensive approach to maritime security, integrating advanced technology, strengthening infrastructure, and enhancing coordination among various agencies. They encompass the development of strategic naval bases, improvement in maritime domain awareness, and active engagement in regional security frameworks. As global maritime dynamics evolve, these initiatives are designed to adapt to emerging threats and opportunities, ensuring that India remains vigilant and prepared to safeguard its maritime interests. The Government of India's proactive stance on maritime security underscores its commitment to securing its maritime domain and contributing to the stability and prosperity of IOR and beyond.

Sahu (2022)This study offers a concise overview of the capabilities and difficulties that India faces in terms of maritime security. Within the context of current order of the globe, maritime security is one of the most important challenges. Since India is a country that is encircled on three sides by different bodies of water, there is an increased requirement for marine security. Terrorism, illegal fishing, robbery, piracy, illicit trafficking of goods and people, and pollution are some of the different areas in which ships and maritime operations need security. Some policies and efforts aimed at enhancing maritime safety have been developed by international organizations as well as various states, one of which is India. Examining marine safety's role in power consolidation as a whole is the major goal of this study. On top of that, it delves into the pros and cons of Indian maritime security.

Khalid (2021) Maintaining a state's existence is the responsibility of the national security apparatus, which includes the military, diplomacy, economy, and politics. These

days, national security encompasses a lot of non-military factors including economic security, energy security, environmental security, etc., and military might and defence preparation are just one part of it. Given this reality, every nation must establish defence mechanisms to ward off both internal and external dangers. Nonetheless, being ready for defence or the military remains a top indicator of national security. Protecting national interests and establishing deterrents are the dual functions of the security forces maintained by all superpowers, great powers, and regional powers. India is a huge, powerful nation in South Asia, and it spans the whole subcontinent. Pakistan, China, Nepal, Bhutan, Myanmar, and Bangladesh are among countries with it has borders. Its continental shelf is rich in resources, and it has a lengthy maritime boundary and territorial waters. Because of its hundreds of islands, it is well-positioned in the Indian Ocean; including Lakshadweep and the Andaman & Nicobar Islands. India has a complex security situation in the seas and on its borders. It is crucial to safeguard Indian Ocean because of its marine trade and the oil it gets from its "Exclusive Economic Zone" (EEZ). Somali-born sea piracy, Rising terrorism, SLOCS, safeguarding India's prized maritime assets, and numerous other national security concerns are among India's pressing challenges. In response to these threats, India strengthened its navy and increased its naval presence throughout Indian Ocean. India has grown into a dominant naval force in the region through the years by increasing its naval outreach. Additionally, it has utilized its advantages strategically and diplomatically to forge partnerships with other regional and global powers. The Indian Navy has grown from its fearsome beginnings to become the world's fifth-largest. Recognised for its expert knowledge, it is a formidable force. That being said, the article sheds light on the growing power of the Indian Navy and how it is safeguarding the country's national security. The study's stated goal is to aid India's force projection in Indian Ocean area by gaining a better

understanding of the dangers to the country's national security and role the navy has played in countering these threats.

India is worried about its marine security because of dangers that affect its maritime interests, most of which are placed in Indian Ocean, which is the country's principal area of interest. Although these dangers affect other regional stakeholders as well, India would feel their effects more acutely because India has already taken on her obligations to protect the Indian Ocean region. (Ministry of External Affairs, 2016). Since the late 1990s, the worldwide community has been deeply concerned about piracy originating from Somalia. To reduce the frequency of these attacks, international community has had to work together (ICC International Maritime Bureau, 2015). With the help of its maritime security forces, India has successfully escorted many merchant ships from all over the world. Thus, in October 2015, the High-Risk Area was moved west of India, and the piracy that had previously extended as far east as the Maldives and Lakshadweep islands is now under control (Sharad Raghvan, 2015). But any easing of counter-piracy measures, along with Somalia's political instability, might lead to a return of the crime. Off the coasts of Bangladesh, Malaysia, and Indonesia, there has been a rise in piracy, mostly including thefts committed at anchorages, while piracy based in Somalia has been trending lower (ICC International Maritime Buereu, 2015). Despite the lack of justification for global anti-piracy measures, littoral governments must take action. It is encouraging that the governments of the Philippines, Indonesia, and Malaysia have recently decided to conduct combined patrols; this will discourage pirate attacks and put the minds of the global maritime community at ease (Sapiie, 2016). In 2008, the Indian Navy hosted the "Indian Ocean Naval Symposium" (IOR), which brought together representatives from every state in the Indian Ocean region. The purpose of the gathering

was to facilitate the sharing of knowledge and ideas related to anti-piracy efforts in the IOR.

Upadhyaya (2018) delves into India's maritime policy, taking a close look at its effectiveness and long-term viability. It also delves into India's aspirations to become a “net security provider” (NSP) for the area. It aims to govern if India's current maritime strategy would enable it to keep the power balance with China and, if not, to offer complementing actions and other strategic choices so that India can achieve its objectives in Indian Ocean. In this report's first section, we examine the security environment of Indian Ocean in the twenty-first century and the strategic maritime dangers and challenges that India faces. Pirates, terrorists at sea, and illicit fishing are all examples of non-traditional dangers, and India also faces the more familiar dangers from its adversarial neighbours, Pakistan and China. The next section examines the influence of Indian foreign policy on the country's maritime doctrine and strategy. Next, we'll examine India's stated maritime strategy objectives, which boil down to becoming the primary NSP for the littoral states and fostering a hospitable environment in the Arabian Sea. The study continues by looking at how maritime security cooperation has been aided by the shifting global security order in the 21st century, and it then suggests a new framework for measuring the level of collaboration between regional governments and India by looking at the data. Within this context, the paper delves into India's efforts to enhance maritime security cooperation with both regional and non-regional powers. It offers a critical analysis of the breadth and depth of these interactions, backed by factual evidence. After that, they discussed the effects of China on the region and compared and contrasted the bilateral security ties between China and India. The research argues that most regional states have established long-lasting bilateral security relationships with India. With China's growing influence in the Indian Ocean, however, this strategy will

not be sustainable in the long run. Using India's geostrategic advantage in the Indian Ocean as a springboard, the paper highlights the shortcomings of India's current maritime policy and suggests a remedy. Investigating India's role in the multilateral maritime security cooperation in the Indian Ocean, the study draws attention to the risks posed by India's isolationist attitude towards regional cooperation and argues that China and other non-regional actors ought to play a role in guaranteeing the maritime security of the region. According to the report, there is a significant risk of China shifting the power balance in favour of itself relative to India, given the extent to which Chinese maritime strength is following its trade in Indian Ocean region. Then, what are India's alternative strategic choices? The study generally suggests the following: Instead of relying on international connections, which may change over time, India should recognise that national policy is about making the most of Indian means. Accordingly, India's present marine strategy, which is centred on fostering bilateral relations, may be fruitless and unable to remain in place. According to the report, India's marine policy is most vulnerable about Andaman and Nicobar Islands. It contends that India might have taken advantage of the Andamans' geostrategic potential by developing them into a fully functional military command, but instead, it has ignored the Strait of Malacca. An ever-increasing Chinese naval presence and increasing political and economic clout in Indian Ocean region pose a danger to India's strategic maritime advantage. Thus, India must advance Andaman and Nicobar's command to a level where it can compete with other naval commands. In addition, India has to work towards better maritime multilateralism in the IOR and push for more integration of the existing sub-regional institutions equally. As part of its current plan to become the sole "security provider" in the area, India is going for the gold at all regional forums. By doing so, China may gain influence in Indian Ocean and limit the growth of marine multilateralism. Ultimately, thesis argues that

establishing an information grid that spans the whole Indian Ocean ought to be India's top initiative. This regional strategic initiative has the potential to bring together different parties involved in regional security, which would enhance India's standing in the region.

CHAPTER III:

METHODOLOGY

3.1 Overview of the Research Problem

Maritime security is protection of sea vessels of all kinds both on a domestic level and internationally, there are many threats like piracy terrorism trafficking of people and resources Ellis fishing pollution of water bodies etc that are posing several problems and difficulties in the maritime industry. Shipping industry is one of the oldest kinds of and most common event today remember how India was discovered by Vasco da Gama while he was on a ship that old is the history of maritime indulgence. Preventive efforts to stop any illegal or immoral behaviour in the sea are part of maritime security, which also includes reactive measures to defend the maritime domain from threats both domestically and internationally as well as legal actions. There have been incidences like spotting of marine vehicle from China Andaman and Nicobar waters which enhance the importance of maritime security in respect to India. In this dissertation, we look at the marine business and the dangers it faces from armed robbery. We explain these dangers in detail and talk about how technology might help fight this problem. Technology is one thing which has helped to solve many problems in marketing of areas and how it can be fruitful for the maritime industry is the goal that the project aims to achieve (Nik Nor Suhaida Ali, Anas Afandi Ahmad Apandi and Laila Suriya Ahmad Apandi, 2016b)

3.2 Research Purpose and Questions:

This dissertation is an honest attempt to advance current understanding of maritime security and the part technology plays in it. To move the dissertation forward, a qualitative approach will be taken. In order to gather perspectives on the marine industry and different aspects of maritime security, three sets of questionnaires will be made and sent to the following groups of people:

- **RQ-1.** Administrative officers that will include officials responsible for overall administration and legal aspects.
- **RQ-2.** Officers responsible for enforcing National Maritime legislation in their respective
- Maritime zones like - coast guard, Navy, Maritime security agency, Marine police etc.
- **RQ-3.** Cast and crew present at the ship that include ship masters, shipping organizations and companies, shipping associations etc.

3.3 Research Design:

A research model on the role of technology in maritime security could focus on the mechanisms through which advanced technologies enhance operational efficiencies, threat detection, and response effectiveness in maritime environments. This model would explore how emerging technologies, such as satellite tracking, automated identification systems (AIS), and unmanned aerial vehicles (UAVs), contribute to secure and monitor maritime boundaries, with a particular emphasis on preventing illegal activities like piracy, trafficking, and unauthorized fishing (Okafor-Yarwood *et al.*, 2024). The study design would involve a mixed-method approach, integrating both qualitative interviews with maritime security experts and quantitative analysis of technological impact on security metrics. These may be threat detection and assessing capability, response time, cost of operation as well as accuracy of tracking systems. The qualitative part would be carrying out thematic analysis of the views of the experts and scholars in order to identify their impressions and experiences and ground realities for the development of the themes The quantitative part could involve use of regression analysis in a bid to estimate the degree of fit between the technology umbrella and the maritime security outcomes (Kiger and Varpio, 2020).

Examining the efficacy of maritime security systems in the Indian Ocean and the Gulf of Aden could be the subject of this research's comparative case study approach. To enhance the reliability of data gathered and data triangulation, secondary data from the government and security, for instance the International Maritime Organisation (IMO) would be reviewed (Baig, Lagdami and Mejia Jr., 2024). This design would enable analysis of the contribution of technology as all four elements captured would present policy direction on enhancing maritime security through technological advancement. The outcomes of the research study may also provide useful information on the cost−benefit factors, so that agencies could understand how to adopt the technologies that are most important for their security while considering financial limitations.

3.4 Population and Sample:

People who work for maritime security services as a career are part of the study's population. as well as participants from governmental maritime organs and organizations, private security service vendors and technology organizations in the area of maritime security and safety. In this particular case, a total of 100 participants will be targeted in order to gather diverse opinions and perceptions regarding how technology might enhance maritime security measures. In the study, convenience sampling will be used to select the respondents, this is because it makes selection to be done based on the willingness and availability of the respondents. This non-probability sampling technique is advantageous in exploratory research, as it enables the researcher to efficiently gather data from a readily accessible sample, which is particularly useful given the specialized nature of the population (Etikan, 2016). While convenience sampling may introduce some biases, it allows for practical data collection and provides valuable insights that can guide further research and policy formulation in maritime security contexts.

3.5 Participant Selection

Criteria	Inclusion	Exclusion
Participants	Administrative officers involved in maritime security administration and legal aspects	Personnel unrelated to maritime security or administrative responsibilities
	Law enforcement personnel from the Coast Guard, Navy, Marine Police, and Maritime Security Agencies	Officers from other sectors (e.g., aviation, land security) not related to maritime enforcement
	Ship-based personnel (shipmasters, crew, shipping organizations, shipping associations) involved in maritime security	Crew members not engaged in maritime security or unfamiliar with maritime technology
Experience in Maritime Security	Participants with a minimum of 1 year of experience in maritime security roles	Individuals with less than 1 year of experience in the maritime sector
Knowledge of Technology	Participants familiar with or actively using technology in maritime operations	Individuals with limited or no exposure to technological tools or systems in maritime contexts
Location	Participants operating within national maritime zones (coastal, territorial, or Exclusive Economic Zones)	Individuals based outside of national maritime zones or international waters
Language	Participants able to communicate effectively in the research language (e.g., English)	Individuals unable to communicate in the research language

Availability for Data Collection	Individuals available to participate in surveys, interviews, or focus group discussions	Individuals unwilling or unable to commit time for data collection activities
Organizational Consent	Organizations willing to permit participation of their staff in the study	Organizations refusing to allow staff to participate in data collection activities

3.6 Instrumentation

The instruments used in this study were a structured questionnaire that was created based on the research questions formulated in an effort to elicit the perceptions and experiences regarding the use of technology in enhancing marine security. The three main variables that the questionnaire was designed to address were “Maritime Administration”, “maritime law enforcement agencies”, ship masters, and shipping companies/shipping associations. Every section was designed to address particular aspects of technology impact on operations, security, and compliance in these fields. A Likert format was used effectively that not only allowed the participants to record their level of approval or disapproval with the statements, but it also made it easy to quantify the data collected as was needed for accurate analysis and understanding. This approach was meant to achieve validity and reliability of data in order to address the research objectives.

3.7 Data Collection Procedures

Data gathering was carried out to acquire views from important players within the marine sector for this study on the role of technology in maritime security. Data was gathered from “administrative officers”, enquire about their views on the formulation of policies and the implementation of regulations from those in charge of the overall administration and the necessary legal frameworks for marine security. Furthermore,

persons from “officers enforcing national maritime legislation” such as coast guard, navy, maritime security agency and marine police were recruited to capture experience in the use of technologies in protecting the maritime areas. profitable completed the survey and focused on the functionality of these tools within their group (Bradbury-Jones *et al.*, 2022).

Moreover, data collection entailed other sea-based employees, including shipmasters, org members from shipping organizations and members from shipping associations task with operational responsibilities of shipping. Their contribution was useful in making establishate the practical issues and the as-is usage of technology in maritime security (Daniel Brown *et al.*, 2023). To capture diverse viewpoints at the various function levels across the purposively selected institutions, structured interviews were combined with semi-structured interviews and focus group interviews Surveys were used along with interviews with the views of different hierarchal levels in the organized institutions included in the study, in focus group conversations that are easy to understand and the big picture Regarding developing the model for the function of technology in marine safety.

3.8 Data Analysis

First, they automatically created frequencies to describe the sample’s response pattern and the trends of attitudes toward prevailing maritime security perceptions and the place of technology in it. Since the study employed closed-ended survey questions, frequency and percentage distributions were computed for each survey question to capture the common viewpoints and to provide an appraisal of what people in general held.

The author conducted a statistical assessment of the acquired data by using a one sample chi square test. This test was performed to see if observed frequencies in the

categorical data substantially deviated from predicted frequencies, hence validating the prevalence of certain attitudes and concerns surrounding marine security technologies. These analyses were conducted using IBM SPSS software due to the precision with which the data could be handled and the accuracy of the statistical significance. This analysis provides insights which make a more nuanced contribution to the understanding of the perceived role and effect of technological advances in maritime security across respondent categories.

3.9 Research Design Limitations

Qualitative approach suits this study to explore perspectives of maritime security, however, limitations regarding this approach are relevant to the generalizability of the findings. The first is that convenience sampling method used to identify participants was practical for targeting professionals in maritime security, but it also was subject to sampling bias, as participants were chosen on the basis of availability and willingness, rather than a true random sampling. Also, it might be hard to apply the results to the whole maritime security community because of this.

Furthermore, the quantitative analysis employed by adhering to the one sample chi square test and frequency percentages analysis on IBM SPSS, principally produce descriptive rather than inferential conclusions. While effective in delineating common viewpoints, these methods do not necessarily correspond to the interaction between maritime security and technology in a statistically robust way.

However, not only do the relatively small, intended sample of 100 respondents provide a variety of viewpoints, but we may lack the statistical power of the analysis, making definitive conclusions difficult. Additionally, self-reported data collected through the questioning may experience response bias in that the participants will attempt to answer in a way that best reflects them in their professional context.

3.10 Conclusion

The perspectives of maritime security experts on the role of technology in enhancing security measures were investigated in this qualitative study. Administrative officers, maritime enforcement officers and ship crew members were consulted on behalf of insights by designing and distributing three sets of tailored questionnaires. There was intentionality in the selection of these groups, as these are representative of diverse levels and roles of technological application throughout the maritime sector. Through IBM SPSS, the data obtained in the study were analyzed using descriptive statistics, one sample chi square test and frequency per cent analysis to summarize and interpret the collected data. By using the convenience sampling method, we had access to relevant participants on hand; however, it also had limitations such as sampling bias and its incomplete generalizability. However, the methodology selected provided some insights and facilitated clearer understanding on how technology is perceived and used in the maritime security landscape. The study's purpose of making a useful contribution to the field is supported by this methodological approach, which also lays a foundation for future work using larger, more randomized samples and more sophisticated statistical techniques for broader application.

CHAPTER IV:

RESULTS

4.1 "Maritime Administration"

Reliability

Table 4.1: Reliability Statistics

"Cronbach's Alpha"	"No. of Items"
.815	33

According to table 4.1 above, the reliability analysis's 33 items have a high level of internal consistency, as shown by their "Cronbach's Alpha of 815". This implies that the elements repeatedly measure the same underlying concept or idea.

Frequency Table

Table 4.2: Is your country a signatory to? (UNCLOS)

	"Frequency"	"Percent"
"Yes"	"38"	"95.0"
"No"	"2"	"5.0"
"Total"	"40"	100.0

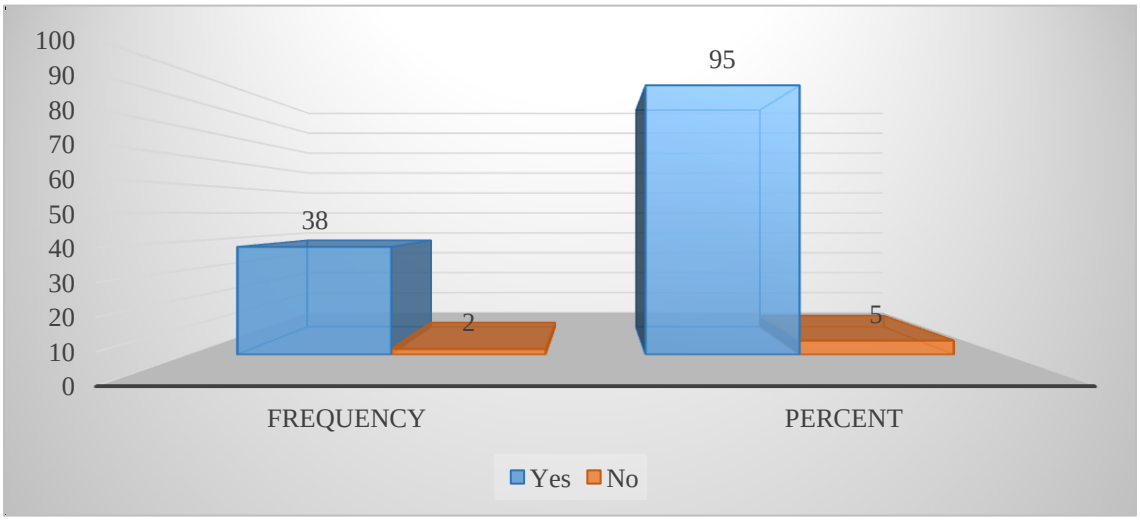


Figure 4.1: Is your country a signatory to? (UNCLOS)

The above Figure 4.1 shows the data on the respondent countries' status as signatories to the (UNCLOS). Meanwhile, 95.0% confirmed that their country is a signatory to UNCLOS, while (5.0%) indicated that their country is not a signatory.

Table 4.3: Is your country a signatory to? (SOLAS)

	"Frequency"	"Percent"
"Yes"	30	75.0
"No"	10	25.0
"Total"	40	100.0

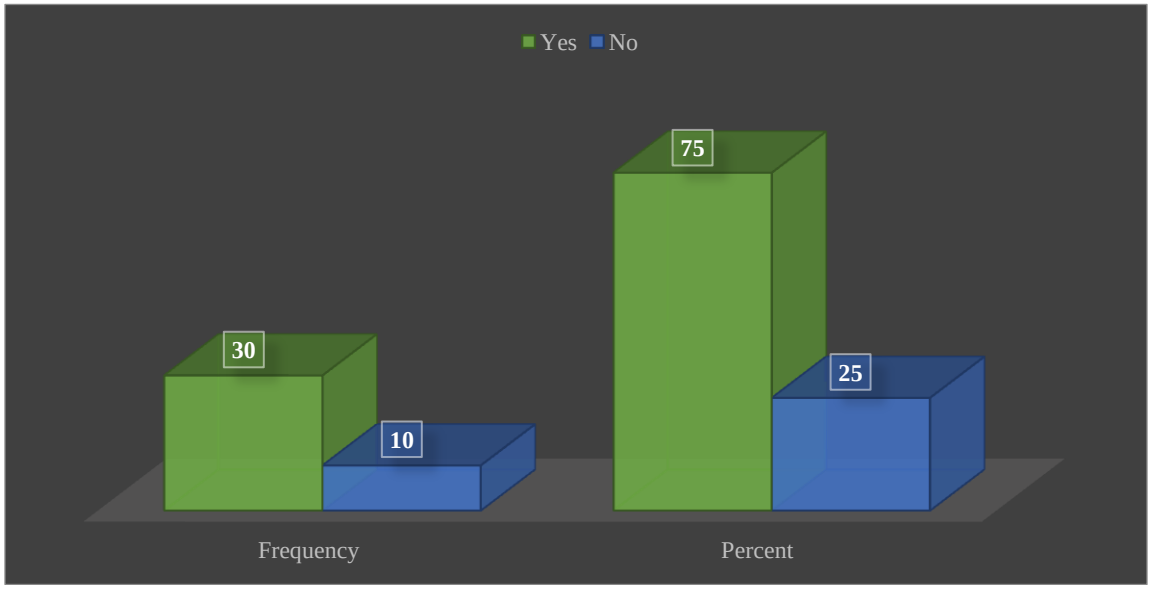


Figure 4.2: Is your country a signatory to? (SOLAS)

According to Figure 4.2, 75% of respondents are from nations that have ratified "the International Convention for the Safety of Life at Sea (SOLAS)", whereas 25% are not.

Table 4.4: Is your country signatory to? (SUA)

	"Frequency"	"Percent"
"Yes"	"33"	"82.5"
"No"	"7"	"17.5"
"Total"	"40"	"100.0"

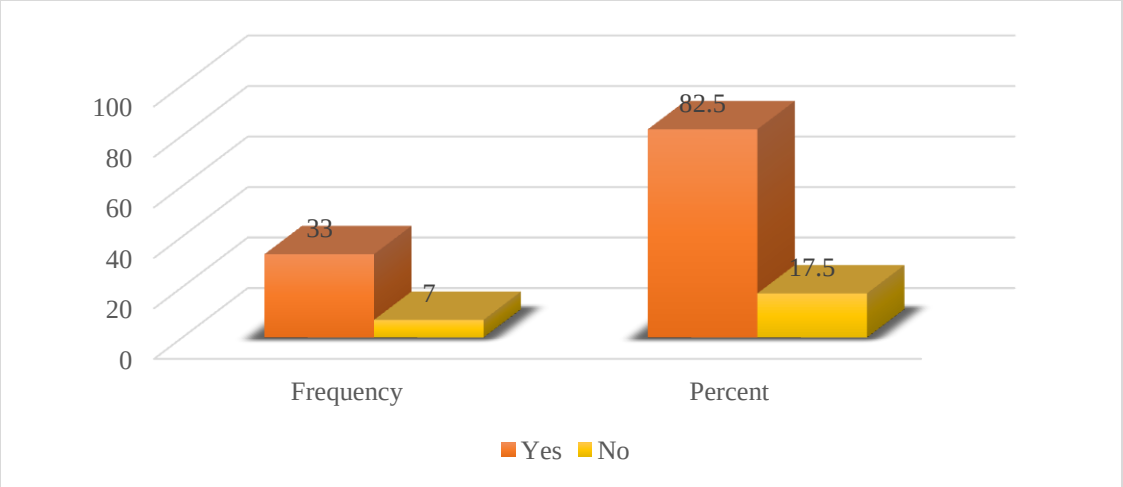


Figure 4.3: Is your country signatory to? (SUA)

Figure 4.3 shows that In contrast to 17.5% of respondents, 82.5% of respondents stated that their nation was a signatory to the "Suppression of Unlawful Acts" Convention (SUA) in opposition to the “Safety of Maritime Navigation”.

Table 4.5: Is your country a signatory to? (STCW)

	“Frequency”	“Percent”
“Yes”	“35”	“87.5”
“No”	“5”	“12.5”
“Total”	“40”	“100.0”

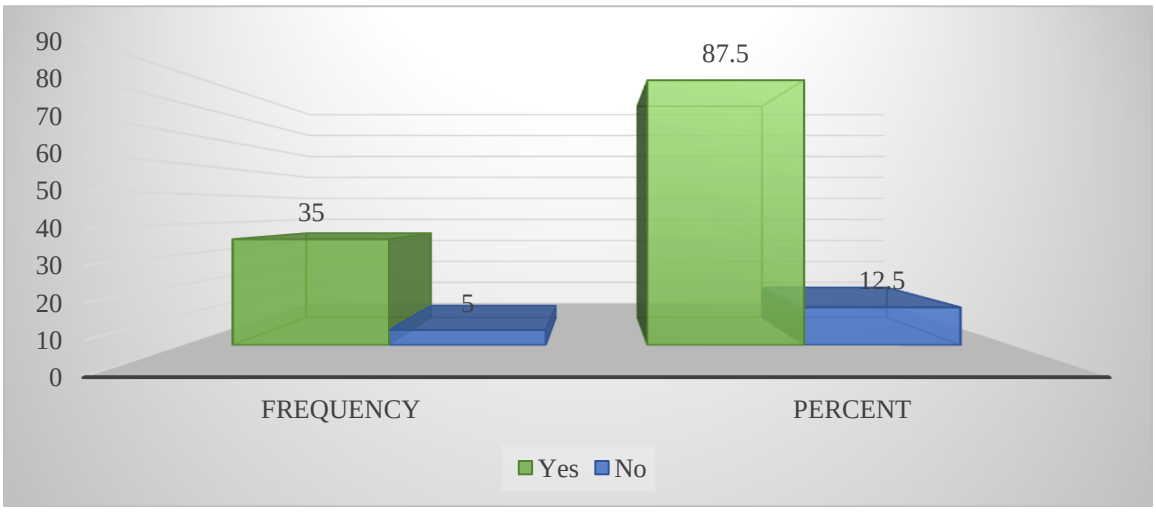


Figure 4.4: Is your country a signatory to? (STCW)

The majority of respondents—87.5%—are satisfied with the distribution of nations that have signed the International Convention on (STCW), as shown in Figure 4.4 above. whereas 12.5%, said their nation is not.

Table 4.6: Is your country signatory to? (ILO Convention 2.185[Sea farers Identity Document (SID)])

	"Frequency"	"Percent"
"Yes"	"30"	"75.0"
"No"	"10"	"25.0"
"Total"	"40"	"100.0"

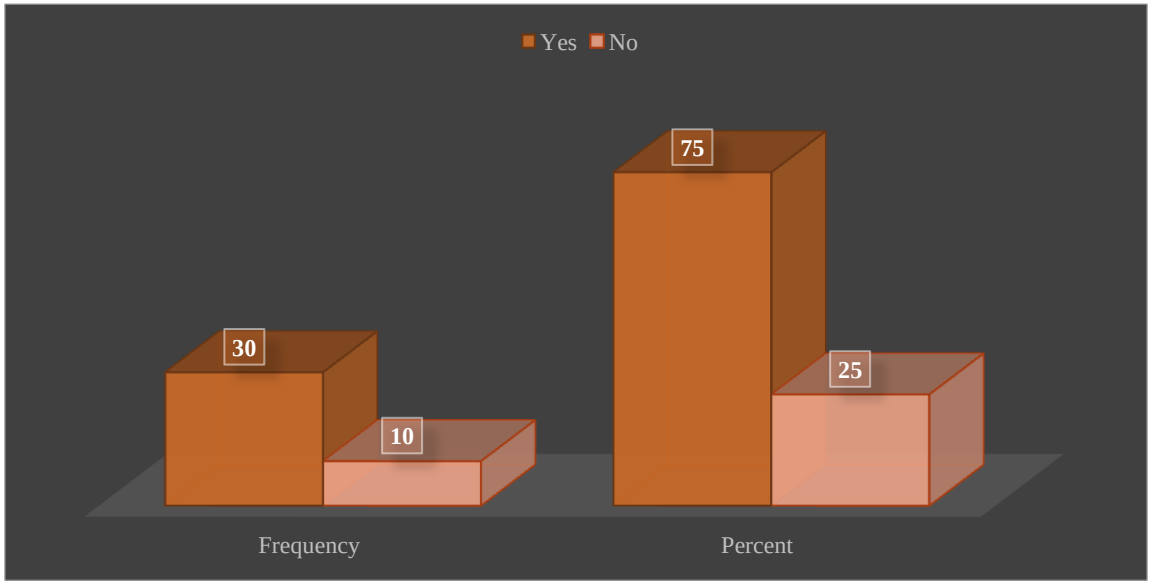


Figure 4.5: Is your country signatory to? (ILO Convention 2.185[Sea farers Identity Document (SID)])

Figure 4.5 demonstrates that most countries have signed ILO Convention 2.185 on Seafarers' Identity Documents (SID), with 75% of respondents holding a signatory status and 25% not.

Table 4.7: Do you think that improving maritime security is necessary in the current situation?

	"Frequency"	"Percent"

“Yes”	“34”	“85.0”
“No”	“6”	“15.0”
“Total”	“40”	“100.0”

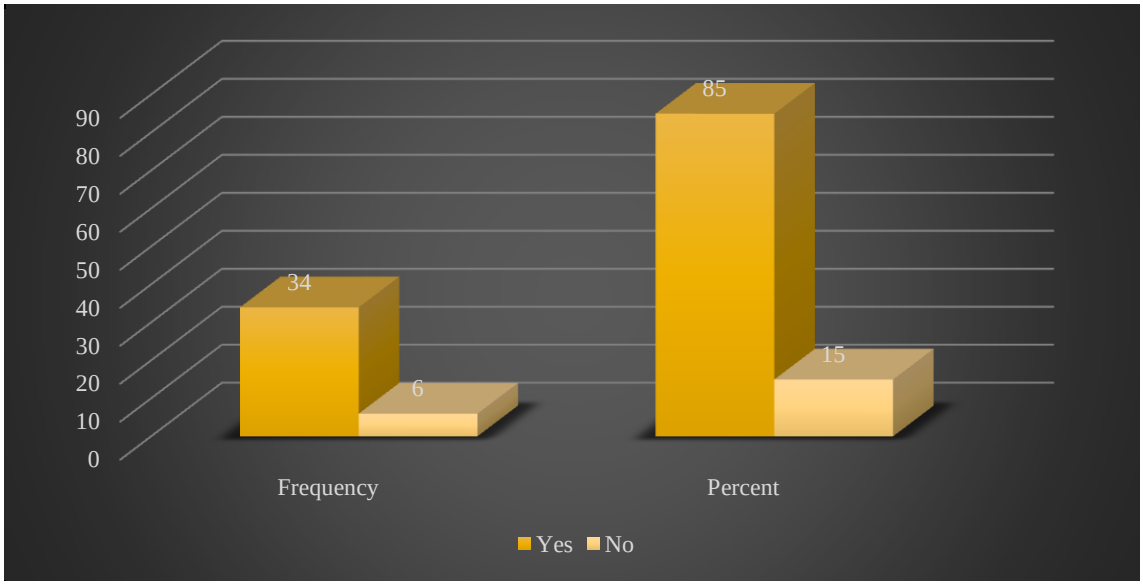


Figure 4.6: Do you think that marine security has to be improved in the current situation?

Figure 4.6's distribution demonstrates that, under the current circumstances, 85% of respondents think that maritime security has to be improved, while 15% disagree. The results reveal that 99% of the respondents approve measures aimed at enhancing marine safety.

Table 4.8: What do you think is the biggest threat to the marine industry?

	Frequency	Percent
“Piracy and Armed Robbery Against Ships”	13	32.5
“Maritime Drug Trafficking and Terrorism”	13	32.5
Illegal Migration	8	20.0

Stowaways	3	7.5
Human Trafficking	2	5.0
Container Crimes	1	2.5
Total	40	100.0

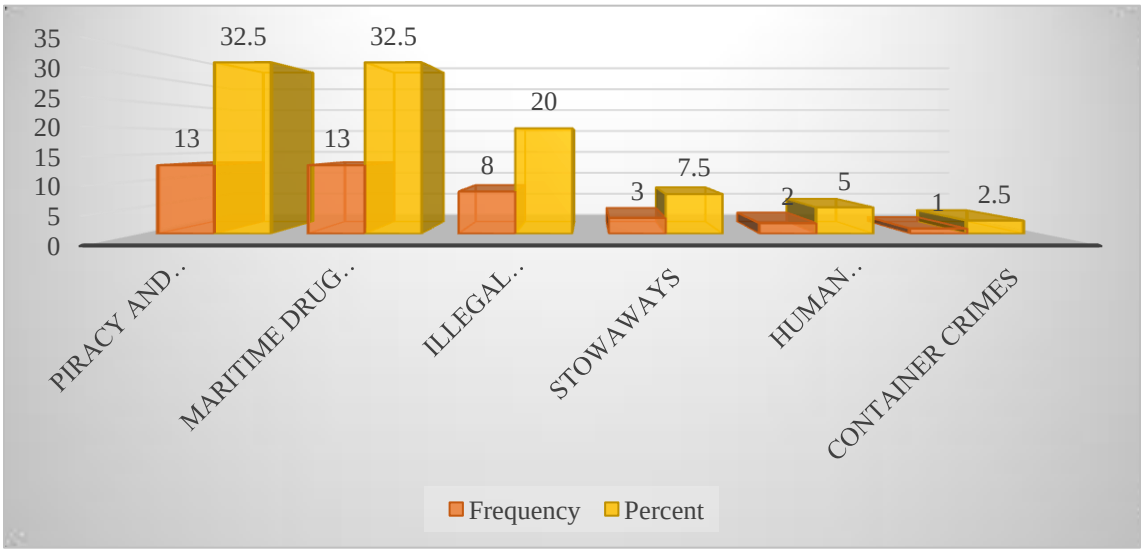


Figure 4.7: Which criminal activity do you think is the biggest threat to the marine industry?

Figure 4.7 reveals that the top three threats to the marine sector, As per 32.5 percent of the respondents, it consists of terrorism, drug trafficking through water, armed robbery against ships, and piracy. Twenty percent of people surveyed ranked illegal immigration as the second most serious problem, behind stowaways at 7.5%, human trafficking at 5%, and container crimes at 2.5%.

Table 4.9: Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?

	"Frequency"	"Percent"
"Yes"	"31"	"77.5"
"No"	"9"	"22.5"
"Total"	"40"	"100.0"

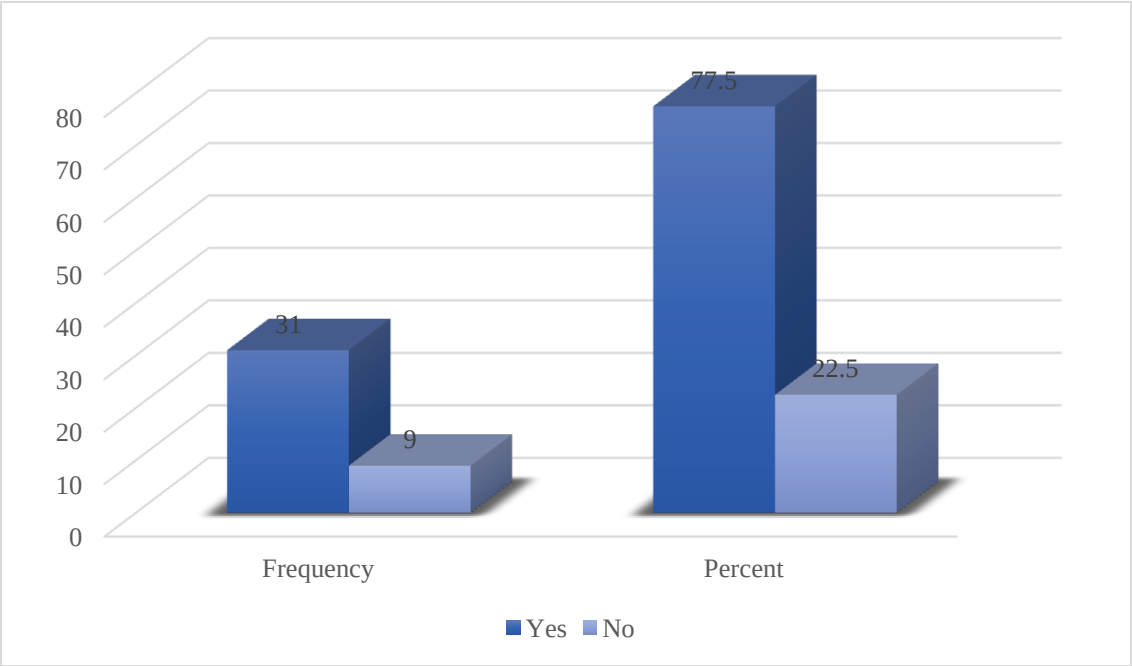


Figure 4.8: Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?

Figure 4.8 demonstrates that in regards to the "International Maritime Organisation" (IMO) and its efforts to prevent maritime crimes, 77.5% of respondents think these measures are sufficient, while 22.5% disagree.

Table 4.10: Is the maritime security in ports, anchorage areas, and ships outside of port authority handled by the same organisation under your "Flag Administration"?

	"Frequency"	"Percent"
"Yes"	"28"	"70.0"
"No"	"12"	"30.0"
"Total"	"40"	"100.0"

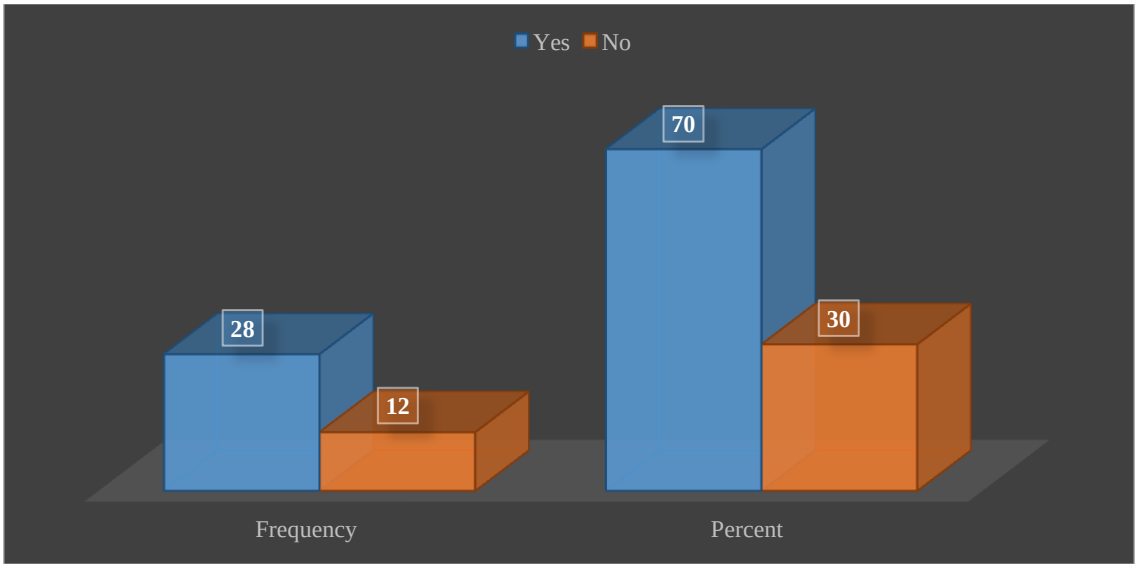


Figure 4.9: Is your "Flag Administration" the same organisation in charge of maritime security for ships outside of port jurisdiction, anchorage zones, and ports?

Figure 4.9 displays the results: 70% of respondents believe that their "Flag Administration" is responsible for marine security at ports, anchorage areas, and ships outside of port authority, whilst 30% believe that other authorities are not.

Table 4.11: How often does the marine administration communicate with law enforcement regarding maritime security issues?

	Frequency	Percent
"Daily basis"	8	20.0
"Weekly basis"	14	35.0
"Monthly basis"	12	30.0
"Quarterly basis"	3	7.5
"Half basis"	2	5.0
"Yearly basis"	1	2.5
Total	40	100.0

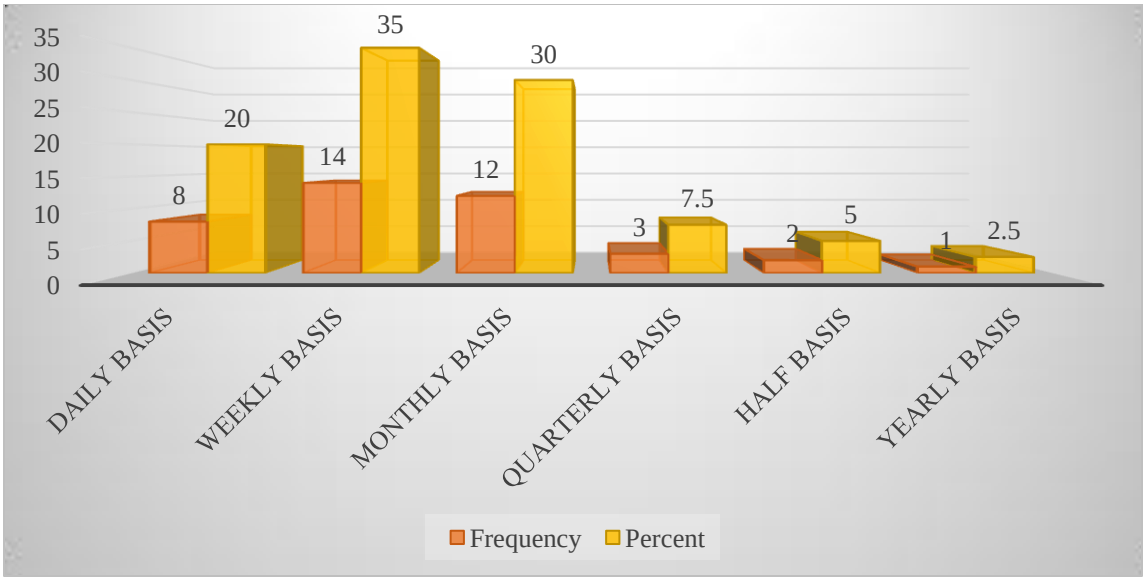


Figure 4.10: How often does the marine administration communicate with law enforcement regarding maritime security issues?

According to what was said before, Figure 4.10 displays the frequency with which law enforcement agencies and marine administrations communicate with regard to maritime security matters. The majority of respondents interact weekly (35%), followed by monthly interactions (30%). 20% report daily interactions, while smaller percentages interact quarterly (7.5%), half-yearly (5%), or yearly (2.5%). This suggests that "Maritime Administration"s generally engage with law enforcement agencies regularly, with a strong focus on weekly or monthly coordination.

Table 4.12: In what ways do the "Flag Administration" and "maritime law enforcement agencies" exchange the following data? (Requirement basis)

	Frequency	Percent
"Ship Reporting"	24	60.0
"AIS"	13	32.5
"Ship entering/leaving ports"	3	7.5
Total	40	100.0

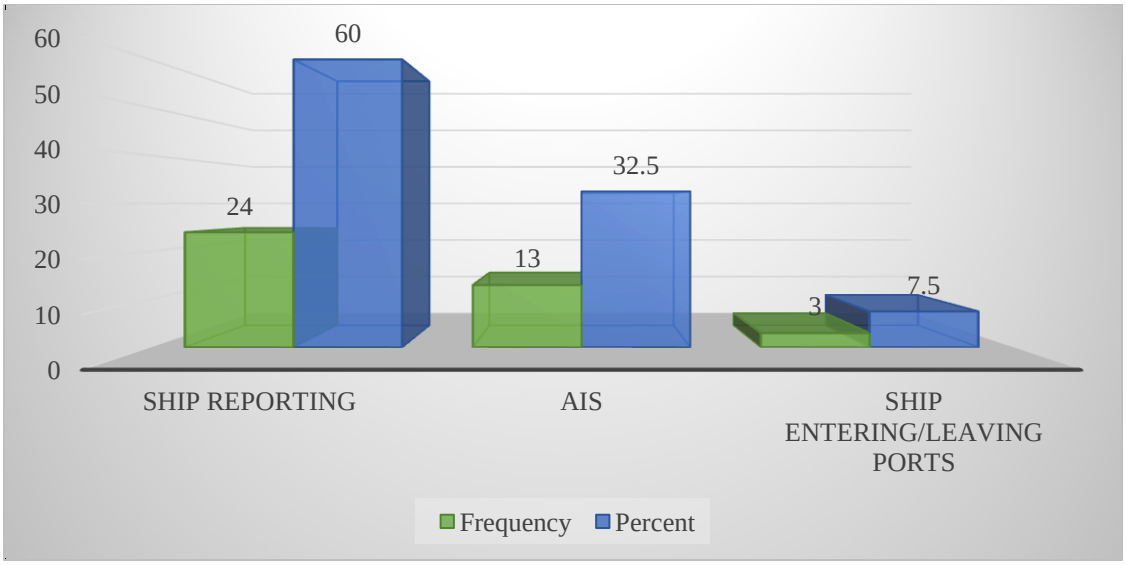


Figure 4.11: How are the maritime law enforcement agency and the "Flag Administration" sharing the information below? (On the basis of requirements)

Figure 4.11 illustrates the data sharing process between "maritime law enforcement agencies" and "Flag Administration"s based on the requirements mentioned above. Sixty percent of people who took the survey said that ships exchange their reporting data, with 32.5 percent saying that AIS data is also shared. Data regarding ships arriving or departing ports is provided, according to only 7.5% of respondents.

Table 4.13: In what ways do the "Flag Administration" and "maritime law enforcement agencies" exchange the following data? (Online)

	Frequency	Percent
"Ship Reporting"	19	47.5
"AIS"	10	25.0
"Ship entering/leaving ports"	"11"	"27.5"
"Total"	"40"	"100.0"

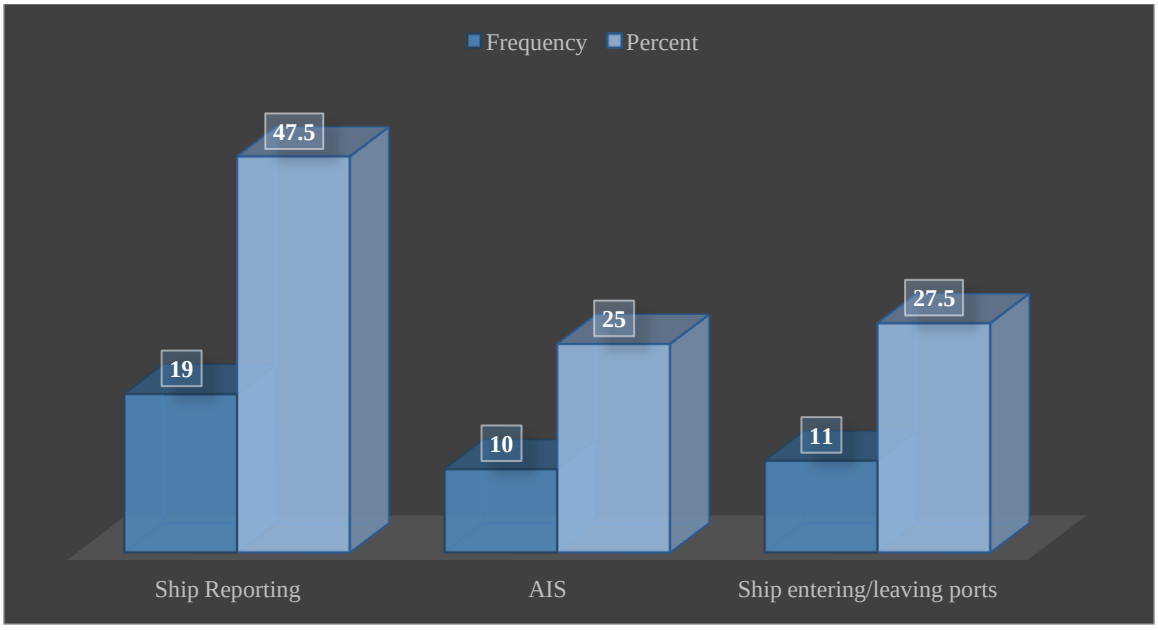


Figure 4.12: How are the maritime law enforcement agency and the "Flag Administration" sharing the information below? (Online)

Figure 4.12 demonstrates the process of online data sharing between marine law enforcement agencies and "Flag Administration" s. Online sharing of ship reporting data is the most popular, with 47.5% of respondents doing this. A quarter of all AIS data is shared online, and 27.5% of all data on ships entering or leaving ports is published online as well.

Table 4.14: In what ways do the "Flag Administration" and "maritime law enforcement agencies" exchange the following data? (2 exchange of data)

	Frequency	Percent
Ship Reporting	17	42.5
AIS	16	40.0
Ship entering/leaving ports	7	17.5
Total	40	100.0

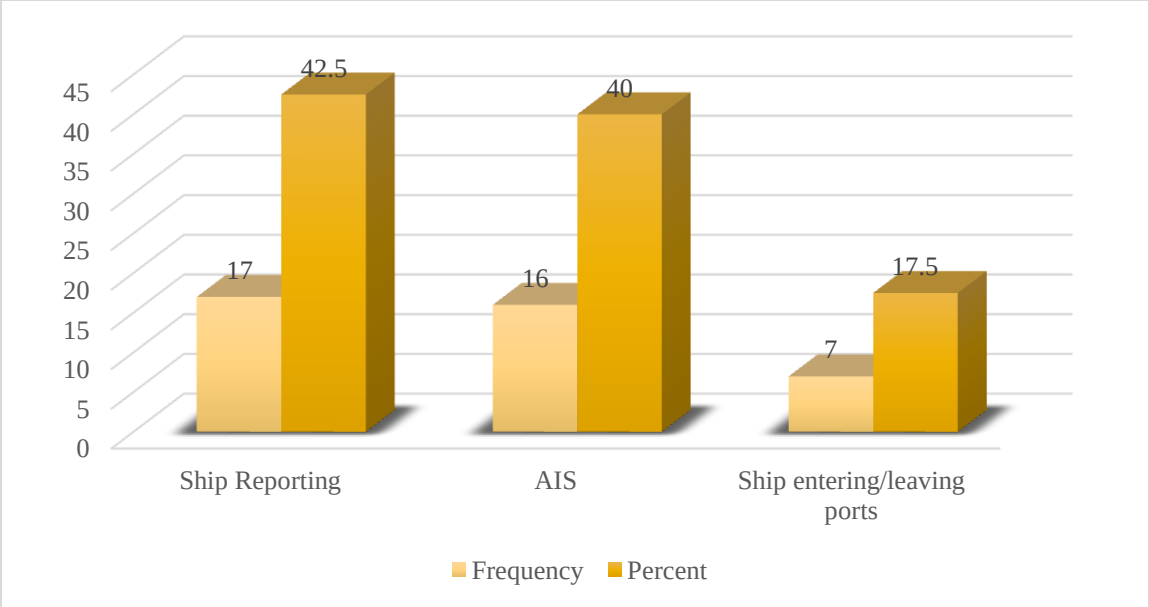


Figure 4.13: In what ways do the "Flag Administration" and "maritime law enforcement agencies" exchange the following data? (2 exchange of data)

The above Figure 4.13 shows how data is exchanged between "Flag Administration" and "maritime law enforcement agencies" through a two-way exchange. Ship reporting data is most commonly exchanged, with 42.5% of respondents indicating this practice. AIS data is exchanged by 40%, while 17.5% the exchange of data on ships entering or leaving ports.

Table 4.15: How do the "Flag Administration" and "maritime law enforcement agencies" exchange the information below? (My County does 2t have the system)

	Frequency	Percent
Ship Reporting	22	55.0
AIS	11	27.5
Ship entering/leaving ports	7	17.5
Total	40	100.0

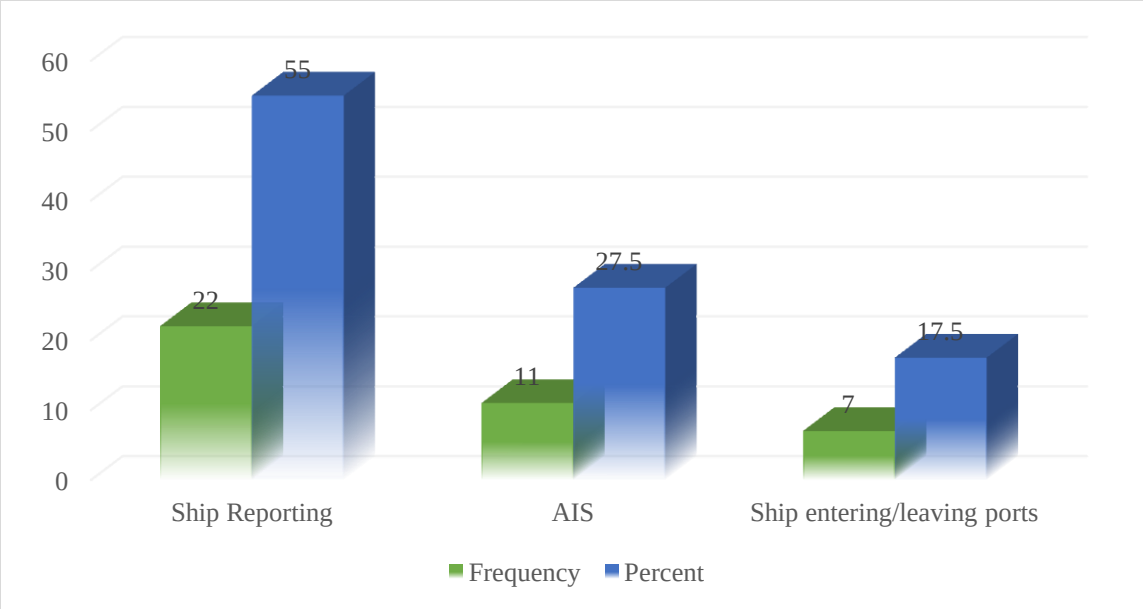


Figure 4.14: How do the "Flag Administration" and "maritime law enforcement agencies" exchange the information below? (My County does 2t have the system)

Figure 4.14 demonstrates the process by which countries without the system share data with maritime law enforcement authorities and "Flag Administration"s. The ship reporting system is the most prevalent one that is missing, according to 55% of responders (22 out of 40). AIS data is absent in 27.5% (11 out of 40), and 17.5% (7 out of 40) reported the absence of a system for tracking ships entering or leaving ports.

Table 4.16: Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? (Ports)

	"Frequency"	"Percent"
"Yes"	"34"	"85.0"
"No"	"6"	"15.0"
"Total"	"40"	"100.0"

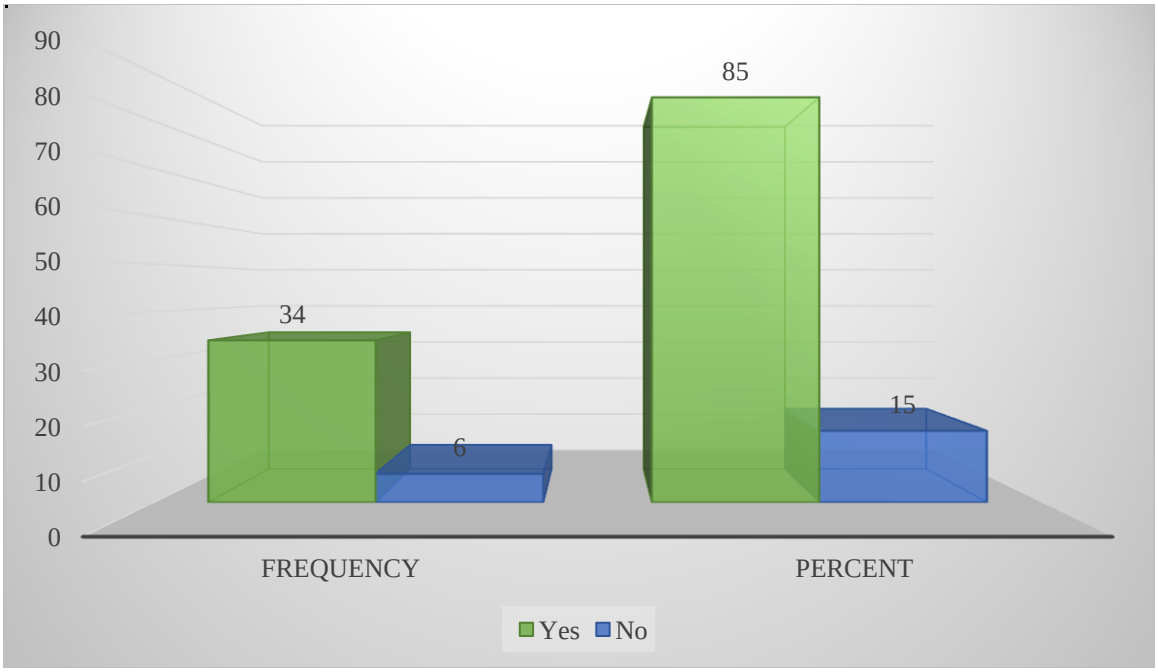


Figure 4.15: Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? (Ports)

As shown in Figure 4.15, the majority of the technology mandated by various IMO instruments effectively enhances maritime security in ports, whereas a small percentage fails to do so. This indicates a strong positive perception of the effectiveness of IMO-recommended technologies in enhancing port security.

Table 4.17: Does the maritime sector indicated below benefit from the tech2logy mandated by several IMO instruments in terms of promoting maritime security? (Ships)

	"Frequency"	"Percent"
"Yes"	"33"	"82.5"
"No"	"7"	"17.5"
"Total"	":40"	"100.0"

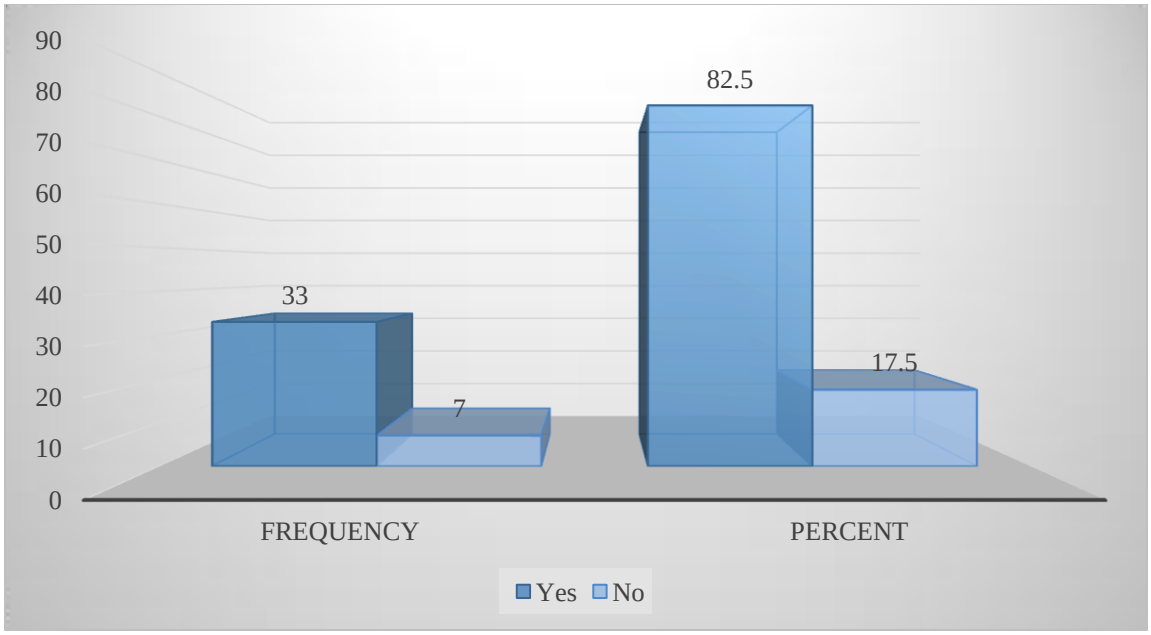


Figure 4.16: Does the maritime sector indicated below benefit from the tech2logy mandated by several IMO instruments in terms of promoting maritime security? (Ships)

Figure 4.16 demonstrates that about 82.5 percent of people think the technology mandated by various IMO instruments is good at making ships safer at sea, whereas 17.5 percent think otherwise.

Table 4.18: Does the "tech2logy" mandated by various IMO treaties effectively promote maritime security in the following maritime sector areas? (Other Installations)

	“Frequency”	“Percent”
“Yes”	“29”	“72.5”
“No”	“11”	“27.5”
“Total”	“40”	“100.0”

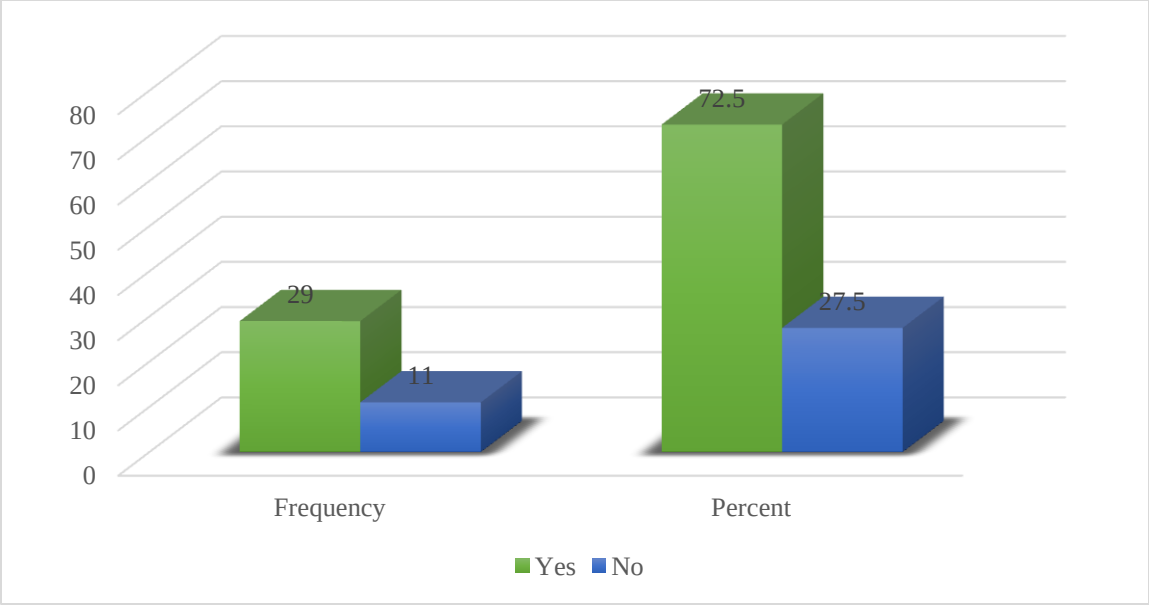


Figure 4.17: Does the "tech2logy" mandated by various IMO treaties effectively promote maritime security in the following maritime sector areas? (Other Installations)

Figure 4.17 shows that while 27.5% of people do not agree, 72.5% believe that the technology mandated by various IMO instruments successfully enhances maritime security at other facilities. This shows that a majority of people believe that technologies recommended by the IMO are useful for improving security at different marine locations.

Table 4.19: In what ways does your organisation encourage employees to adhere to security protocols?

	Frequency	Percent
monetary rewards, such as promotion medals, certificates, or prize money given out of turn, etc.	23	57.5
Recognition in public, by insignia or than above	15	37.5
Other incentives Mentioned response	2	5.0
Total	40	100.0

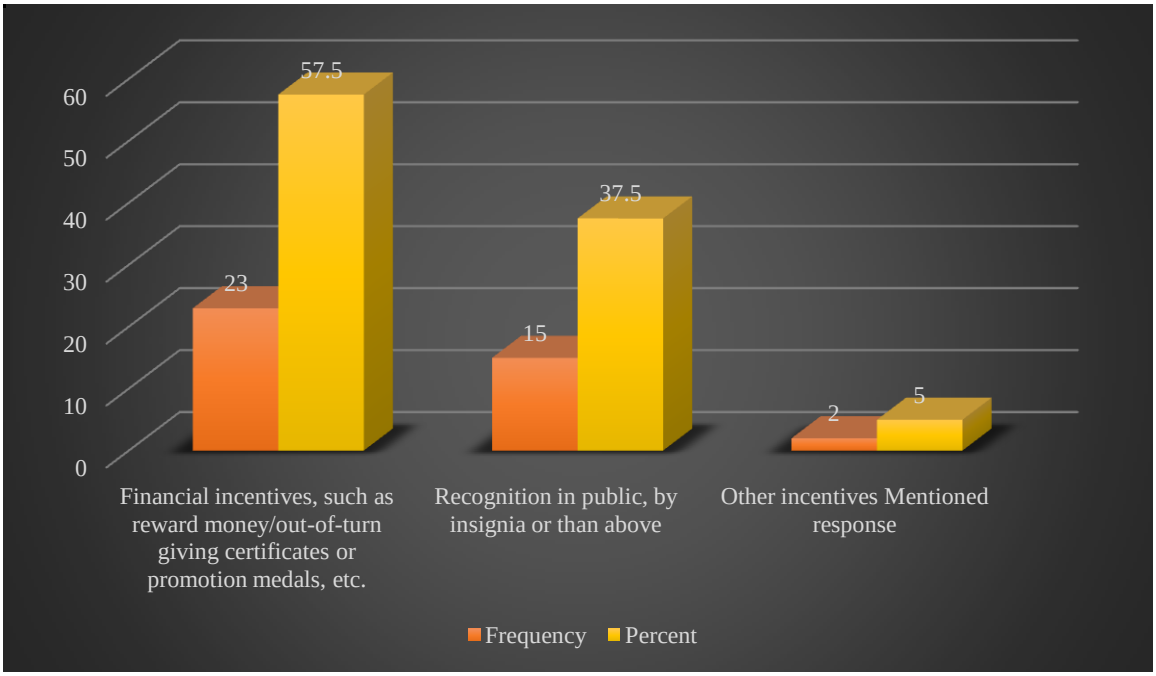


Figure 4.18: In what ways does your organisation encourage employees to adhere to security protocols?

As illustrated in Figure 4.18, the organisations incentivise their employees to adhere to security protocols. Money, out-of-turn certificates, or promotion medals are the most common forms of monetary incentives, according to 57.5% of respondents. 37.5% mentioned recognition in public, through insignia or other means, as a motivating factor. Only 5% cited other incentives.

Table 4.20: Do your flagships currently have enough personnel on board to meet security requirements?

	Frequency	Percent
"Yes"	31	77.5
"No"	9	22.5
Total	40	100.0

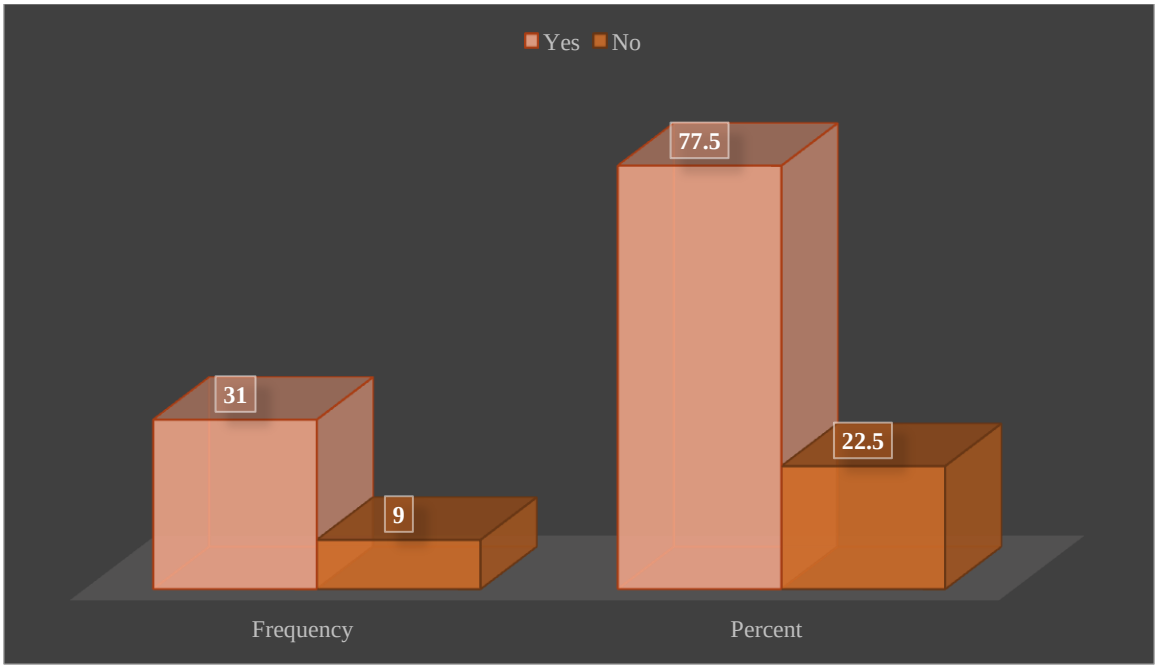


Figure 4.19: Do your flagships currently have enough personnel on board to meet security requirements?

You can see the distribution in Figure 4.19 up there. While 22.5% of respondents disagree, 77.5% think their flagships' present staffing levels are sufficient to meet security laws. It is evident that the majority of people believe that the current staffing numbers are adequate to meet the security needs.

Table 4.21: Current trends indicate that certain flag state administrations issue safe manning certifications without paying enough attention to security standards, onboard administrative tasks, and vessel trading. Considering the current state of global security,

	“Frequency”	“Percent”
“Yes”	“29”	“72.5”
“No”	“11”	“27.5”
“Total”	“40”	“””100.0””

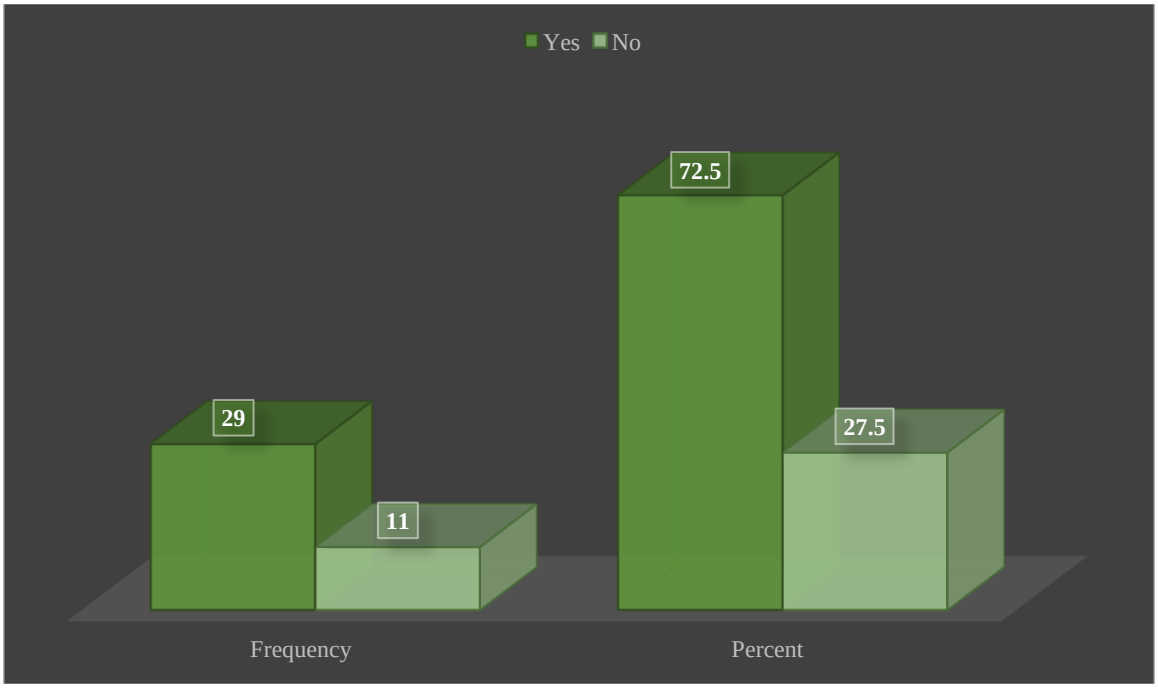


Figure 4.20: Current trends indicate that certain flag state administrations issue safe manning certifications without paying enough attention to security standards, onboard administrative tasks, and vessel trading. Considering the current state of global security,

The administrations continue to issue safe manning certifications without taking into account the administrative work onboard, security needs, and the current state of global security (as mentioned in 4.20). In the meanwhile, 72.5% of people think that some things are true, while 27.5% think otherwise.

Table 4.22: To what extent do you believe the Ship Security Alarm System (SSAS) contributes to maritime security? 2t in warships

	“Frequency”	“Percent”
Effective	“29”	“72.5”
Not Effective	“11”	“27.5”
“Total”	“40”	“100.0”

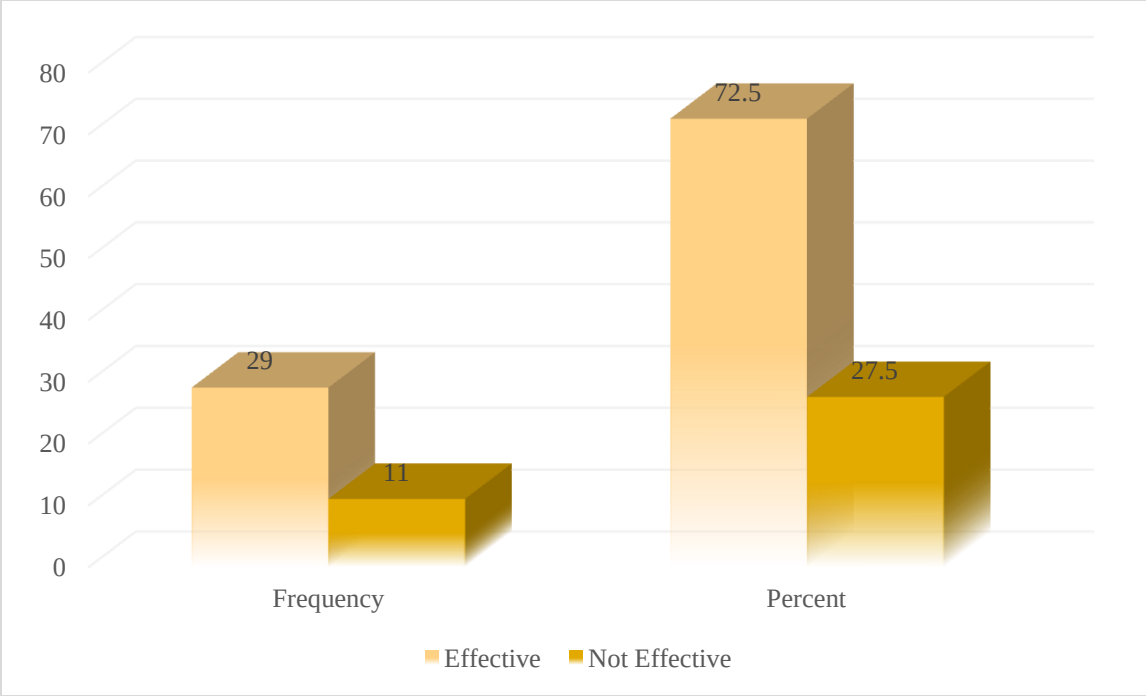


Figure 4.21: To what extent do you believe the Ship Security Alarm System (SSAS) contributes to maritime security? 2t in warships

As can be seen in figure 4.21, the Ship Security Alarm System (SSAS) does a good job of enhancing maritime security aboard warships. According to the majority, 72.5 percent think it works and 27.5 percent don't.

Table 4.23: Have you had to handle a security incident at work?

	"Frequency"	"Percent"
"Yes"	"30"	"75.0"
"No"	"10"	"25.0"
"Total"	"40"	"100.0"

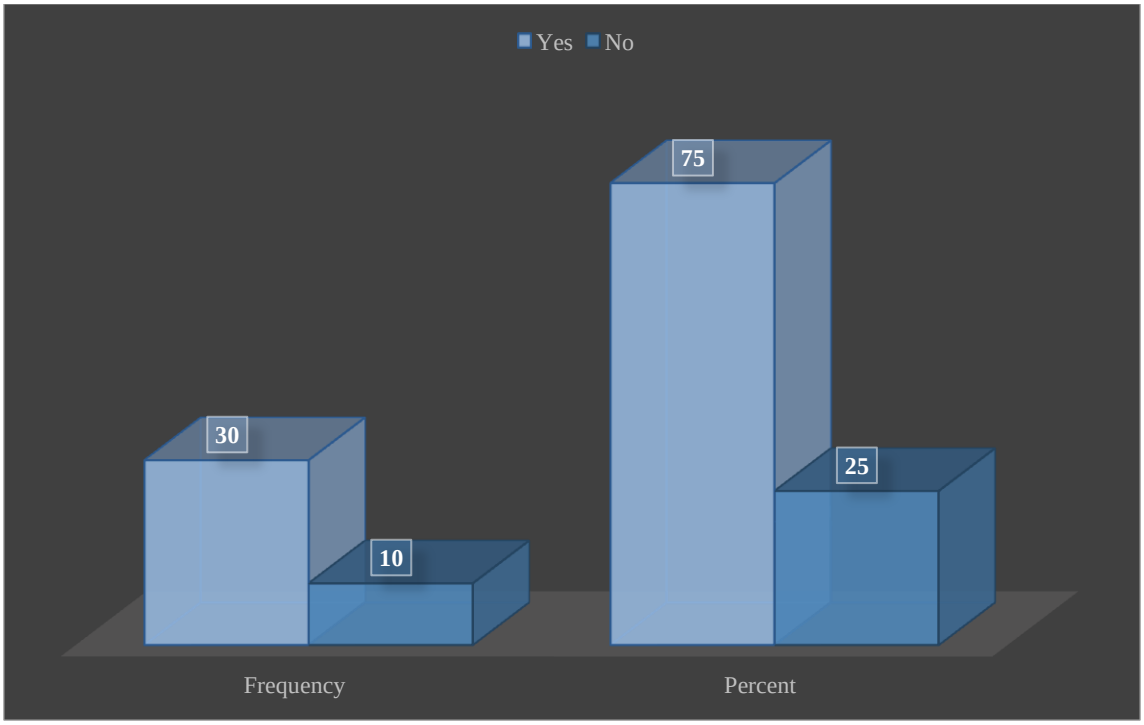


Figure 4.22: Have you had to handle a security incident at work?

As shown in Figure 4.22, 75% of the participants have handled a security incident at work, whilst 25% have not. That most people have dealt with security incidents in the workplace is a strong indicator of that.

Table 4.24: Regarding the aforementioned occurrence or incidents, how would you rank the response of the "Maritime Administration" and "maritime law enforcement agencies"?

	"Frequency"	"Percent"
"Effective"	"23"	"57.5"
"Inadequate"	"17"	"42.5"
Total	"40"	"100.0"

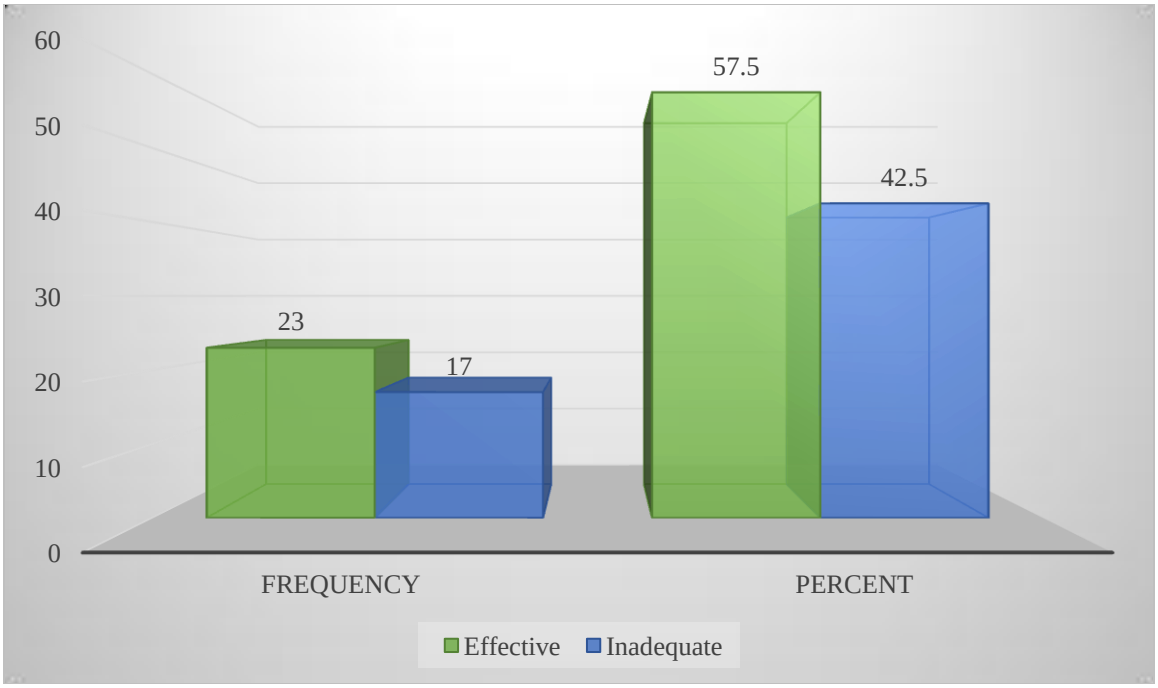


Figure 4.23: Regarding the aforementioned occurrence or incidents, how would you rank the response of the "Maritime Administration" and "maritime law enforcement agencies"?

As seen in Figure 4.23, 57.5% of the reactions to incidents by law enforcement and the "Maritime Administration" are successful in addressing security. But over half (42.5%) felt that the response was not enough (17 out of 40).

Table 4.25: Does the Vessel Traffic System (VTS) promote or hinder security?

	Frequency	Percent
"Effective for security"	32	80.0
"Hindrance for security"	8	20.0
Total	40	100.0

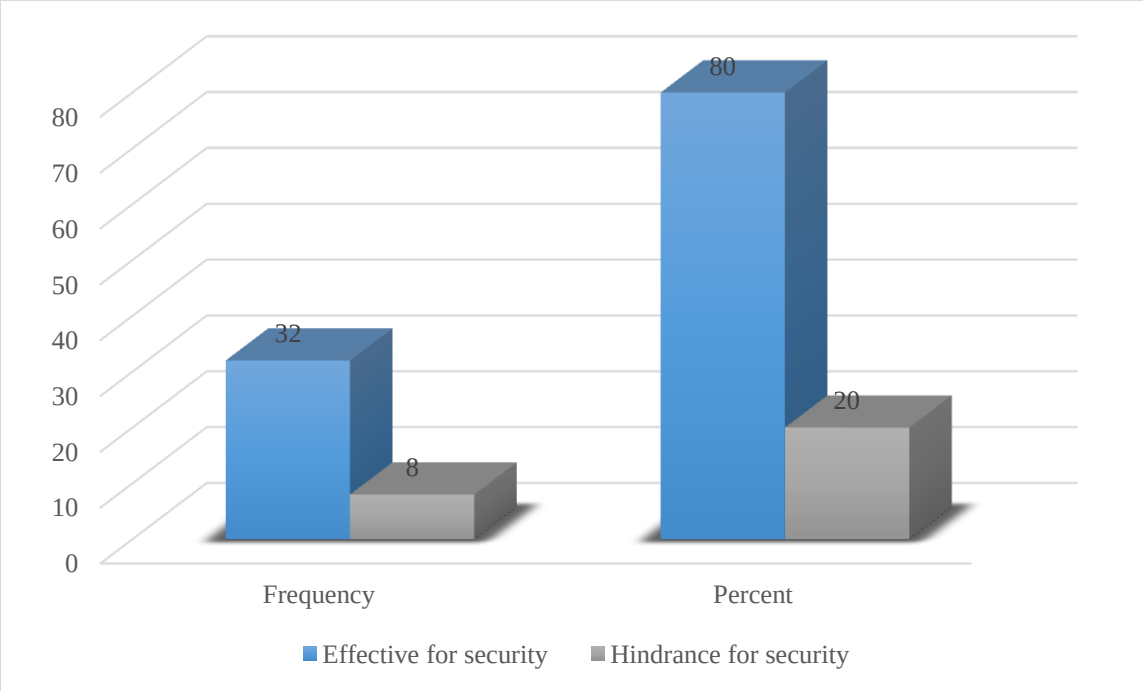


Figure 4.24: Does the Vessel Traffic System (VTS) promote or hinder security?

The Vessel Traffic System (VTS), as seen in figure 4.24, is a practical instrument for enhancing safety. Twenty percent believe it impedes security, whilst 80 percent believe it helps.

Table 4.26: Is VTS an active security threat mitigation strategy or a deterrent?

	"Frequency"	"Percent"
"Deterrent"	"23"	"57.5"
"Active measure"	"17"	"42.5"
"Total"	"40"	"100.0"

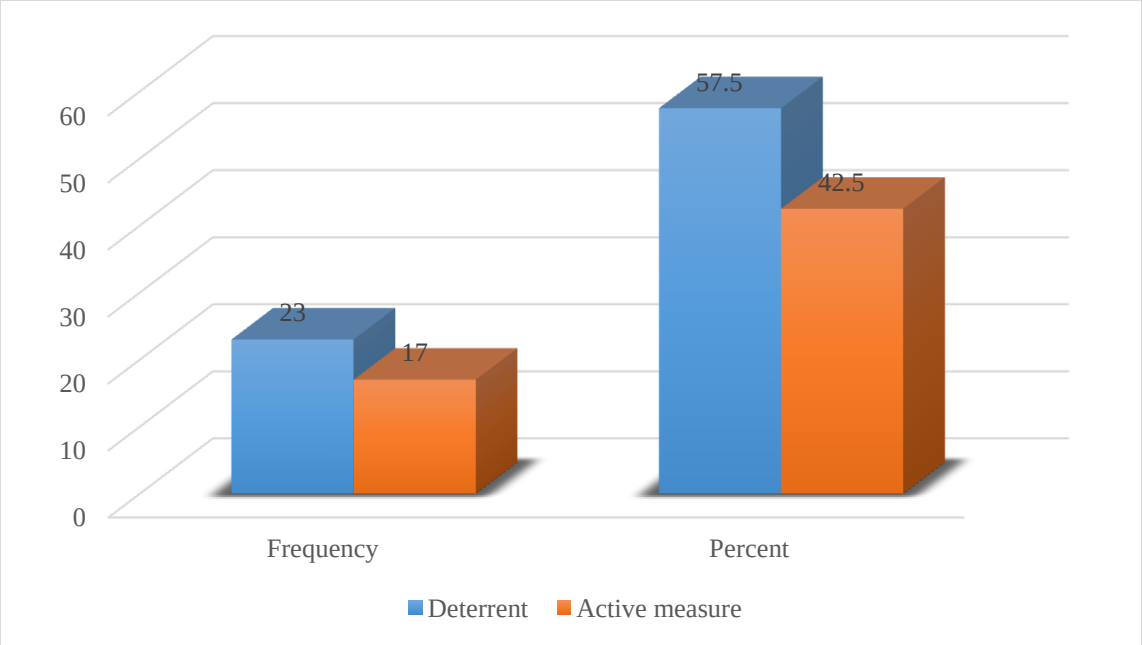


Figure 4.25: Is VTS an active security threat mitigation strategy or a deterrent?

The above Figure 4.25 shows that 57.5% of respondents consider the Vessel Traffic System (VTS) a deterrent for mitigating security threats, while 42.5% view it as an active measure. This shows a slight majority remarks VTS primarily as a preventive measure rather than a direct intervention tool.

Table 4.27: Will the operator's efficiency in identifying and preventing security incidents be improved by radar-AIS interface?

	“Frequency”	“Percent”
“Yes”	“31”	“77.5”
“No”	“9”	“22.5”
“Total”	“40”	“100.0”

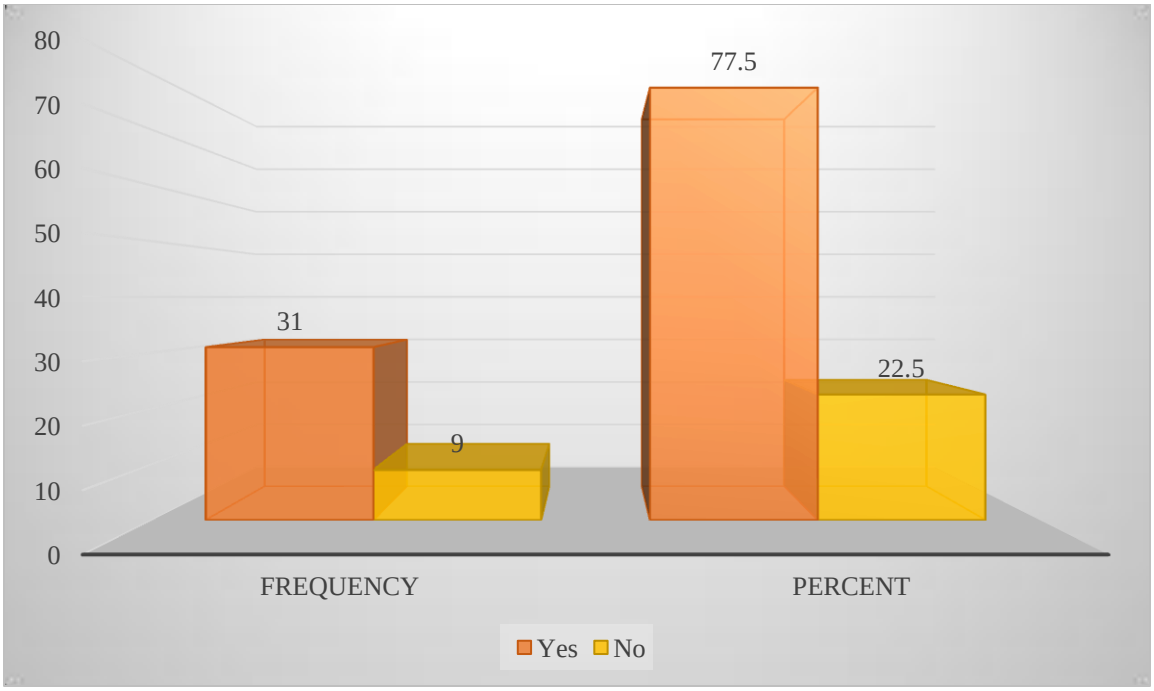


Figure 4.26: Will the operator's efficiency in identifying and preventing security incidents be improved by radar-AIS interface?

Figure 4.26 illustrates that while 22.5% of people don't think that connecting radar and AIS will improve operator efficiency in detecting and preventing security situations early, 77.5% do.

Table 4.28: Will the goal of safe transportation be aided or hindered by "long-range identification and tracking of ships" (LRIT)? Advantage

	Frequency	Percent
"Foster maritime security"	35	87.5
"Will be a hindrance"	5	12.5
Total	40	100.0

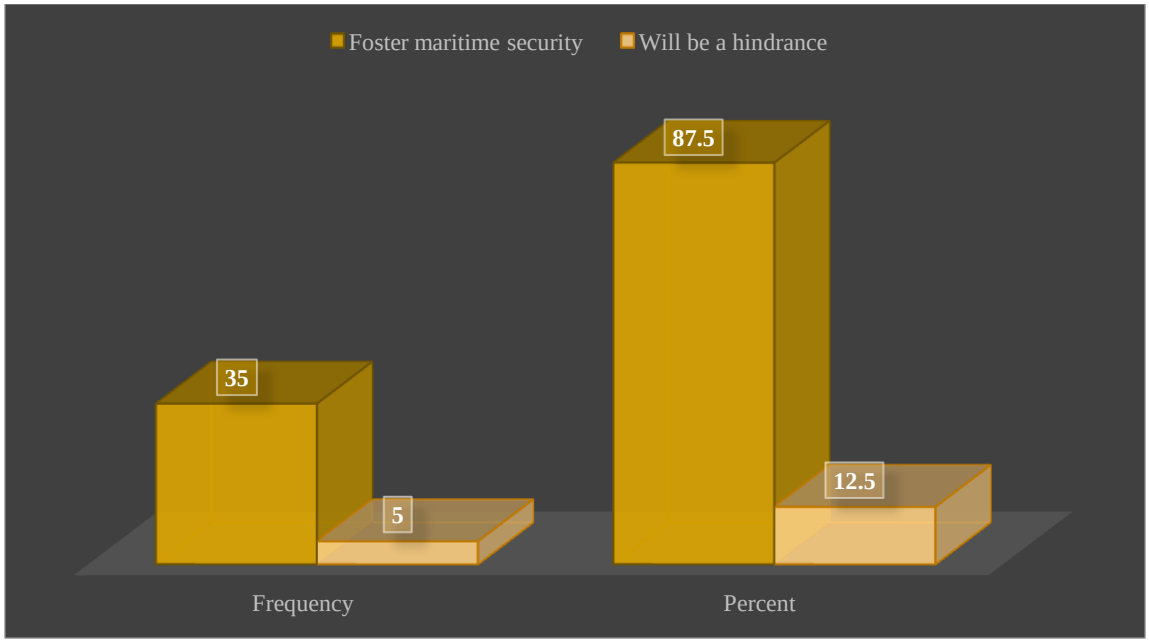


Figure 4.27: Will the goal of safe transportation be aided or hindered by "long-range identification and tracking of ships" (LRIT)? Advantage

Long-range ship tracking and identification (LRIT) promotes marine security, yet 12.5% of respondents see it as a drawback (see figure 4.27 above). 87.5% of respondents say they support marine security. This demonstrates the broad agreement that LRIT is beneficial for accomplishing secure transportation goals.

Table 4.29: Have you ever conducted a security inspection of containers before?

	"Frequency"	"Percent"
"Yes"	"31"	"77.5"
"No"	"9"	"22.5"
"Total"	"40"	"100.0"

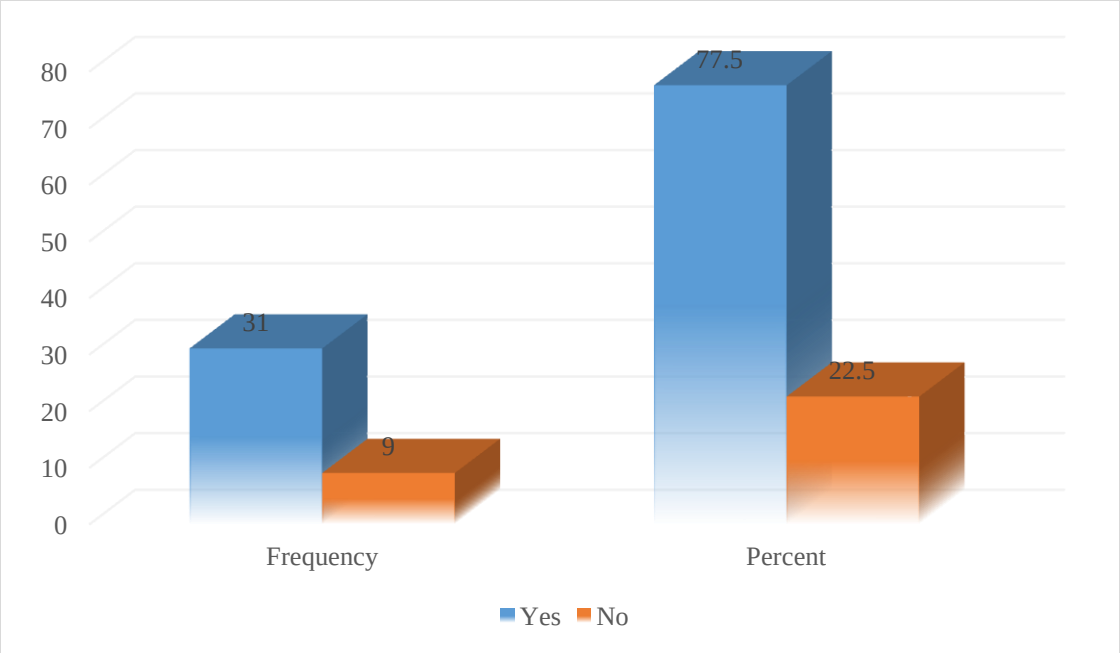


Figure 4.28: Have you ever conducted a security inspection of containers before?

The data in Figure 4.28 demonstrates that 75.5% of the participants have handled container security scanning before, whilst 22.5% had no such experience. That most people are aware of how to scan containers for security is evident from the results.

Table 4.30: What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment?

	Frequency	Percent
"Random scanning"	25	62.5
100% scanning	15	37.5
Total	40	100.0

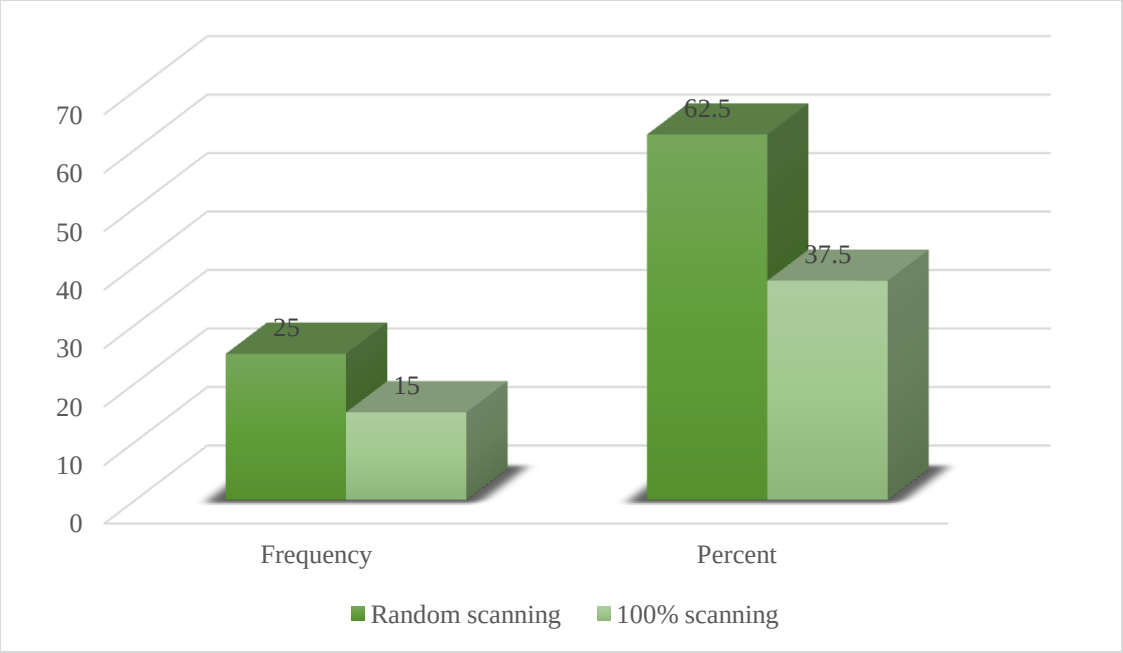


Figure 4.29: What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment?

Figure 4.29 shows the optimal approach to improving marine security, taking into account security threats and the business obligations of ship owners. Sixty-2.5 percent prefer random scanning, whereas 37.5 percent want 100% scanning.

Table 4.31: Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER).

	"Frequency"	"Percent"
"Yes"	"31"	"77.5"
"No"	"9"	"22.5"
"Total"	"40"	"100.0"

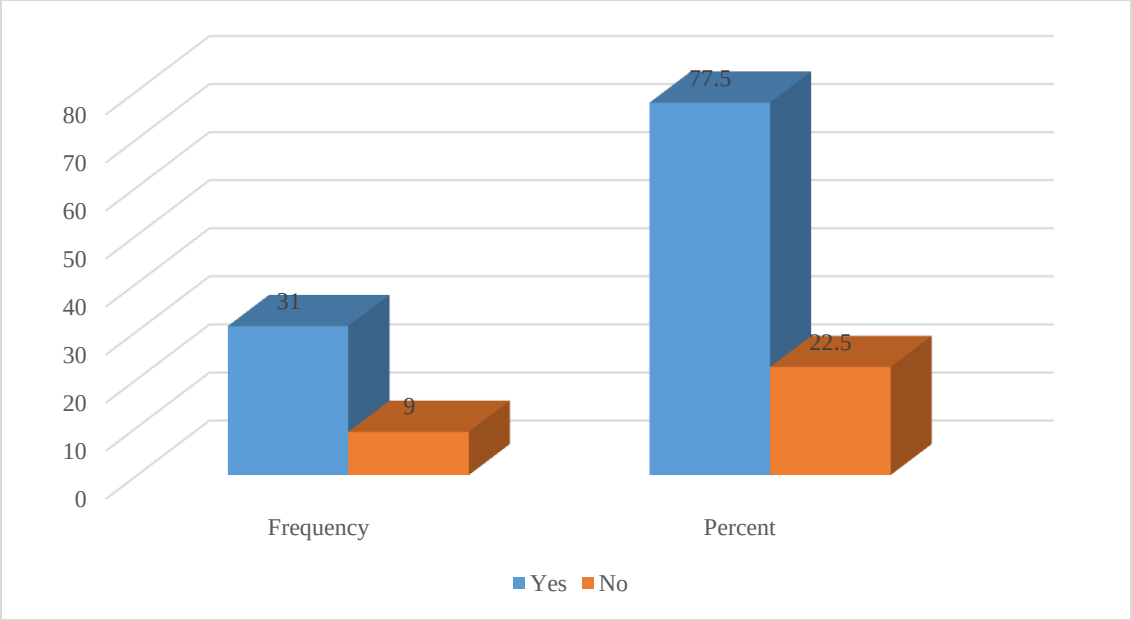


Figure 4.30: Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER).

The above Figure 4.30 shows that 77.5% of respondents are familiar with different global ship reporting systems, such as AMVER, JASREP, and INDSAR, while 22.5% are not.

Table 4.32: Do you think all ships on international journeys should be required to report to one of the global ship reporting systems?

	“Frequency”	“Percent”
“Yes”	“26”	“65.0”
“No”	“14”	“35.0”
“Total”	“40”	“100.0”

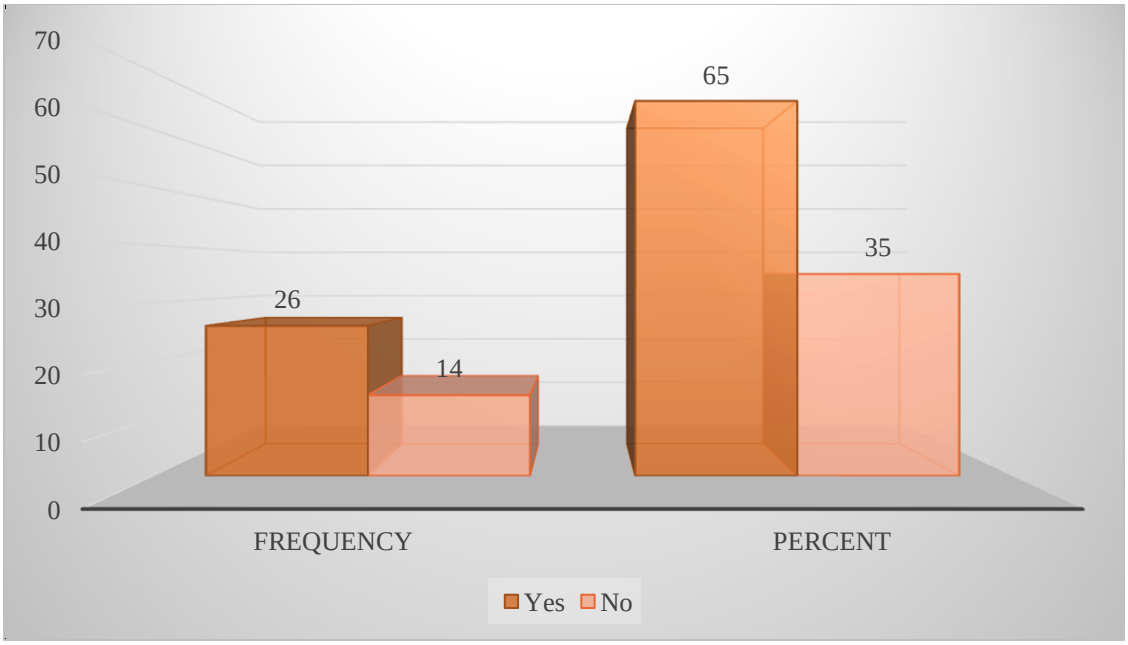


Figure 4.31: Do you think all ships on international journeys should be required to report to one of the global ship reporting systems?

Figure 4.31 illustrates that while 35% of respondents do not think all ships should be required to use a worldwide ship reporting system, 65% of respondents think it should be necessary.

Table 4.33: Does maritime security training benefit from the use of the Vessel Data Recorder (VDR)?

	"Frequency"	"Percent"
Yes"	"28"	"70.0"
"No"	"12"	"30.0"
"Total"	"40"	"100.0"

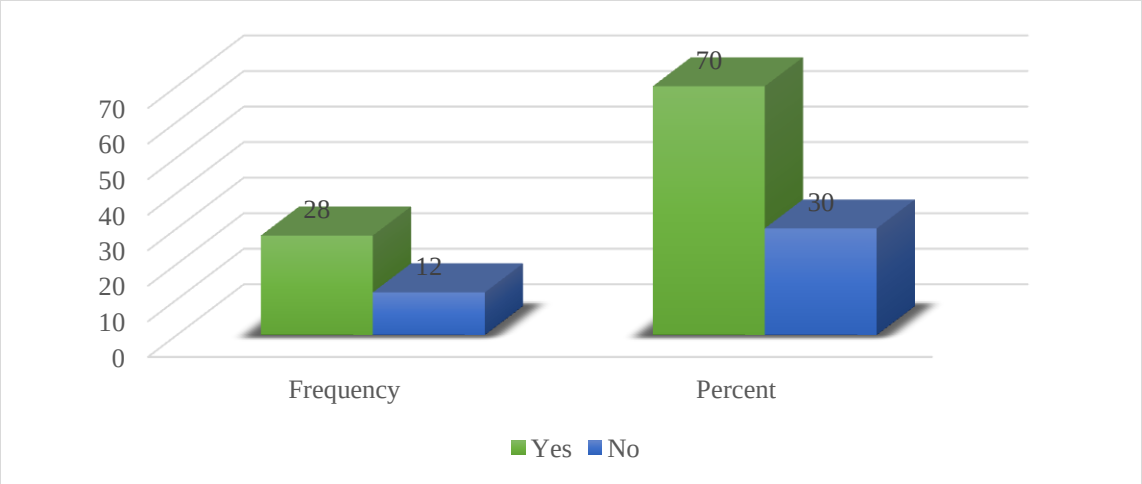


Figure 4.32: Does maritime security training benefit from the use of the Vessel Data Recorder (VDR)?

Figure 4.32, up top, illustrates that while 30% of people think the VDR doesn't contribute to marine security training, 70% think it does.

Table 4.34: In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?

	"Frequency"	"Percent"
"Yes"	"29"	"72.5"
"No"	"11"	"27.5"
"Total"	"40"	"100.0"

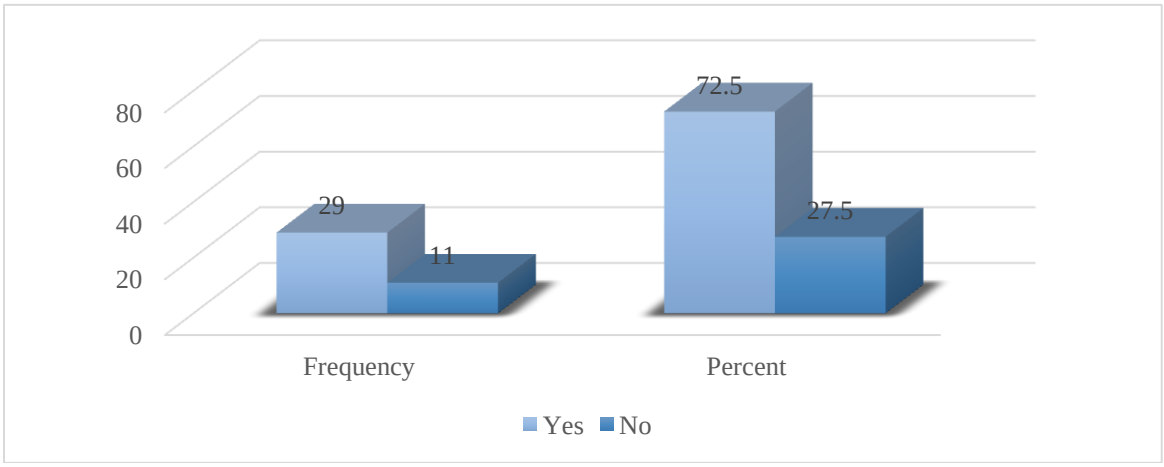


Figure 4.33: In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?

Figure 4.33 demonstrates that out of all the VDRs, 72.5% contribute to maritime security by providing useful data for analysis, while 27.5% do not. This suggests that the vast majority of people think VDR is useful for security-related research in the marine industry.

Logistic Regression

Table 4.35: "Dependent Variable Encoding"

"Original Value"	"Internal Value"
Yes	0
No	1

In this encoding, a response of "Yes" is mapped to 0, and a response of "No" is mapped to 1. This encoding allows for easier use in statistical or machine learning models that require numerical input.

Block 0: Beginning Block

Table 4.36: Classification

			Predicted		
			Is the organisation in charge of marine security in ports, anchorage areas, and ships outside of port jurisdiction also your "Flag Administration"?		Percentage
	Observed		Yes	No	Correct
Step 0	Is your "Flag	Yes	28	0	100.0

	Administration" the same organisation in charge of maritime security for ships outside of port jurisdiction, anchorage areas, and ports?	No	12	0	.0
	Overall Percentage				70.0

a. Constant is included in the model.

b. The cut value is .500

The classification table provides a summary of a model's initial step (Step 0) in predicting responses to the question, "Is the same agency responsible for providing maritime security in ports, anchorage areas, and ships outside port jurisdiction?" In this table, "Observed" represents the actual responses, while "Predicted" shows the model's initial predictions. The model achieved 100% accuracy for this category by properly classifying 28 out of 40 situations where the observed response was "Yes." The model, however, consistently predicted "Yes" erroneously in the 12 instances where the observed response was "No," yielding 0% accuracy for the "No" category. Overall, the model correctly predicted 28 out of 40 cases, yielding a prediction accuracy of 70.0%.

This table suggests that, in its initial step, the model defaults to predicting "Yes" regardless of the actual response, achieving perfect accuracy for "Yes" responses but failing to classify any "No" responses correctly. This pattern often occurs in Step 0 of logistic regression, where the model has not yet applied any complex decision-making criteria and may rely on a baseline classification. As a result, while the model shows a

reasonably high overall accuracy, its predictive power for “No” responses is currently ineffective.

Table 4.37: Variables in the Equation

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 0	Constant	-.847	.345	6.030	1	.014	.429

In Step 0 of this logistic regression model, only the constant term is included, with a coefficient (B) of -0.847. This negative value suggests a lower initial likelihood of a “Yes” outcome when no other predictors are present. The constant’s standard error is 0.345, and its Wald statistic is 6.030, indicating statistical significance ($p = 0.014$), meaning the log-odds differ from zero. The odds ratio (Exp(B)) is 0.429, suggesting that, at this baseline level, a “No” outcome is more likely than “Yes.” This initial model sets the groundwork for further analysis once additional predictors are added.

Table 4.38: Variables not in the Equation

			Score	df	Sig.
Step 0	Variables	Is your country signatory to?	6.234	1	.013
		Does the technology mandated by several IMO treaties effectively promote maritime security in the region?	5.079	1	.024
		Do you think that marine security has to be improved in the current situation?	4.519	1	.034
		Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?	.061	1	.804

		Do your flagships currently have enough personnel on board to meet security requirements?	.061	1	.804
		Current trends indicate that certain flag state administrations issue safe manning certifications without paying enough attention to security standards, onboard administrative tasks, and vessel trading. Considering the current state of global security,	4.353	1	.037
		Have you had to handle a security incident at work?	.000	1	1.000
		Will the operator's efficiency in identifying and preventing security incidents be improved by radar-AIS interface?	1.154	1	.283
		Do you have any prior experience with container security scanning?	1.154	1	.283
		Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). In your	.061	1	.804

		Do you think all ships on international journeys should be required to report to one of the global ship reporting systems?	1.695	1	.193
		In terms of training, does the Vessel Data Recorder (VDR) improve maritime security?	3.265	1	.071
		In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?	1.726	1	.189
	Overall Statistics		15.889	13	.255

This table displays variables that have not yet been included in the model and assesses their potential significance if added. Three variables stand out with p-values below 0.05, suggesting they could improve the model: *"Is your country signatory to?"* ($p = 0.013$), *"Is the technology required under different IMO instruments effective in fostering maritime security?"* ($p = 0.024$), and *"Do you feel, in the present-day scenario there is a need to enhance maritime security?"* ($p = 0.034$). These variables show statistically significant potential to influence maritime security outcomes. Other variables, however, such as *"In your opinion, are the instruments adopted by IMO adequate to combat the above maritime crimes?"* ($p = 0.804$) and *"Have you dealt with a security incident in your place of work?"* ($p = 1.000$), are statistically insignificant, indicating they would likely add minimal predictive value. The overall score statistic ($p = 0.255$) suggests no strong cumulative effect from adding these variables, though select variables could still be beneficial for enhancing model accuracy.

Block 1: Method = Enter

Table 4.39: Omnibus Tests of Model Coefficients

		Chi-square	df	Sig.
Step 1	Step	17.357	13	.183
	Block	17.357	13	.183
	Model	17.357	13	.183

The logistic regression model's fit is assessed in the Omnibus Tests of Model Coefficients table following the addition of predictors in Step 1. The improved model fit over a model without predictors is indicated by the chi-square value of 17.357 with 13 degrees of freedom. It is not statistically significant, though, because the significance level (p = 0.183) is higher than the usual cutoff of 0.05. Thus, the predictive power of the model was not significantly increased by the predictors added in Step 1.

Table 4.40: "Model Summary"

Step	-2 Log likelihood	Cox & Snell R Square	Nagelkerke R Square
1	31.512[a]	.352	.499
a. Because the parameter estimations changed by less than.001, the estimation was stopped at iteration number 6.			

Table 4.41: Classification[al]

	Observed	Predicted

			Is the organisation in charge of marine security in ports, anchorage areas, and ships outside of port jurisdiction also your "Flag Administration"?		Percentage Correct
			Yes	No	
Step 1	Is the maritime security in ports, anchorage areas, and ships outside of port authority handled by the same organisation under your "Flag Administration"?	Yes	26	2	92.9
		No	4	8	66.7
	Overall Percentage				85.0
a. The cut value is .500					

Following the addition of predictors in Step 1, the model's prediction accuracy is shown in the Classification Table. The model's accuracy for this category was 92.9%; in cases where the response was "Yes," it properly predicted "Yes" 26 times and wrongly predicted "No" twice. In instances when a "No" response was seen, the model achieved 66.7% accuracy for "No" replies by correctly predicting "No" 8 times and mistakenly predicting "Yes" 4 times. With an overall accuracy of 85.0% across all cases, the model outperforms the baseline model in terms of prediction. The model predicts "Yes" if the likelihood of "Yes" is 0.5 or higher and "No" if it is less than 0.5, with a cut-off value of

0.500. Compared to the first step, this one shows improved accuracy in both categories, particularly for the "No" answers.

Table 4.42: "Variables in the Equation"

		B	S.E.	Wald	df	Sig.	Exp(B)
Step 1[a]	Is your country signatory to?	1.626	1.229	1.749	1	.186	5.083
	Does the technology mandated by several IMO treaties effectively promote maritime security in the region?	1.582	1.222	1.677	1	.195	4.867
	Do you think that marine security has to be improved in the current situation?	1.497	1.662	.810	1	.368	4.467
	Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?	.301	1.601	.035	1	.851	1.351

	Do your flagships currently have enough personnel on board to meet security requirements?	-1.222	1.442	.717	1	.397	.295
	Current trends indicate that certain flag state administrations issue safe manning certifications without paying enough attention to security standards, onboard administrative tasks, and vessel trading. Considering the current state of global security,	1.074	1.302	.680	1	.409	2.926
	Have you had to handle a security incident at work?	-1.539	1.410	1.191	1	.275	.215

	When radar and AIS are interfaced, will operator efficiency in identifying and preventing security incidents increase?	.250	1.521	.027	1	.869	1.285
	Do you have any prior experience inspecting containers for security?	2.035	1.246	2.667	1	.102	7.650
	Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). In your	.067	1.439	.002	1	.963	1.069

	Do you think all ships on international journeys should be required to report to one of the global ship reporting systems?	-.381	1.330	.082	1	.774	.683
	In terms of training, does the Vessel Data Recorder (VDR) improve maritime security?	1.762	1.376	1.640	1	.200	5.822
	Is there any analytical benefit to maritime security from the Vessel Data Recorder (VDR)?	-1.191	1.727	.476	1	.490	.304
	Constant	-8.968	3.669	5.976	1	.014	.000

The coefficients, significance thresholds, and odds ratios for the predictors that were part of Step 1 of the logistic regression model are shown in the Variables in the Equation table. Although the majority are not statistically significant at the 0.05 level, a few of variables exhibit the ability to affect maritime security. For example, the variable *In terms of training, does the "Vessel Data Recorder" (VDR) improve maritime security? has a p-value of 0.200, which means it is not statistically significant, but its odds ratio of 5.822 suggests a high positive effect if it were significant.* Similarly, *"Is your country signatory to?"* and *"Is the technology required under different IMO instruments effective*

in fostering maritime security?" have odds ratios of 5.083 and 4.867, respectively, suggesting a strong positive impact, but neither is statistically significant (p-values of 0.186 and 0.195). Some variables, such as *"Do you feel there is a need to enhance maritime security?"* and *"Are the present manning levels onboard your flagships adequate to comply with security regulations?"*, are also not significant, with p-values of 0.368 and 0.397. The variable *"Do you have any experience in security scanning of containers?"* has an odds ratio of 7.650, indicating a strong positive association, but its p-value of 0.102 still places it above the significance threshold. The constant term is significant (p = 0.014), but its odds ratio is effectively zero, suggesting a very low baseline prediction for the outcome without any predictors. Overall, while several predictors show promising odds ratios, further analysis is needed to confirm their statistical significance and practical impact on maritime security.

4.2 Foreign Naïve

Reliability

Table 4.43: Reliability Statistics

Cronbach's Alpha	N of Items
.804	27

The scale of 27 items has good reliability, with a Cronbach's Alpha of 0.804, indicating strong internal consistency.

Frequency Table

Table 4.44: Do you think that marine security has to be improved in the current situation?

	Frequency	Percent
Yes	32	88.9
No	4	11.1

Total	36	100.0

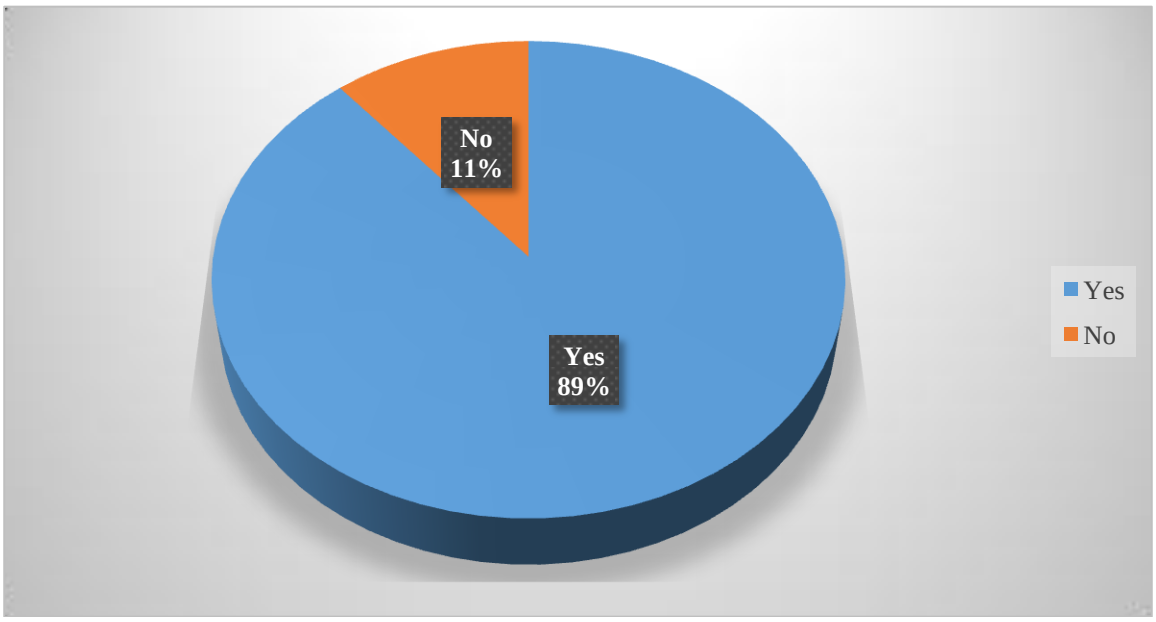


Figure 4.34: Do you think that marine security has to be improved in the current situation?

According to the above number, 32 out of 36 respondents, or 88.9% of the total, feel that improving maritime security is necessary in the current environment. Only 4 respondents (11.1%) do not see the need for enhancement. This indicates strong support for improving maritime security.

Table 4.45: Which criminal activity do you think is the biggest threat to the marine industry?

	Frequency	Percent
Piracy and Armed Robbery Against Ships	13	36.1
Maritime Drug Trafficking and Terrorism	7	19.4
Illegal Migration	8	22.2
Stowaways	6	16.7

Human Trafficking	1	2.8
Other	1	2.8
Total	36	100.0

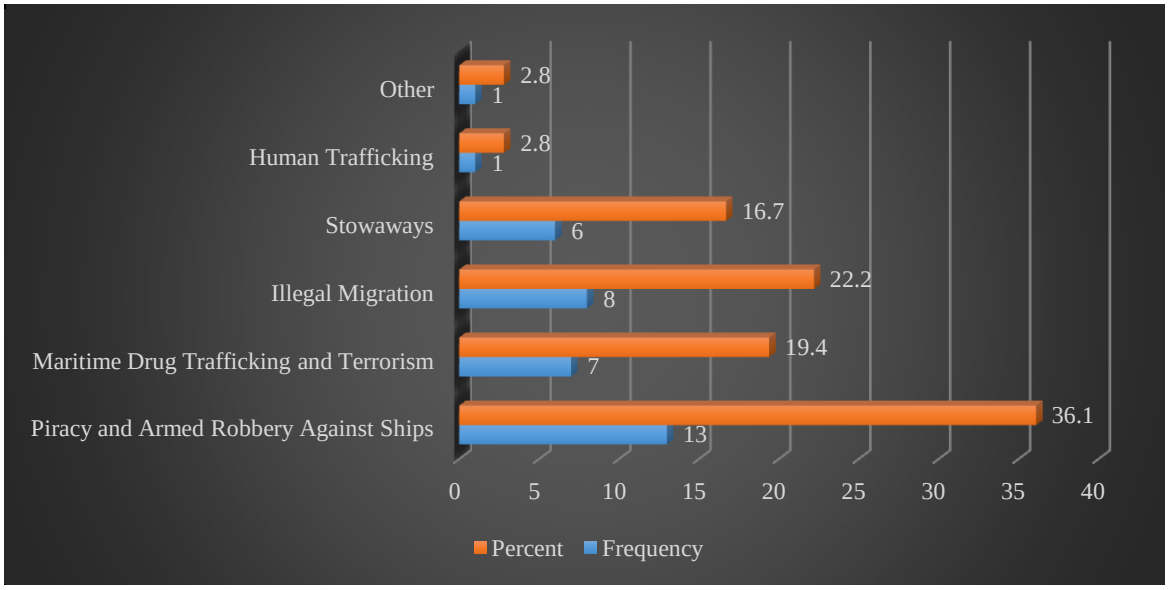


Figure 4.35: Which criminal activity do you think is the biggest threat to the marine industry?

The above figure indicates that "**Piracy and Armed Robbery Against Ships"** is viewed as the greatest threat to the maritime sector, with 36.1% (13 out of 36) of respondents identifying it as the top concern. This is followed by **Illegal Migration** (22.2%) and **Maritime Drug Trafficking and Terrorism** (19.4%). Other threats like **Stowaways** and **Human Trafficking** are considered less significant, each with lower percentages. Overall, piracy and armed robbery are perceived as the most pressing threat in the sector.

Table 4.46: Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?

	Frequency	Percent
Yes	30	83.3
No	6	16.7

Total	36	100.0

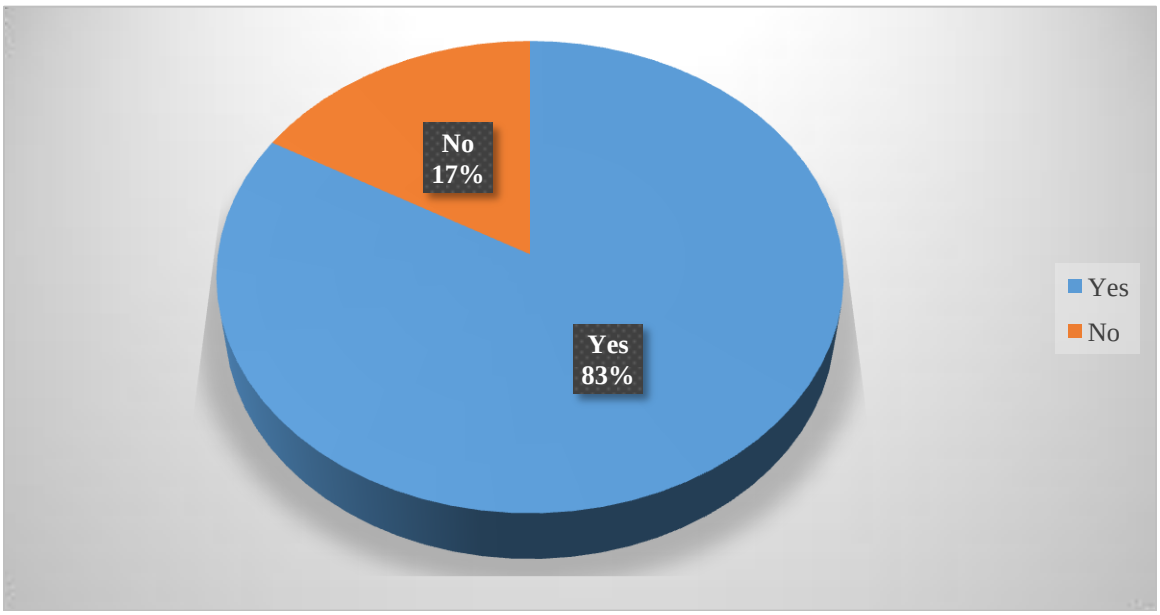


Figure 4.36: Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?

The above figure shows that a majority (83.3%) of respondents believe that the instruments adopted by "International Maritime Organization "(IMO) are adequate to combat maritime crimes, with 30 out of 36 in agreement. However, 16.7% (6 respondents) feel that these instruments are insufficient. This suggests a high level of confidence in IMO measures, though a minority sees room for improvement.

Table 4.47: How frequently does the "Maritime Administration" interact for maritime security issues with Law enforcement agencies? Tick your answer (only one)

	Frequency	Percent
Daily basis	9	25.0
Weekly basis	12	33.3
Monthly basis	5	13.9
Quarterly basis	8	22.2
Half basis	2	5.6

Total	36	100.0

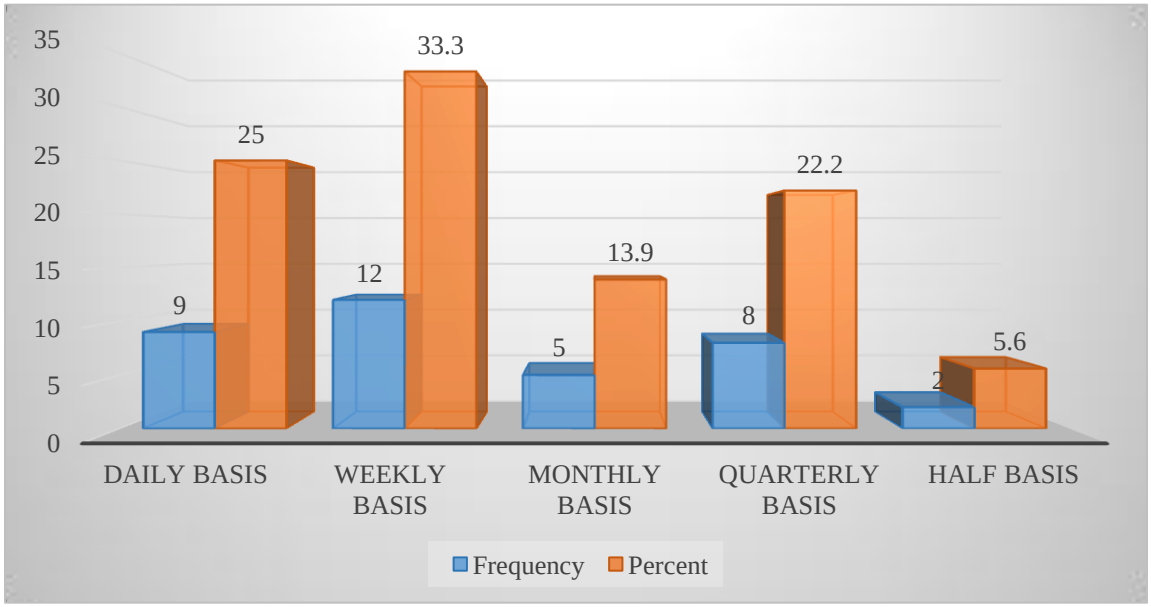


Figure 4.37: How frequently does the "Maritime Administration" interact for maritime security issues with Law enforcement agencies? Tick your answer (only one)

The above figure shows that **weekly interactions** amid "Maritime Administration" and law enforcement agencies for maritime security issues are the most common, with 33.3% (12 out of 36) of respondents selecting this option. This is followed by **daily interactions** (25.0%) and **quarterly interactions** (22.2%). Less frequent interactions, such as **monthly** (13.9%) and **biannual** (5.6%), are chosen by fewer respondents. This indicates that most interactions are fairly regular, with weekly and daily being the most common.

Table 4.48: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (Requirement basis)

	Frequency	Percent
Ship Reporting	22	61.1
AIS	8	22.2
Ship entering/leaving ports	6	16.7

Total	36	100.0

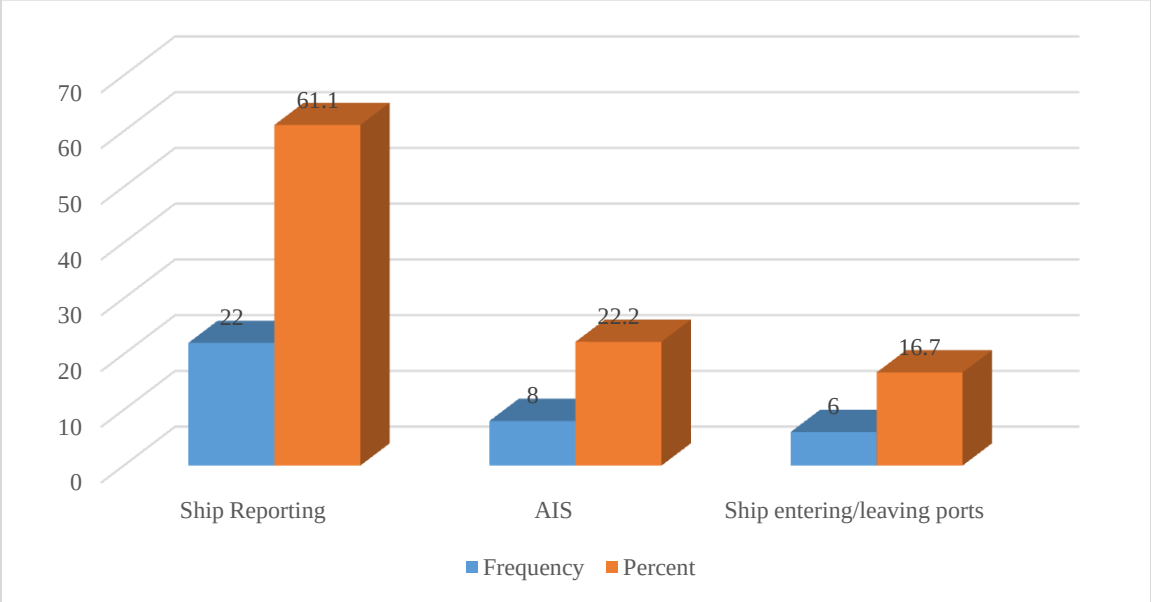


Figure 4.38: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (Requirement basis)

The above figure illustrates that **Ship Reporting** is the primary method for data sharing between "Flag Administration" and maritime law enforcement agencies on a requirement basis, with 61.1% (22 out of 36) indicating this method. **AIS (Automatic Identification System)** follows with 22.2%, and **data on ships entering or leaving ports** is the least common, with 16.7%. This suggests that ship reporting is the preferred data-sharing method for maritime security coordination.

Table 4.49: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (Online)

	Frequency	Percent
Ship Reporting	17	47.2
AIS	14	38.9
Ship entering/leaving ports	5	13.9
Total	36	100.0

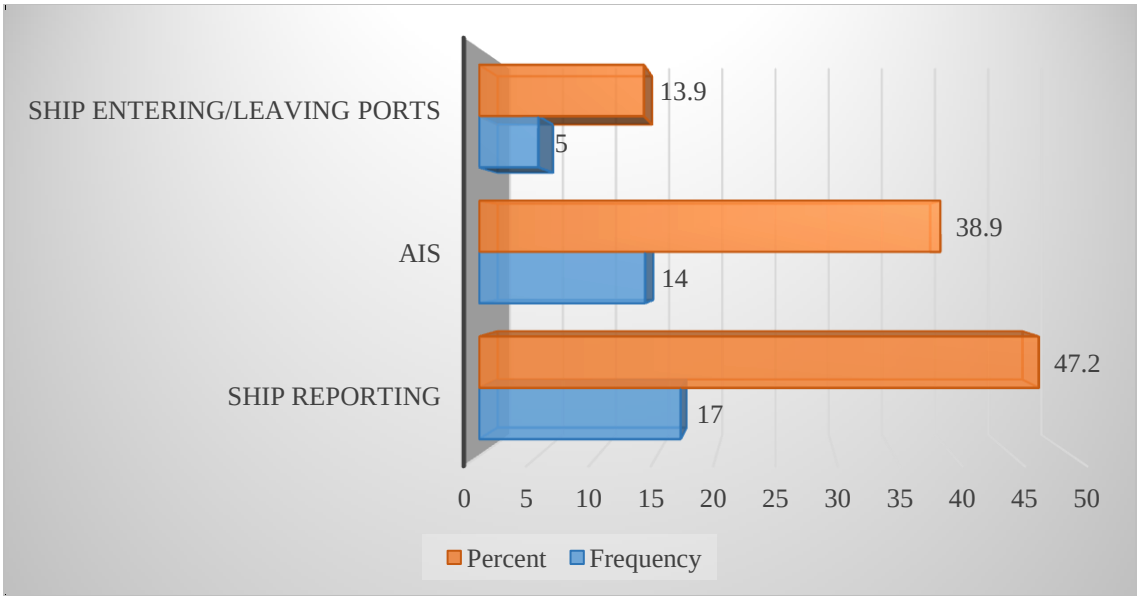


Figure 4.39: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (Online)

The above figure indicates that **Ship Reporting** is the most commonly shared data online among "Flag Administration" and "maritime law enforcement agencies", chosen by 47.2% (17 out of 36) of respondents. **AIS (Automatic Identification System)** data follows at 38.9%, while **data on ships entering or leaving ports** is the least commonly shared online, at 13.9%. This suggests that Ship Reporting and AIS are the primary data types shared digitally for maritime security.

Table 4.50: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (2 exchange of data)

	Frequency	Percent
Ship Reporting	22	61.1
AIS	6	16.7
Ship entering/leaving ports	8	22.2
Total	36	100.0

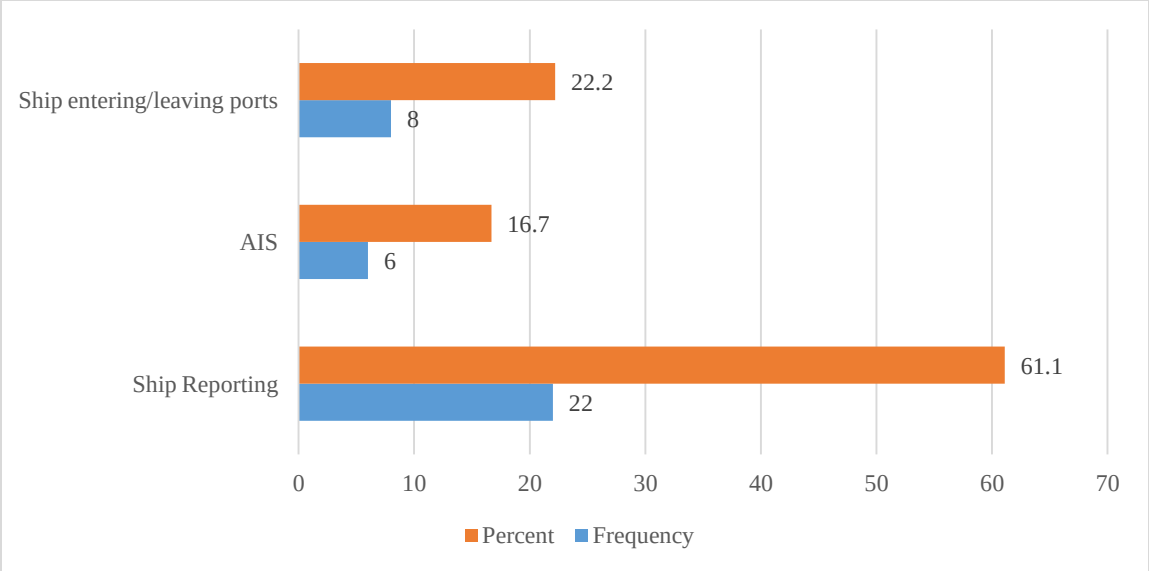


Figure 4.40: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (2 exchange of data)

The above figure shows that **Ship Reporting** is the most common method for the exchange of data between the "Flag Administration" and ""maritime law enforcement agencies"", with 61.1% (22 out of 36) of respondents selecting this option. **Data on ships entering or leaving ports** follows at 22.2%, while **AIS (Automatic Identification System)** data is the least exchanged method, at 16.7%. This indicates that ship reporting is the primary method for data exchange between the two entities.

Table 4.51: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (My country does not have the system)

	Frequency	Percent
Ship Reporting	16	44.4
AIS	14	38.9
Ship entering/leaving ports	6	16.7
Total	36	100.0

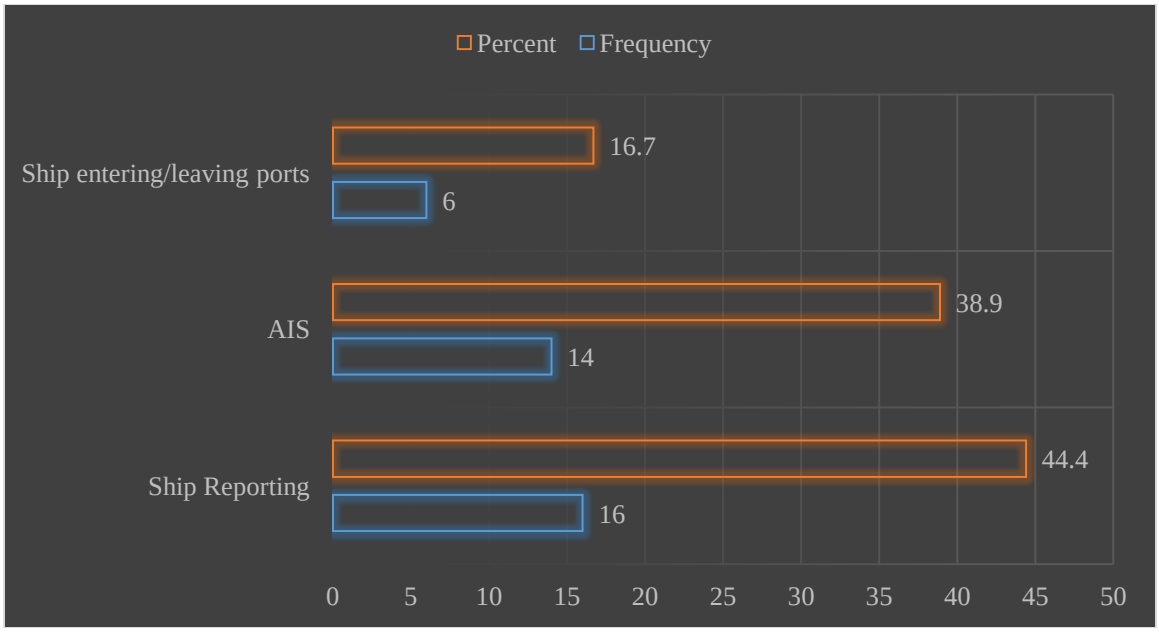


Figure 4.41: How are the data listed below being shared between the "Flag Administration" and maritime law enforcement agency? (My country does not have the system)

The above figure shows that **Ship Reporting** is the most common data-sharing method not implemented in the respondent's country, with 44.4% (16 out of 36) indicating that their country does not have this system. **AIS (Automatic Identification System)** follows at 38.9%, and **data on ships entering or leaving ports** is the least absent, with 16.7%. This suggests that the lack of a ship reporting system is the most significant gap in maritime data-sharing systems in the countries represented by the respondents.

Table 4.52: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ports)

	Frequency	Percent
Yes	24	66.7
No	12	33.3
Total	36	100.0

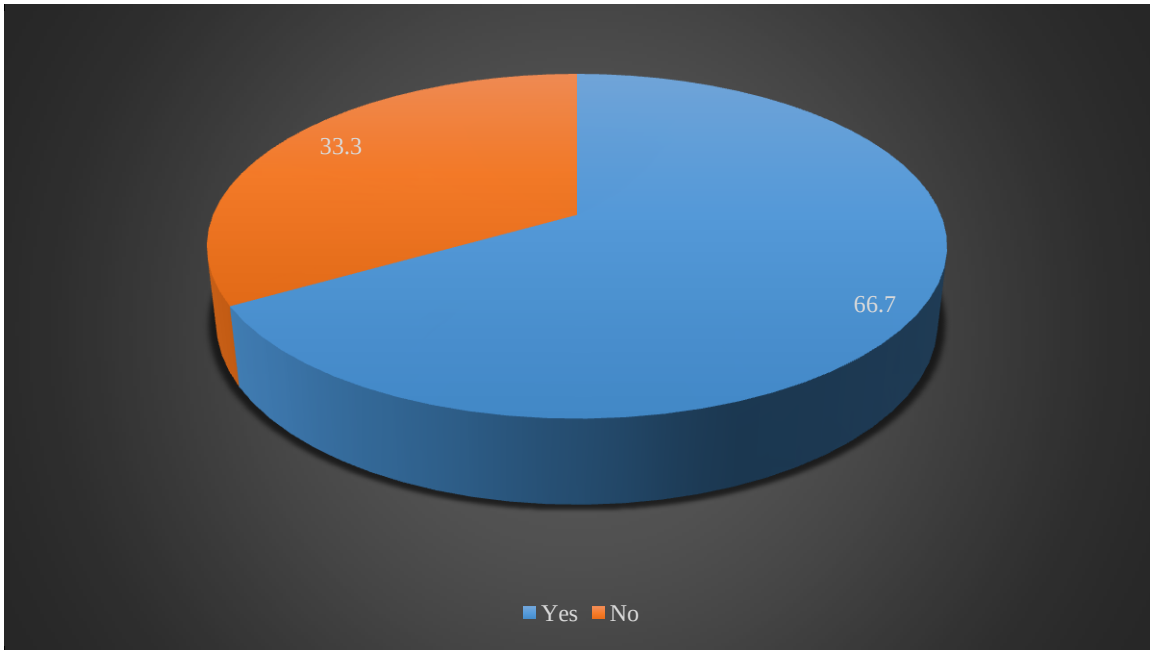


Figure 4.42: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ports)

The above figure shows that **66.7%** (24 out of 36) of respondents believe the technology required under different IMO instruments is effective in fostering maritime security in **ports**, while **33.3%** (12 respondents) do not. This indicates that a majority of respondents feel the technology is beneficial in enhancing security at ports.

Table 4.53: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ships)

	Frequency	Percent
Yes	29	80.6
No	7	19.4
Total	36	100.0

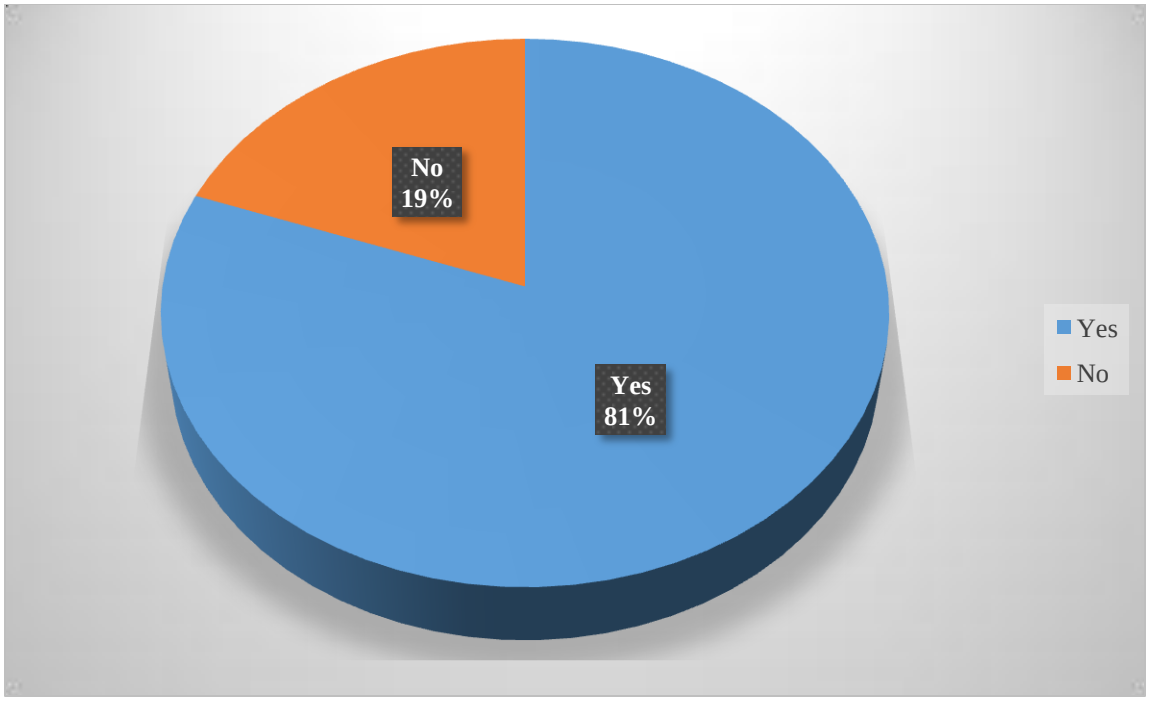


Figure 4.43: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ships)

The above figure shows that **80.6%** (29 out of 36) of respondents believe the technology required under different IMO instruments is effective in fostering maritime security in **ships**, while **19.4%** (7 respondents) do not. This indicates a strong majority feel the technology is effective in enhancing security for ships.

Table 4.54: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Other Installations)

	Frequency	Percent
Yes	27	75.0
No	9	25.0
Total	36	100.0

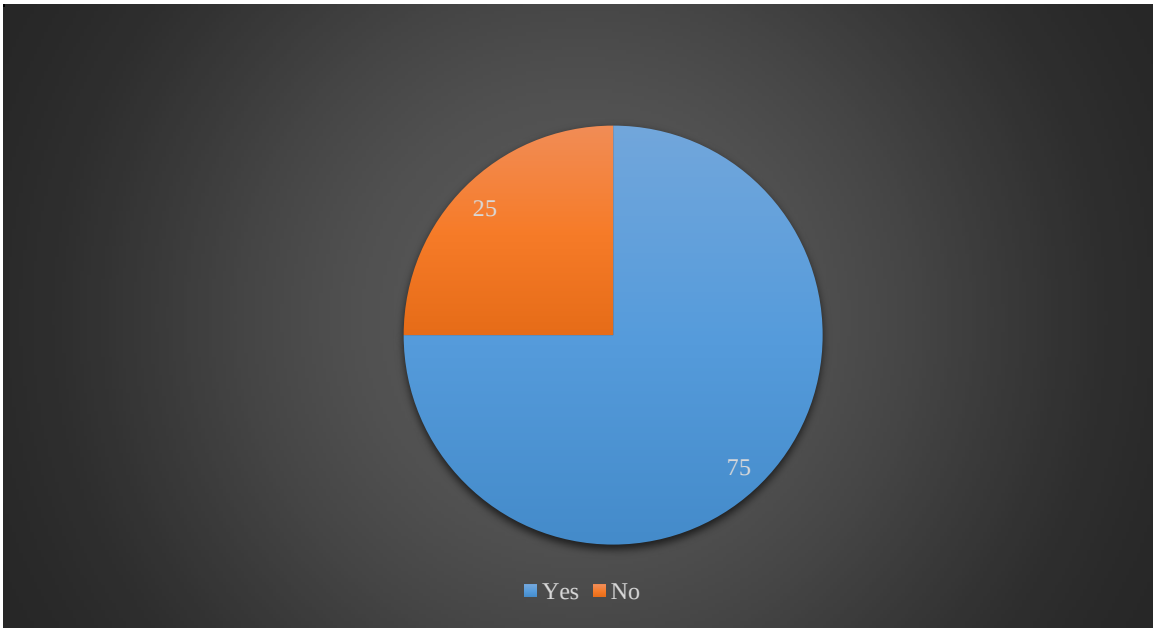


Figure 4.44: Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Other Installations)

The above figure states that **75.0%** (27 out of 36) of respondents believe the technology required under different IMO instruments is effective in fostering maritime security in **other installations**, while **25.0%** (9 respondents) do not. This indicates a positive perception of the effectiveness of IMO-required technology in enhancing security in other maritime installations.

Table 4.55: As a maritime law enforcement agency, do you have access to the data bank for the ships registered in your country?

	Frequency	Percent
Yes	26	72.2
No	10	27.8
Total	36	100.0

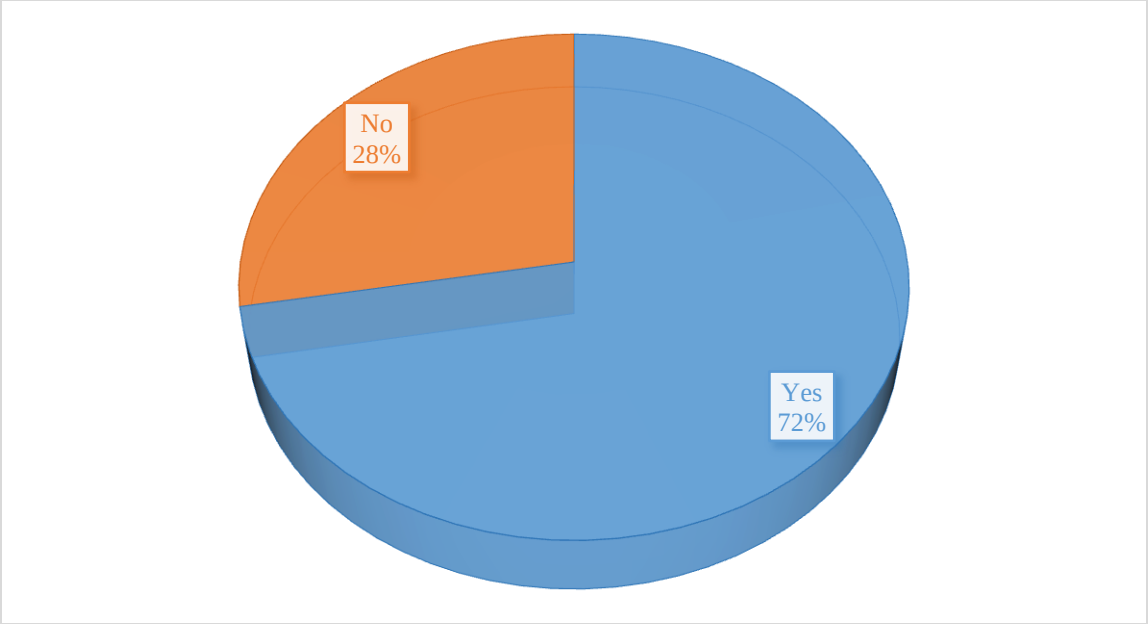


Figure 4.45: As a maritime law enforcement agency, do you have access to the data bank for the ships registered in your country?

The above figure shows that **72.2%** (26 out of 36) of respondents from "maritime law enforcement agencies" have access to the data bank for ships registered in their country, while **27.8%** (10 respondents) do not. This indicates that the majority of agencies have access to this important data for security and regulatory purposes.

Table 4.56: How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security?

	Frequency	Percent
Effective	24	66.7
Not Effective	12	33.3
Total	36	100.0

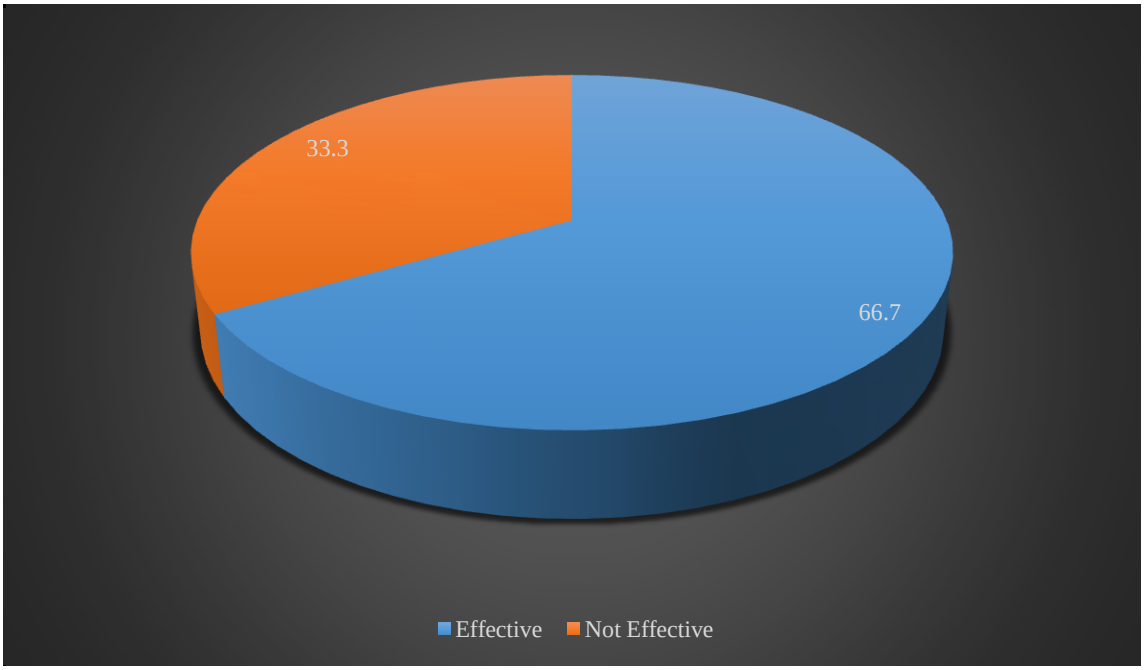


Figure 4.46: How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security?

The above figure shows that **66.7%** (24 out of 36) of respondents believe the "**Ship Security Alarm System" (SSAS)** is **effective** in promoting "maritime security", while **33.3%** (12 respondents) believe it is **not effective**. This indicates that a majority of respondents view SSAS as an important tool in enhancing maritime security.

Table 4.57: Have you dealt with a security incident in your place of work?

	Frequency	Percent
Yes	26	72.2
No	10	27.8
Total	36	100.0

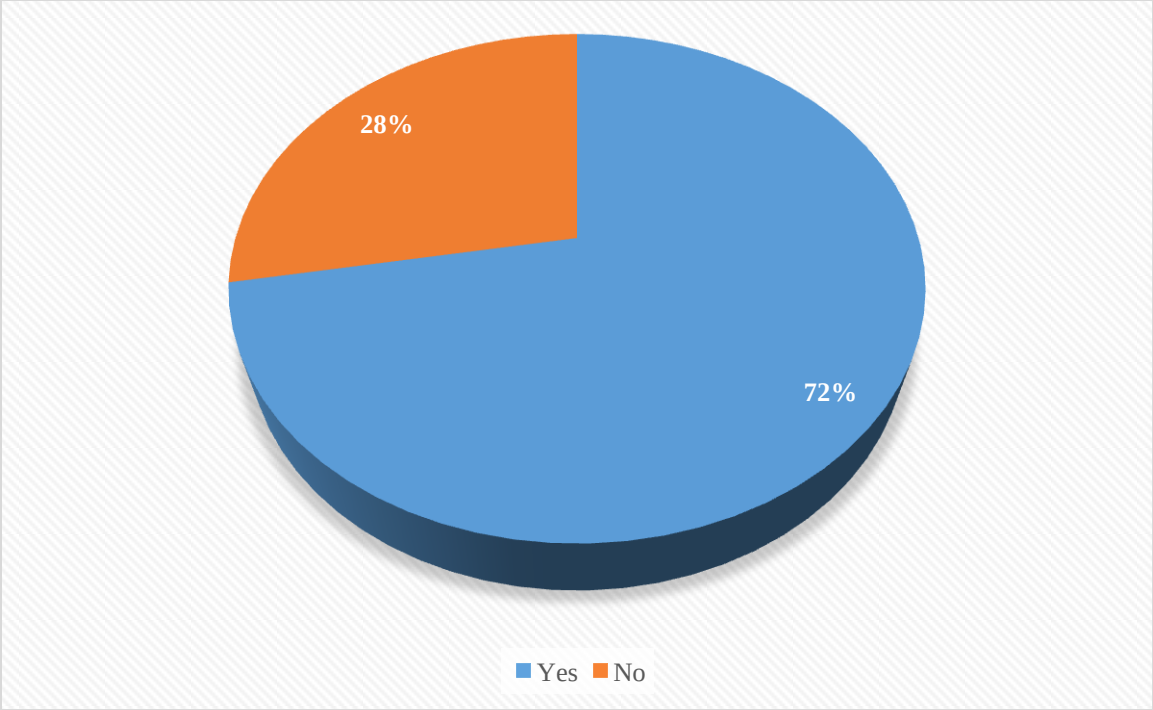


Figure 4.47: Have you dealt with a security incident in your place of work?

The above figure shows that **72.2%** (26 out of 36) of respondents have dealt with a security incident in their place of work, while **27.8%** (10 respondents) have not. This suggests that a significant portion of respondents has experience with security incidents in their maritime work environment.

Table 4.58: How would you rate the response of "Maritime Administration" / "maritime law enforcement agencies" in the above incident(s)?

	Frequency	Percent
Effective	29	80.6
Inadequate	7	19.4
Total	36	100.0

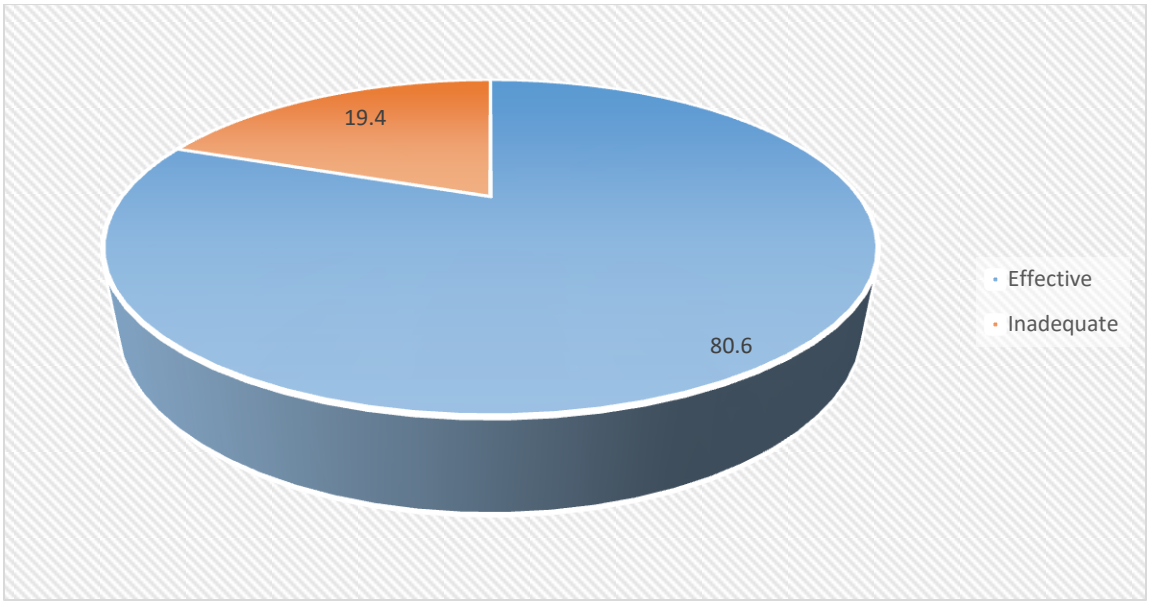


Figure 4.48: How would you rate the response of "Maritime Administration" / "maritime law enforcement agencies" in the above incident(s)?

The aforementioned figure shows that **80.6%** (29 out of 36) of respondents rated the response of ""**Maritime Administration**""/""**maritime law enforcement agencies**"" as **effective** in handling the security incident(s), while **19.4%** (7 respondents) considered it **inadequate**. This indicates that the majority of respondents felt the agencies responded effectively to security incidents.

Table 4.59: Does Automatic Identification System (2) promote security or does it create obstacles?

	Frequency	Percent
Effective for security	21	58.3
Hindrance for security	15	41.7
Total	36	100.0

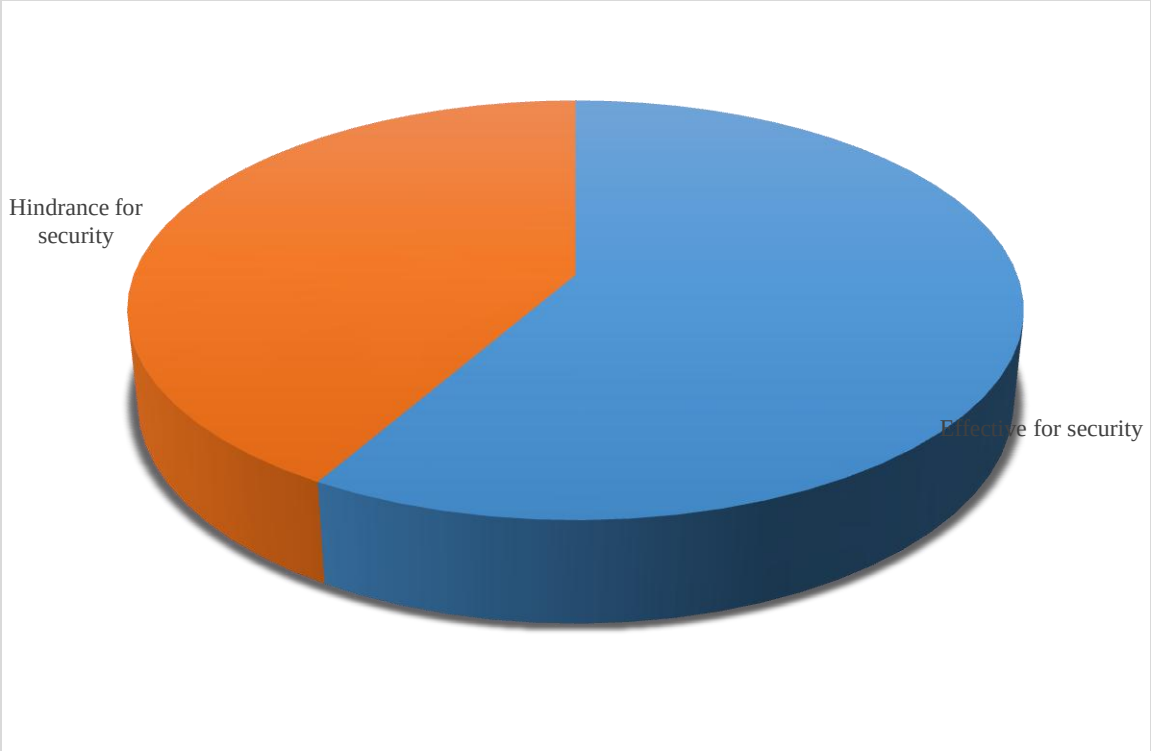


Figure 4.49: Does Automatic Identification System (2) promote security or does it create obstacles?

The above figure shows that **58.3%** (21 out of 36) of respondents believe the **Automatic Identification System (AIS)** is **effective for security**, while **41.7%** (15 respondents) consider it a **hindrance** to security. This suggests that while a majority view AIS as beneficial for security, a significant portion believes it may present challenges.

Table 4.60: Does the Vessel Traffic System (VTS) promote or hinder security?

	Frequency	Percent
Effective for security	29	80.6
Hindrance for security	7	19.4
Total	36	100.0

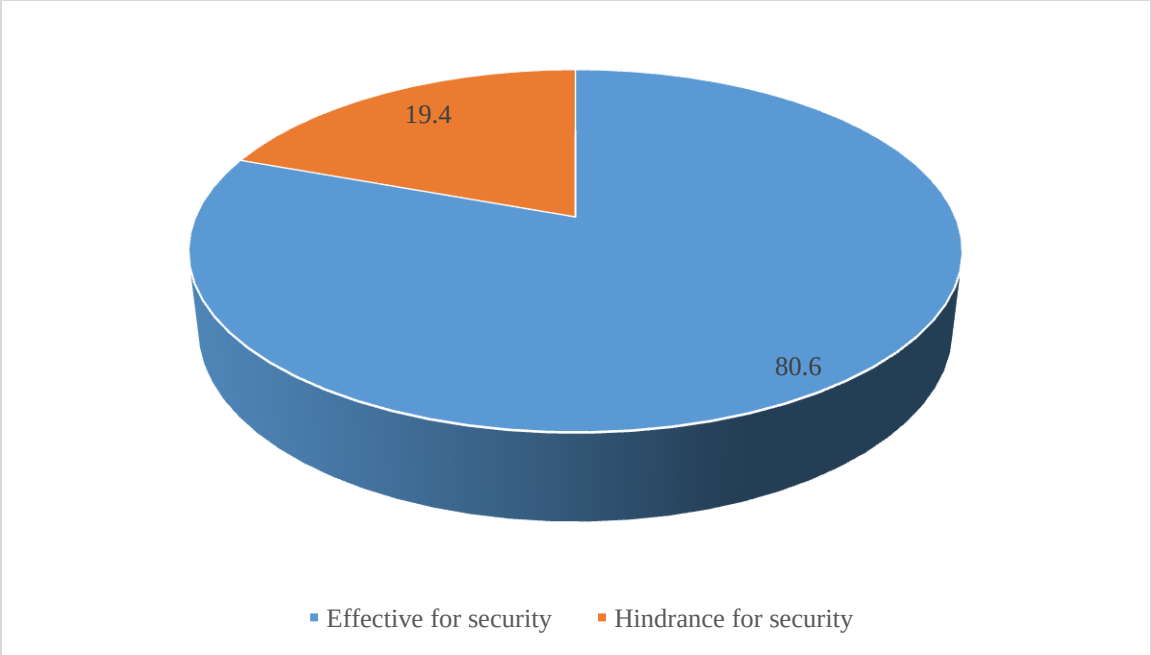


Figure 4.50: Does the Vessel Traffic System (VTS) promote or hinder security?

The aforementioned figure shows that **80.6%** (29 out of 36) of respondents believe the **Vessel Traffic System (VTS)** is **effective for security**, while **19.4%** (7 respondents) consider it a **hindrance** to security. This indicates strong support for the effectiveness of VTS in enhancing maritime security.

Table 4.61: Is VTS an active security threat mitigation strategy or a deterrent?

	Frequency	Percent
Deterrent	18	50.0
Active measure	18	50.0
Total	36	100.0

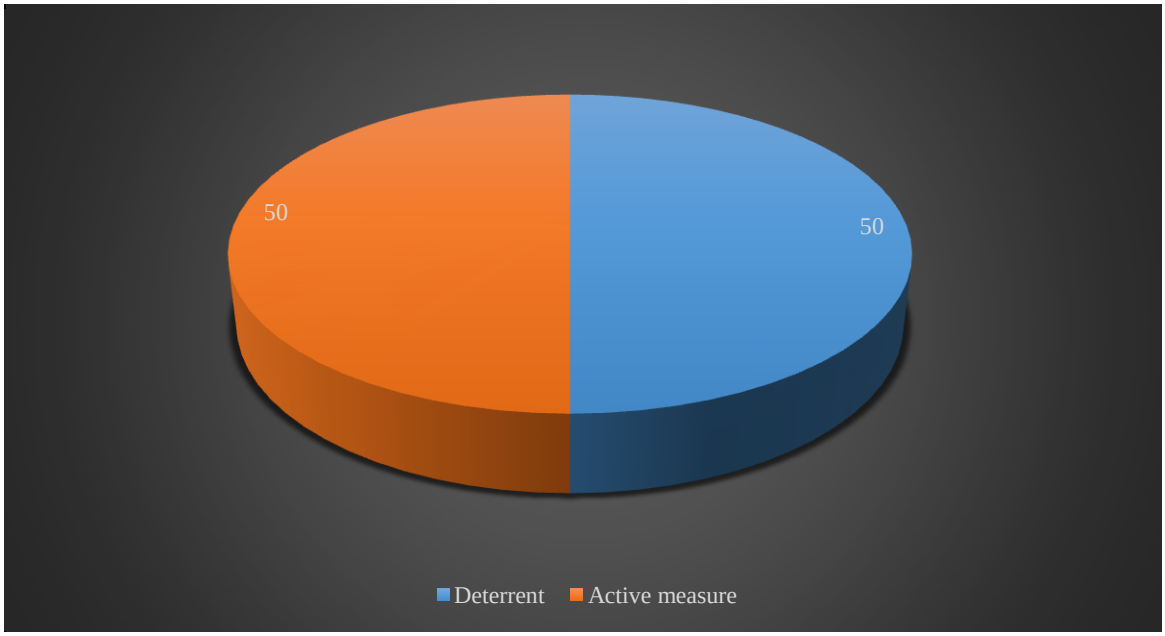


Figure 4.51: Is VTS an active security threat mitigation strategy or a deterrent?

The table shows that **50.0%** (18 out of 36) of respondents view the **Vessel Traffic System (VTS)** as a **deterrent**, while the other **50.0%** (18 respondents) see it as an **active measure** for "mitigating security threats". This indicates that respondents are evenly divided on whether VTS primarily deters threats or actively addresses them.

Table 4.62: Will requiring reporting to the Vessel Traffic System (VTS) improve local security as a whole?

	Frequency	Percent
Yes	28	77.8
No	8	22.2
Total	36	100.0

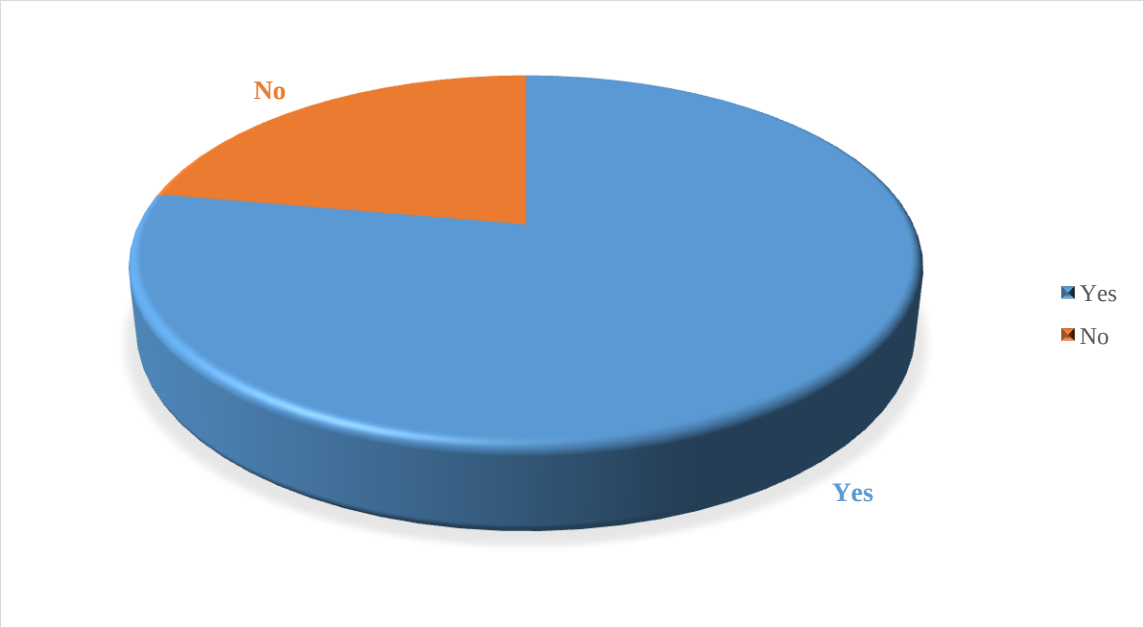


Figure 4.52: Will requiring reporting to the Vessel Traffic System (VTS) improve local security as a whole?

The above figure shows that **77.8%** (28 out of 36) of respondents believe that **mandatory reporting to the "Vessel Traffic System" (VTS)** will enhance overall security in the area, while **22.2%** (8 respondents) disagree. This indicates strong support for the idea that mandatory reporting can improve maritime security.

Table 4.63: Will connecting radar to two improve operator effectiveness in seeing security incidents early and preventing them?

	Frequency	Percent
Yes	29	80.6
No	7	19.4
Total	36	100.0

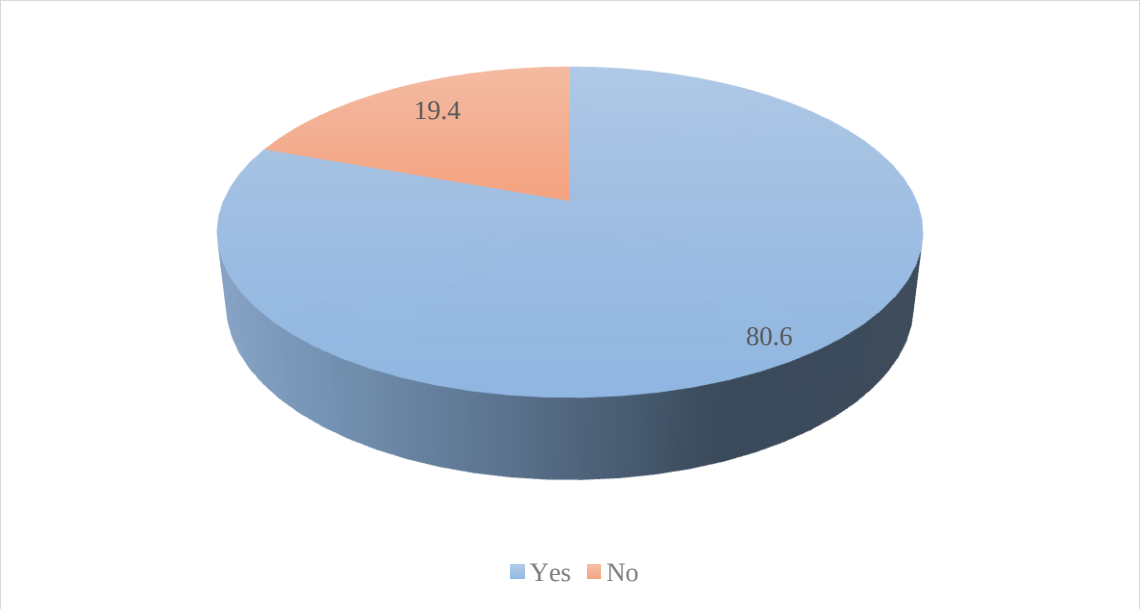


Figure 4.53: Will connecting radar to two improve operator effectiveness in seeing security incidents early and preventing them?

The figure shows that **80.6%** (29 out of 36) of respondents believe that **interfacing radar with AIS** will enhance operator efficiency in the **early identification and prevention** of security incidents, while **19.4%** (7 respondents) do not. This indicates strong support for the potential benefits of combining radar and AIS to improve security monitoring and response.

Table 4.64: Will the goal of safe transportation be aided or hindered by long-range identification and tracking of ships (LRIT)?

	Frequency	Percent
Foster maritime security	24	66.7
Will be a hindrance	12	33.3
Total	36	100.0

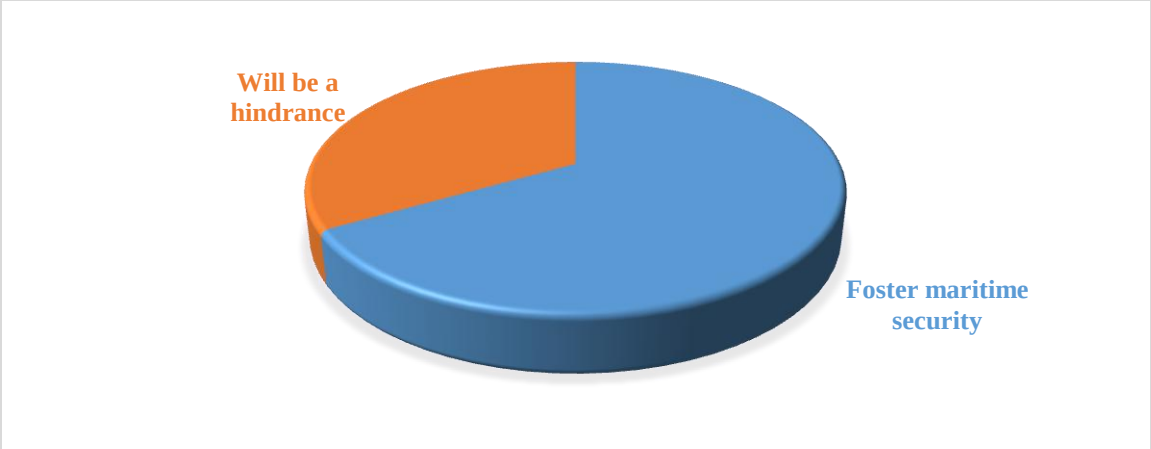


Figure 4.54: Will the goal of safe transportation be aided or hindered by long-range identification and tracking of ships (LRIT)?

The above figure shows that **66.7%** (24 out of 36) of respondents believe that "**Long-Range Identification and Tracking" (LRIT)** will "**foster maritime security"**, while **33.3%** (12 respondents) consider it a **hindrance**. This indicates a majority view that LRIT is beneficial for enhancing maritime security.

Table 4.65: Do you have any prior experience inspecting containers for security?

	Frequency	Percent
Yes	24	66.7
No	12	33.3
Total	36	100.0

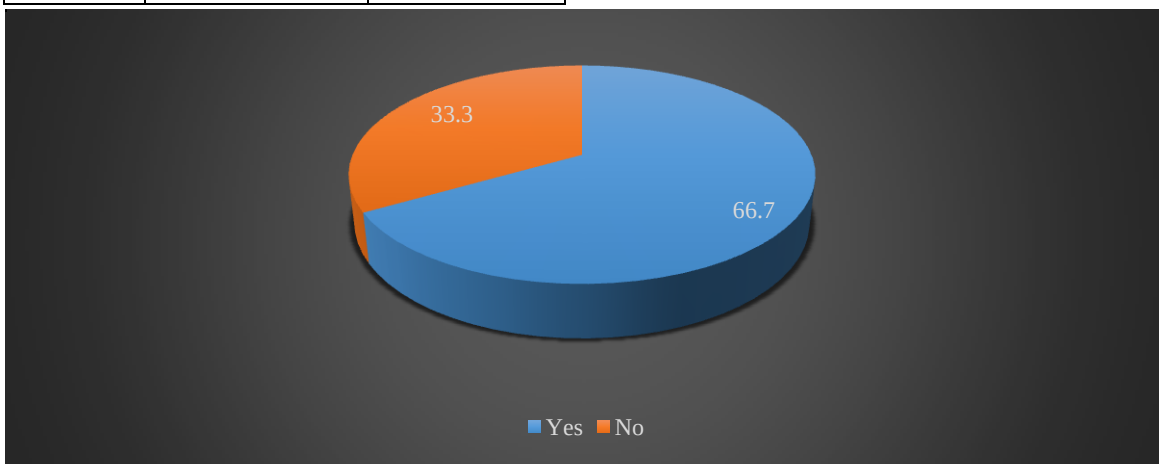
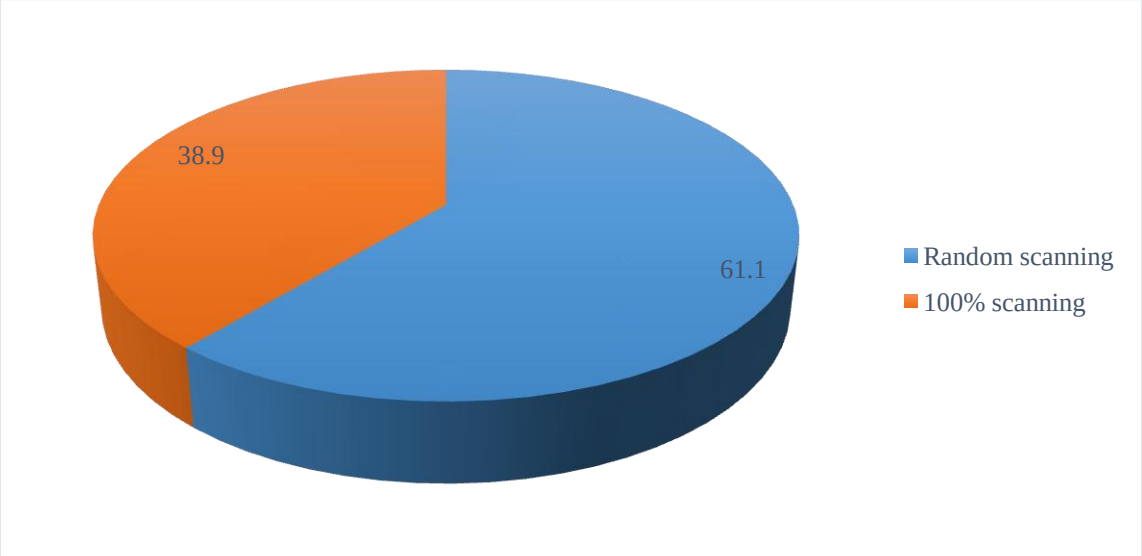


Figure 4.55: Do you have any prior experience inspecting containers for security?

The aforementioned figure shows that **66.7%** (24 out of 36) of respondents have experience in **security scanning of containers**, while **33.3%** (12 respondents) do not. This indicates that a majority of respondents have hands-on experience with container security scanning.

Table 4.66: What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment?

	Frequency	Percent
Random scanning	22	61.1
100% scanning	14	38.9
Total	36	100.0



Figute 4.56: What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment?

The above figure shows that **61.1%** (22 out of 36) of respondents believe that **random scanning** would be the best solution for enhancing maritime security, while **38.9%** (14 respondents) favour **100% scanning**. This suggests that a majority of respondents consider random scanning a more feasible or effective approach, possibly balancing security risks and commercial concerns.

Table 4.67: There are various 1 systems in the world, including the Indian (Maritime) Search and Rescue Computerised 1 System (INDSAR), the Japanese 1 System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). In your opinion

	Frequency	Percent
Yes	25	69.4
No	11	30.6
Total	36	100.0

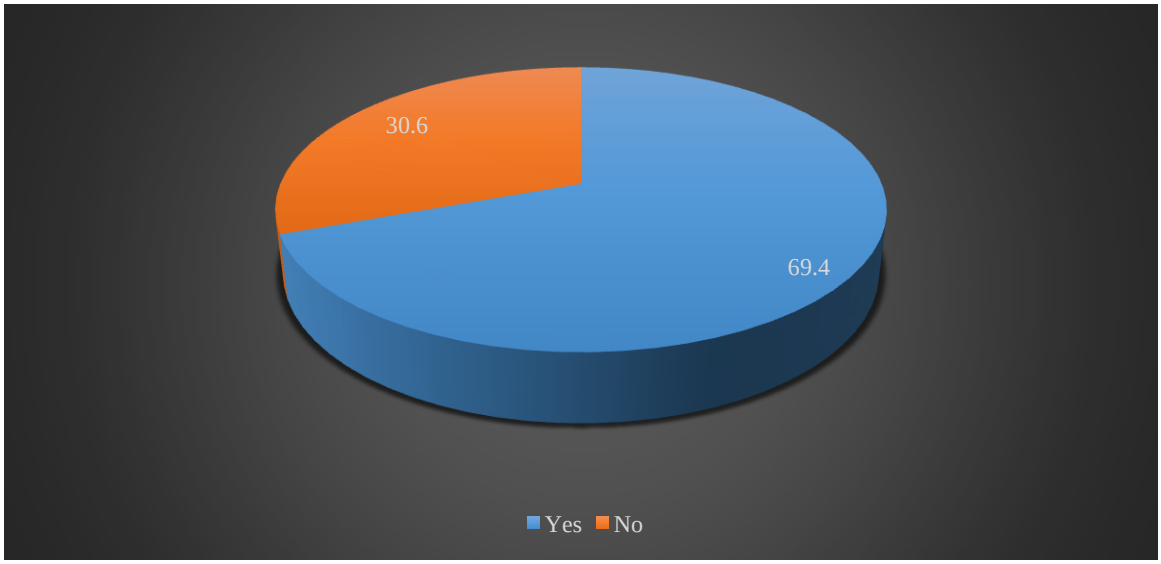


Figure 4.57: There are various 1 systems in the world, including the Indian (Maritime) Search and Rescue Computerised 1 System (INDSAR), the Japanese 1 System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). In your opinion

The aforementioned figure shows that **69.4%** (25 out of 36) of respondents believe that different **maritime rescue systems** worldwide, such as AMVER, JASREP, and INDSAR, are important, while **30.6%** (11 respondents) do not. This indicates strong support for the effectiveness or importance of these systems in maritime search and rescue operations.

Table 4.68: Should all ships on international journeys be required to report to one of the World Wide One systems, in your opinion?

	Frequency	Percent
Yes	25	69.4

No	11	30.6
Total	36	100.0

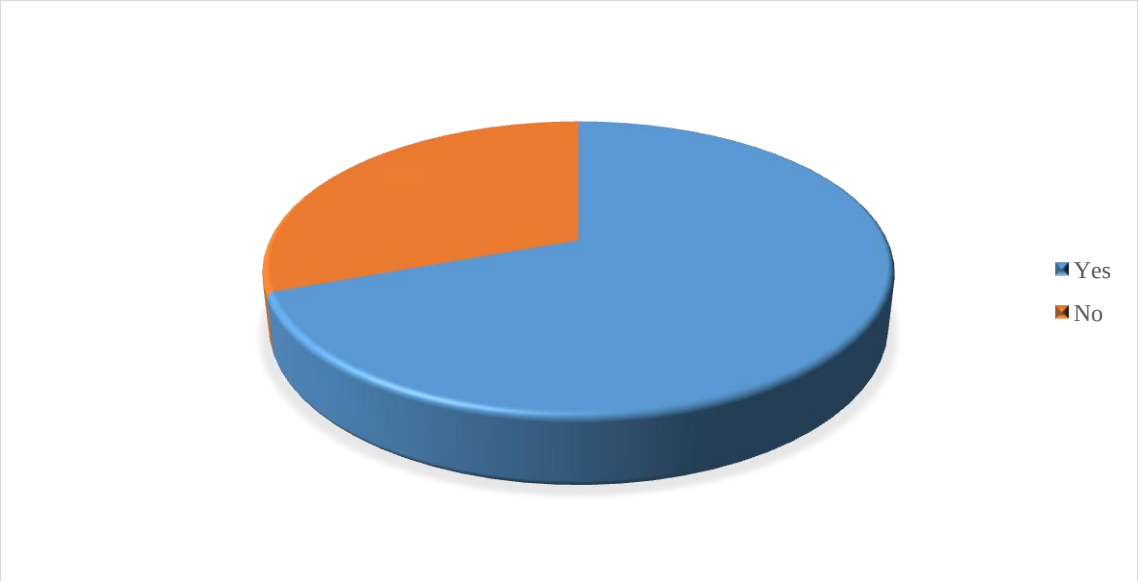


Figure 4.58: Should all ships on international journeys be required to report to one of the World Wide One system, in your opinion?

The aforementioned figure illustrates that **69.4%** (25 out of 36) of respondents believe that reporting to any one of the worldwide maritime rescue systems should be **mandatory** for all ships on "international voyages", while **30.6%** (11 respondents) disagree. This indicates strong support for making reporting to these systems a requirement for enhancing maritime safety and security.

Table 4.69: In terms of training, does the Vessel Data Recorder (VDR) improve maritime security?

	Frequency	Percent
Yes	30	83.3
No	6	16.7
Total	36	100.0

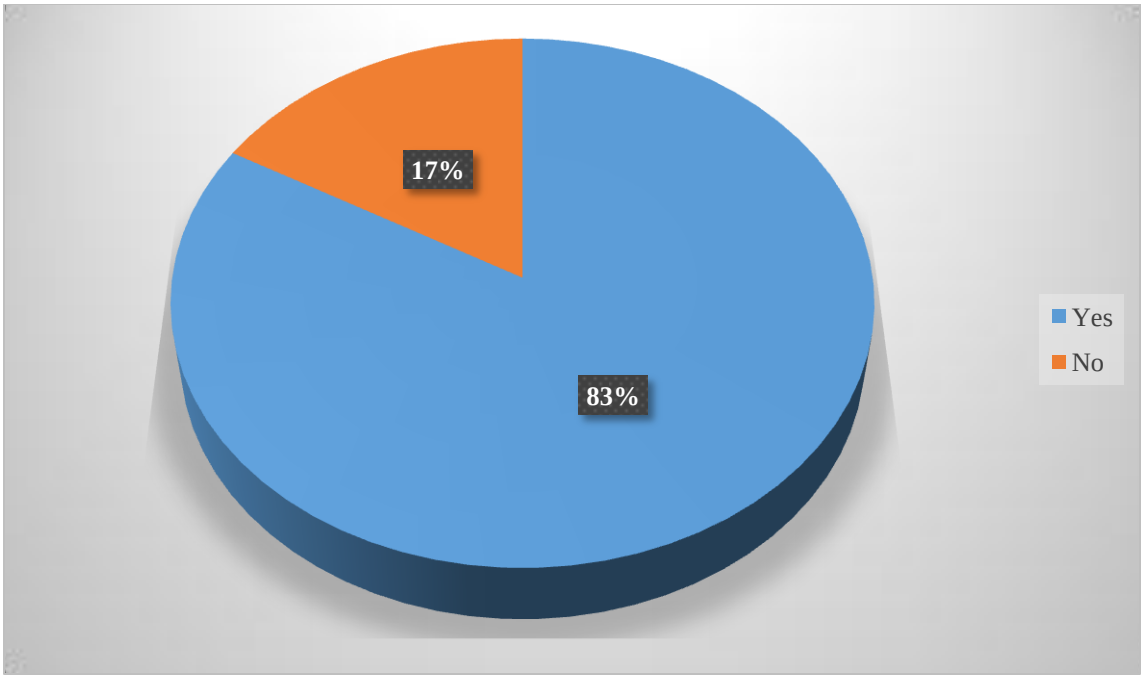


Figure 4.59: In terms of training, does the Vessel Data Recorder (VDR) improve maritime security?

The aforementioned figure shows that **83.3%** (30 out of 36) of respondents believe the "**Vessel Data Recorder" (VDR)** adds value to "maritime security", particularly with regard to **training**, while **16.7%** (6 respondents) do not. This suggests strong support for the role of VDR in enhancing training and improving maritime security.

Table 4.70: In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?

	Frequency	Percent
Yes	24	66.7
No	12	33.3
Total	36	100.0

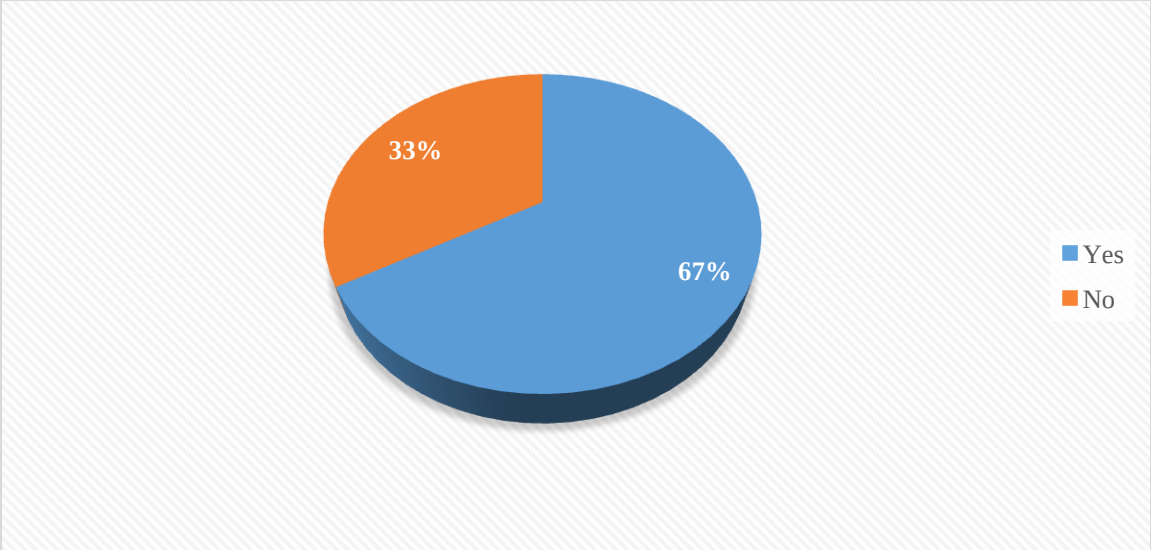


Figure 4.60: In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?

The aforementioned shows that **66.7%** (24 out of 36) of respondents believe the "**Vessel Data Recorder" (VDR)** adds value to maritime security, particularly in **analysis**, while **33.3%** (12 respondents) do not. This indicates a majority view that VDR contributes significantly to enhancing security through data analysis.

Nonparametric Tests

Table 4.71: Hypothesis Test Summary

	Null Hypothesis	Test	Test Statistic	Sig.	Decision
1	Do you think that improving maritime security is necessary given the current situation? happen with equal odds.	One-Sample Chi-Square Test	21.778[a]	.000	"Reject the null hypothesis".
2	Which crime, in your opinion, is the biggest danger to the maritime industry? happen with equal odds.	"One-Sample Chi-Square Test"	17.333[a]	.004	"Reject the null hypothesis".

3	Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes? happen with equal odds.	“One-Sample Chi-Square Test”	16.000[a]	.000	“Reject the null hypothesis”.
4	How often does the marine administration communicate with law enforcement regarding maritime security issues? happen with equal odds.	“One-Sample Chi-Square Test”	8.167[a]	.086	Retain the null hypothesis.
5	How are the maritime law enforcement agency and the “Flag Administration” sharing the information below? (Requirement basis) happen equally likely.	“One-Sample Chi-Square Test”	12.667[a]	.002	“Reject the null hypothesis”.
6	How are the maritime law enforcement agency and the “Flag Administration” sharing the information below? (online) have identical odds of happening.	“One-Sample Chi-Square Test”	6.500[a]	.039	“Reject the null hypothesis”.
7	In what ways do the “Flag Administration” and “maritime law enforcement agencies” exchange the following data?	“One-Sample Chi-Square Test”	12.667[a]	.002	“Reject the null hypothesis”.

	Two data exchanges happen with equal odds.				
8	How are the maritime law enforcement agency and the "Flag Administration" sharing the information below? occur with equal probability (the system is not in place in my country).	"One-Sample Chi-Square Test"	4.667[a]	.097	Retain the null hypothesis.
9	Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? Ports are equally likely to occur.	"One-Sample Chi-Square Test"	4.000[a]	.046	"Reject the null hypothesis".
10	Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? Ships are equally likely to occur.	"One-Sample Chi-Square Test"	13.444[a]	.000	"Reject the null hypothesis".
11	Does the following maritime sector effectively promote maritime security with the technology mandated by various	"One-Sample Chi-Square Test"	9.000[a]	.003	"Reject the null hypothesis".

	IMO instruments? The likelihood of (Other Installations) happening is equal.				
12	Do you have access to the data bank for ships registered in your nation as a maritime law enforcement agency? happen with equal odds.	"One-Sample Chi-Square Test"	7.111[a]	.008	"Reject the null hypothesis".
13	To what extent do you believe the Ship Security Alarm System (SSAS) contributes to maritime security? happen with equal odds.	"One-Sample Chi-Square Test"	4.000[a]	.046	"Reject the null hypothesis".
14	Have you handled any security-related issues at work? occur with equal odds.	"One-Sample Chi-Square Test"	7.111[a]	.008	"Reject the null hypothesis".
15	Regarding the aforementioned occurrence or incidents, how would you rank the response of the "Maritime Administration" and "maritime law enforcement agencies"? happen with equal odds.	"One-Sample Chi-Square Test"	13.444[a]	.000	"Reject the null hypothesis".
16	Does the Automatic	"One-Sample Chi-Square	1.000[a]	.317	Retain the null

	Identification System (2) promote or hinder security? happen with equal odds.	Test"			hypothesis.
17	Does the Vessel Traffic System (VTS) promote or hinder security? happen with equal odds.	"One-Sample Chi-Square Test"	13.444[a]	.000	"Reject the null hypothesis".
18	Is VTS an active security threat mitigation strategy or a deterrent? happen with equal odds.	"One-Sample Chi-Square Test"	.000[a]	1.000	Retain the null hypothesis.
19	Will required Vessel Traffic System (VTS) reporting improve local security as a whole? occur with equal odds.	"One-Sample Chi-Square Test"	11.111[a]	.001	"Reject the null hypothesis".
20	Will connecting radar to two improve operator effectiveness in seeing security incidents early and preventing them? happen with equal odds.	"One-Sample Chi-Square Test"	13.444[a]	.000	"Reject the null hypothesis".
21	Will the goal of safe transportation be aided or hindered by long-range identification and tracking of ships (LRIT)? happen with	"One-Sample Chi-Square Test"	4.000[a]	.046	"Reject the null hypothesis".

	equal odds.				
22	Do you have any prior experience inspecting containers for security? happen with equal odds.	"One-Sample Chi-Square Test"	4.000[a]	.046	"Reject the null hypothesis".
23	What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment? happen with equal odds.	"One-Sample Chi-Square Test"	1.778[a]	.182	Retain the null hypothesis.
24	Numerous systems exist throughout the world, including the Indian (Maritime) Search and Rescue Computerised System (INDSAR), the Japanese System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). occur in your o with equal chances.	"One-Sample Chi-Square Test"	5.444[a]	.020	"Reject the null hypothesis".
25	Do you believe that all ships on international journeys should be required to report to one of the	"One-Sample Chi-Square Test"	5.444[a]	.020	"Reject the null hypothesis".

	World Wide One systems? happen with equal odds.				
26	In terms of training, does the Vessel Data Recorder (VDR) improve maritime security? happen with equal odds.	"One-Sample Chi-Square Test"	16.000[a]	.000	"Reject the null hypothesis".
27	Is there any analytical benefit to maritime security from the Vessel Data Recorder (VDR)? occur with equal odds.	"One-Sample Chi-Square Test"	4.000[a]	.046	"Reject the null hypothesis".

Asymptotic significances are displayed. The significance level is .050.

A one-sample chi-square test was used to assess the question "Do you feel, in the present-day scenario, there is a need to enhance maritime security?" At the.000 level of significance, the test statistic has a value of 21.778. This study's null hypothesis, which predicted that all replies would be equally likely (i.e., without strong opinions in either direction), is rejected since the p-value is less than the conventional significance level (usually.05). This result suggests that respondents overwhelmingly believe there is a need to enhance maritime security in the present-day context, indicating a significant level of agreement on the importance of bolstering security measures in this field.

Using a one-sample chi-square test, the question "In your opinion, which crime poses the greatest threat to the maritime sector?" was examined. A p-value of.004 is associated with the test statistic value of 17.333. We can rule out the possibility that all crimes are equally terrifying (the null hypothesis) because the p-value is less than the

conventional.05 level of significance. This result indicates that respondents do not view all crimes as equal threats; instead, there is a statistically significant preference or perception that certain crimes are more threatening to the maritime sector than others. This insight helps to identify which types of crime require more attention and resources in maritime security planning.

The question "In your opinion, are the instruments adopted by the IMO adequate to combat the above maritime crimes?" was analyzed using a one-sample chi-square test. With a p-value of.000, the test statistic value is 16.000. This study's null hypothesis, which predicted that respondents' views on the sufficiency of IMO instruments would be distributed evenly, is rejected since the p-value is smaller than the normal significance level, which is typically just.05. This result suggests that respondents hold a statistically significant view regarding the adequacy of IMO measures, indicating a predominant perception—either that the instruments are largely sufficient or insufficient to address maritime crimes. This finding highlights the importance of reassessing or reinforcing IMO measures based on the perception of their effectiveness among stakeholders.

The question "How frequently does the “Maritime Administration” interact for maritime security issues with law enforcement agencies?" was analyzed using a one-sample chi-square test. A p-value of.086 is associated with the test statistic value of 8.167. We keep the null hypothesis, which states that responses about interaction frequency are normally distributed, since the p-value is greater than the widely accepted significance level (.05). Based on these findings, it appears that there is no clear pattern to the frequency with which “Maritime Administration” and law enforcement organisations engage; rather, interactions may occur at varying frequencies. This could indicate that the frequency of interaction varies based on situational needs or other factors rather than a consistent routine.

The question "How are the data listed below being shared between the “Flag Administration” and maritime law enforcement agency? (Requirement basis)" used a one-sample chi-square test to analyse the data. A p-value of.002 is associated with the test statistic, which is 12.667. We may reject the null hypothesis, which held that replies on data-sharing procedures would occur with equal probabilities, because the p-value is smaller than the normal significance level of e. Based on this data, it seems that there is a clear preference or trend in the way data is shared between the “Flag Administration” and maritime law enforcement, particularly when it comes to requirements. This suggests that data-sharing practices are not equally distributed across various methods but are instead concentrated around certain procedures, likely indicating a more selective or conditional approach to data sharing. This insight can guide policy improvements for more standardized or frequent data exchanges where necessary.

The question "How are the data listed below being shared between the “Flag Administration” and maritime law enforcement agency? (Online)" was analyzed using a one-sample chi-square test. With a p-value of.039. The test statistic value is 6.500. We may reject the null hypothesis, which stated that replies regarding online data-sharing procedures occur with identical probabilities, because the p-value is less than the standard significance level of.05. This result suggests that respondents have a statistically significant perception about the frequency or manner in which data is shared online between the “Flag Administration” and maritime law enforcement. This may indicate that online data sharing is not uniformly practiced, with certain frequencies or patterns of use being more common. This finding could imply either a predominant reliance on or a limited adoption of online methods, potentially guiding stakeholders to evaluate the consistency and effectiveness of online data-sharing protocols.

The question "How are the data listed below being shared between the “Flag Administration” and maritime law enforcement agency? (2 exchange of data)" a one-sample chi-square test was used for research. After calculating the p-value, the test statistic comes out as 12.667. We can reject the null hypothesis, which held that both the frequency and kind of data exchange would be responded to with equal probability, because the p-value is less than the conventional significance threshold, which is usually.05. Respondents see a statistically significant pattern in data interchange between “maritime law enforcement agencies” and the “Flag Administration”, according to this conclusion. This suggests that certain modes or frequencies of data exchange (possibly bilateral or reciprocal exchanges) are more common than others. Such a finding could highlight the importance of specific data-sharing protocols, potentially guiding the improvement or standardization of exchange practices to enhance collaboration and information flow between these entities.

The question "How are the data listed below being shared between the “Flag Administration” and maritime law enforcement agency? (My country does not have the system)" used a one-sample chi-square test to analyse the data. A p-value of.097 is associated with the test statistic value of 4.667. We keep the null hypothesis, which states that replies regarding this data-sharing system are distributed evenly, since the p-value is greater than the usual significance level (usually.05). This finding implies that respondents do not have a strong preference or trend regarding the presence of a data-sharing mechanism between their country's “Flag Administration” and maritime law enforcement. This could imply that opinions or awareness levels on the existence of such systems are varied, with no dominant response. This finding may highlight an area where further assessment is needed to understand the presence or absence of data-sharing systems across different countries.

The question "Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ports)" used a one-sample chi-square test to analyse the data. At the p-value level of.046, the test statistic value is 4.000. It was believed that replies regarding the usefulness of technology specified by the IMO in port security would occur with equal probabilities, but since the p-value is below the conventional significance level (usually.05), we reject this hypothesis. This result indicates that respondents have a statistically significant view on the effectiveness of IMO-mandated technology in enhancing port security. This suggests a predominant opinion—either that the technology is effective or that it has notable limitations—rather than a neutral or evenly split perspective. The finding may guide further examination of specific technologies and their impact on port security, potentially informing decisions about technology enhancements or adjustments under IMO frameworks.

The question "Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ships)" was analyzed using a one-sample chi-square test. The test statistic value is 13.444, with a p-value of .000. Since the p-value is below the standard significance level of .05, we reject the null hypothesis, which assumed that responses about the effectiveness of IMO-mandated technology for ships would occur with equal probabilities. This result indicates that respondents perceive the technology required under IMO instruments to be either highly effective or ineffective in fostering maritime security for ships, with a statistically significant preference in one direction. The findings suggest that the technology is viewed as playing an important role in improving maritime security on ships, or conversely, there might be concerns about its effectiveness. This

insight could be used to guide future assessments or improvements to the technologies mandated by the IMO for enhancing security in the maritime sector.

The result of the one-sample chi-square test indicates that the technology required under IMO instruments is perceived as significantly effective (or ineffective) in fostering maritime security in "Other Installations." The p-value is less than the.05 significance level, and the test statistic is 9.000. Respondents' views on the technology's efficacy are clearly biassed towards its effect on security in this domain, leading us to reject the null hypothesis.

The result of the one-sample chi-square test shows that the responses to the question "As a maritime law enforcement agency, do you have access to the data bank for the ships registered in your country?" are not equally likely to happen. The p-value is.008, which is less than the.05 significance level, and the test statistic is 7.111. Thus, we may conclude that maritime law enforcement organisations do, in fact, have access to the database of ships registered in their country, as opposed to a lack of clear preference or distribution, and we can reject the null hypothesis as a result.

The result of the one-sample chi-square test indicates that responses to the question "How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security?" are not equally likely to happen. With a p-value of only.046, the test statistic is 4.000, which is significantly lower than the.05 level of significance. In light of this evidence, we conclude that respondents do, in fact, hold strong opinions on the efficacy of SSAS in bolstering maritime security, leaning more towards a positive or negative than a neutral one.

The result of the one-sample chi-square test indicates that responses to the question "Have you dealt with a security incident in your place of work?" do not occur with equal probabilities. The test statistic is 7.111, with a p-value of .008, which is below

the .05 significance level. Therefore, we reject the null hypothesis, suggesting that there is a significant trend in the responses, meaning that dealing with a security incident in the workplace is either common or uncommon, rather than occurring with an equal likelihood.

The result of the one-sample chi-square test indicates that the responses to the question "How would you rate the response of “Maritime Administration” / “maritime law enforcement agencies” in the above incident(s)?" do not occur with equal probabilities. The test statistic is 13.444, with a p-value of .000, which is below the .05 significance level. Therefore, we reject the null hypothesis, suggesting that respondents perceive the response of “Maritime Administration” / “maritime law enforcement agencies” in the incident(s) as significantly different—either more positive or more negative—rather than having an evenly distributed opinion.

The result of the one-sample chi-square test indicates that responses to the question "Is the Automatic Identification System (2) fostering security or is it a hindrance?" occur with equal probabilities. The test statistic is 1.000, with a p-value of .317, which is greater than the standard significance level of .05. Therefore, we retain the null hypothesis, suggesting that there is no significant preference or trend in the responses. This implies that opinions on whether the Automatic Identification System (2) fosters security or acts as a hindrance are evenly distributed among respondents.

The result of the one-sample chi-square test indicates that the responses to the question "Is Vessel Traffic System (VTS) fostering security or is it a hindrance?" do not occur with equal probabilities. The test statistic is 13.444, with a p-value of .000, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents have a significant opinion on the effectiveness of the Vessel Traffic System (VTS) in fostering security or acting as a hindrance. This indicates a clear

trend in the perception of VTS, either viewed as fostering security or posing challenges, rather than an evenly distributed or neutral response.

The result of the one-sample chi-square test indicates that the responses to the question "Is VTS a deterrent or an active measure for mitigating security threat?" occur with equal probabilities. The test statistic is 0.000, with a p-value of 1.000, which is greater than the standard significance level of .05. Therefore, we retain the null hypothesis, suggesting that there is no significant preference or trend in the responses. This means that opinions on whether the Vessel Traffic System (VTS) serves more as a deterrent or an active measure for mitigating security threats are evenly distributed among respondents.

The result of the one-sample chi-square test indicates that the responses to the question "Will mandatory reporting to Vessel Traffic System (VTS) enhance overall security in the area?" do not occur with equal probabilities. The test statistic is 11.111, with a p-value of .001, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents have a statistically significant opinion on whether mandatory reporting to VTS would enhance overall security. This indicates a clear trend in the responses, with most respondents likely viewing mandatory reporting as beneficial for improving security, rather than having an evenly distributed or neutral opinion.

The result of the one-sample chi-square test indicates that the responses to the question "Will interfacing of radar with 2 enhance the operator efficiency in early identification and prevention of security incidents from occurring?" do not occur with equal probabilities. The test statistic is 13.444, with a p-value of .000, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents perceive a significant trend regarding the impact of radar interfacing on

operator efficiency. This indicates that most respondents believe that interfacing radar with the system enhances operator efficiency in early identification and prevention of security incidents, rather than there being an evenly distributed or neutral opinion.

The result of the one-sample chi-square test indicates that the responses to the question "Will long-range identification and tracking of ships (LRIT) foster the objective of secure shipping or will be a hindrance?" do not occur with equal probabilities. The test statistic is 4.000, with a p-value of .046, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents have a significant opinion on whether LRIT fosters secure shipping or acts as a hindrance. This indicates a clear trend, with respondents likely seeing LRIT as either beneficial for security or problematic, rather than having an evenly distributed or neutral perspective.

The result of the one-sample chi-square test indicates that the responses to the question "Do you have any experience in security scanning of containers?" do not occur with equal probabilities. The test statistic is 4.000, with a p-value of .046, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that there is a significant trend in the responses. This means that respondents either have experience in security scanning of containers or do not, rather than having an evenly distributed or neutral opinion.

The result of the one-sample chi-square test indicates that the responses to the question "Taking into consideration the security risk and commercial commitment of ship owners, what in your opinion would be the best solution for enhancing maritime security will be?". The test statistic is 1.778, with a p-value of .182, which is greater than the standard significance level of .05. Therefore, we retain the null hypothesis, suggesting that there is no significant preference or trend in the responses. This means that opinions

on the best solution for enhancing maritime security are evenly distributed among the respondents, with no clear consensus emerging.

The result of the one-sample chi-square test indicates that the responses to the question "There are different systems worldwide, such as Automated Mutual-Assistance Vessel Rescue System (AMVER), Japanese System (JASREP), Indian (Maritime) Search and Rescue Computerized System (INDSAR), etc. In your opinion, do these systems effectively contribute to maritime security?" do not occur with equal probabilities. The test statistic is 5.444, with a p-value of .020, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that there is a significant difference in the responses, indicating a general consensus either for or against the effectiveness of these systems in enhancing maritime security.

The result of the one-sample chi-square test indicates that the responses to the question " In your opinion should reporting to any one of the world wide 1 systems be made mandatory for all ships on international voyages?" do not occur with equal probabilities. The test statistic is 5.444, with a p-value of .020, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents have a significant opinion on whether reporting to one of the worldwide systems should be mandatory for all ships on international voyages. This indicates a clear trend in the responses, likely indicating a preference for or against the mandatory reporting requirement, rather than an evenly distributed or neutral viewpoint.

The result of the one-sample chi-square test indicates that the responses to the question "Does the Vessel Data Recorder (VDR) add value to maritime security with regard to training?" do not occur with equal probabilities. The test statistic is 16.000, with a p-value of .000, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents perceive the VDR as having a

significant impact on maritime security training. This indicates a clear trend, with respondents either viewing the VDR as valuable for training purposes or not, rather than having an evenly distributed or neutral opinion.

The result of the one-sample chi-square test indicates that the responses to the question "Does the Vessel Data Recorder (VDR) add value to maritime security with regard to analysis?" do not occur with equal probabilities. The test statistic is 4.000, with a p-value of .046, which is below the standard significance level of .05. Therefore, we reject the null hypothesis, suggesting that respondents perceive the VDR as significantly contributing to maritime security analysis. This indicates a clear trend, with respondents either viewing the VDR as valuable for analysis or not, rather than having an evenly distributed or neutral opinion.

4.3 Shipping Companies

Reliability

Table 4.72: "Reliability Statistics"

Cronbach's Alpha	N of Items
.816	25

The above table 4.1 shows Cronbach's Alpha of 0.816, your 25-item scale shows good internal consistency, indicating reliable measurement of the construct.

Frequency Table

Table 4.73: Do you think that marine security has to be improved in the current situation?

	Frequency	Percent
Yes	32	91.4
No	3	8.6
Total	35	100.0

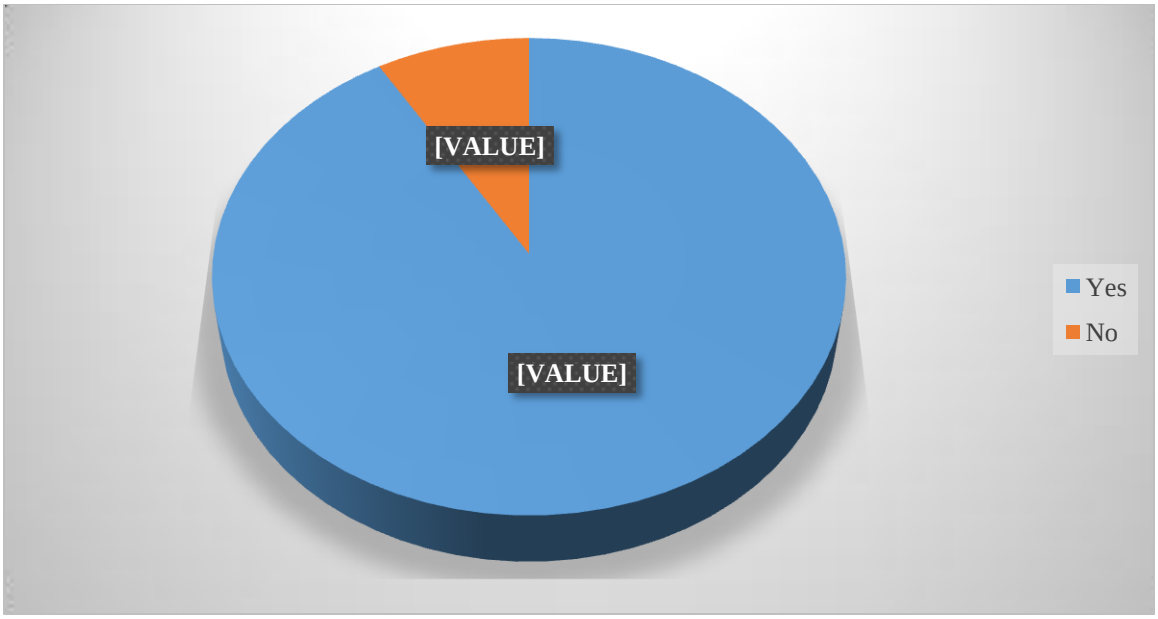


Figure 4.61: Do you think that improving maritime security is necessary in the current situation?

The above Figure 4.61 shows that a significant majority of respondents (91.4%) believe there is a need to enhance maritime security in the current scenario, with only a small portion (8.6%) indicating otherwise.

Table 4.74: Which crime, in your opinion, is the biggest danger to the maritime industry?

	Frequency	Percent
"Piracy and Armed Robbery Against Ships"	9	25.7
"Maritime Drug Trafficking and Terrorism"	9	25.7
Illegal Migration	7	20.0
Stowaways	6	17.1
Human Trafficking	3	8.6
Container Crimes	1	2.9
Total	35	100.0

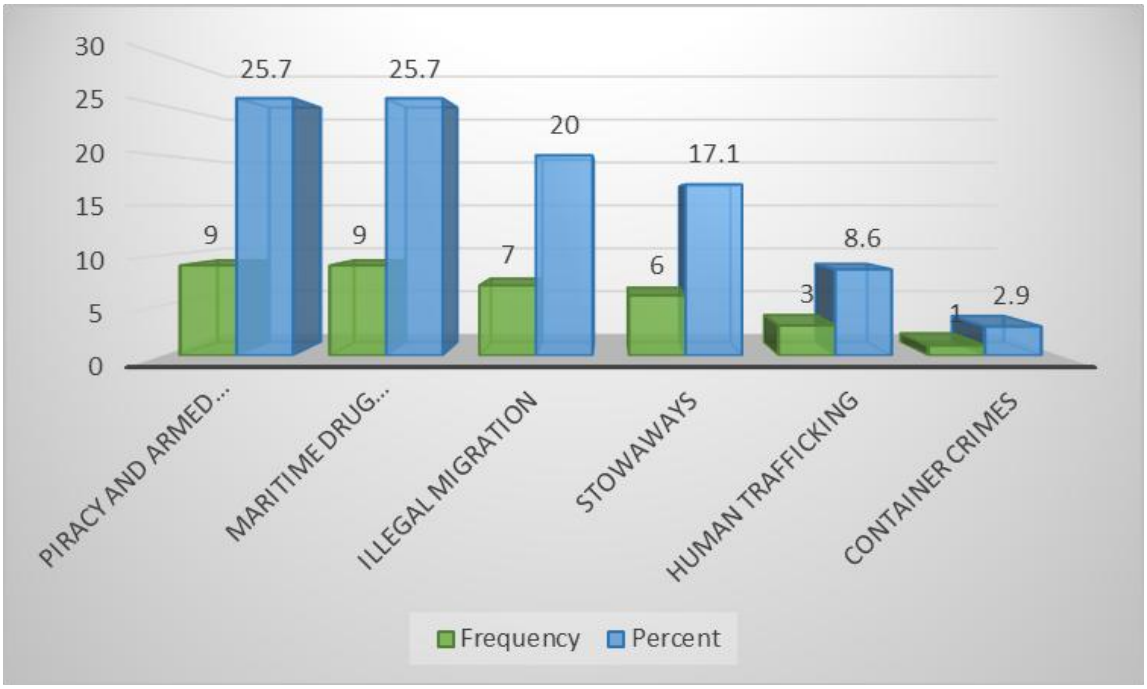


Figure 4.62: What do you think is the biggest threat to the marine industry?

According to above Figure 4.62 shows varied perceptions regarding the greatest crime threats to the maritime sector. The top concerns are Piracy and Armed Robbery Against Ships and "Maritime Drug Trafficking" and Terrorism, each known by 25.7% of respondents, suggesting these issues are seen as equally significant threats. Illegal Migration follows, mentioned by 20% of participants, while Stowaways are viewed as a primary concern by 17.1%. Lesser concerns include Human Trafficking (8.6%) and Container Crimes (2.9%).

Table 4.75: Do you think the IMO's adopted tools are sufficient to address the aforementioned marine crimes?

	"Frequency"	"Percent"
"Yes"	"29"	"82.9"
"No"	"6"	"17.1"
"Total"	"35"	"100.0"

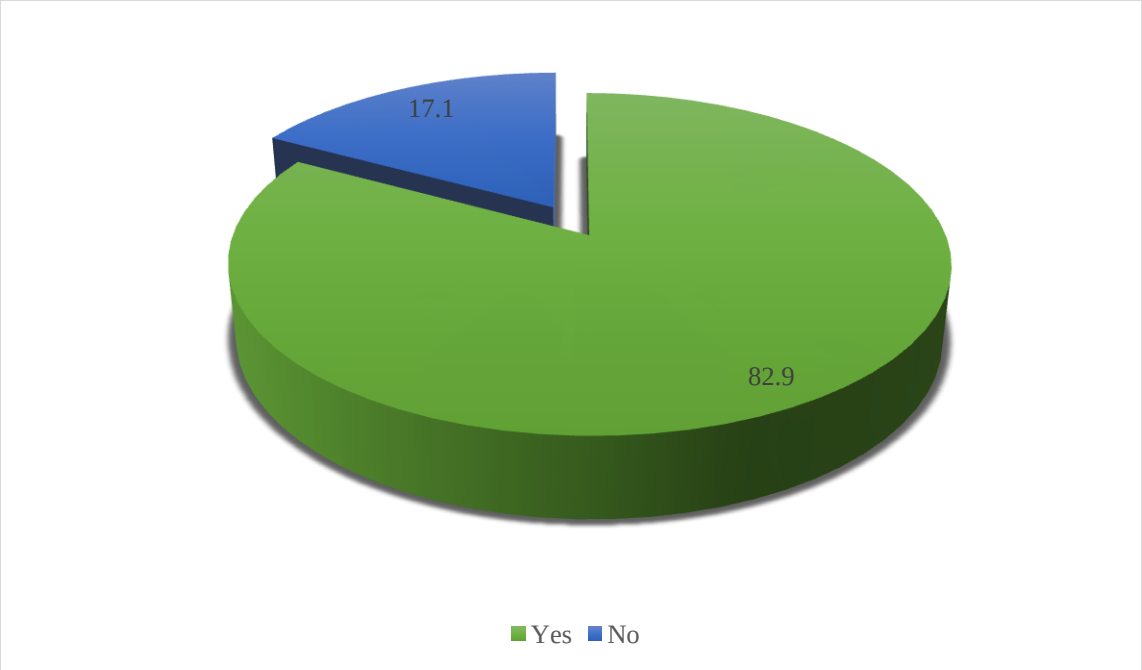


Figure 4.63: Are the IMO's established tools sufficient to combat the aforementioned marine crimes, in your opinion?

The majority of respondents (82.9%) believe the instruments adopted by the IMO are adequate for combating maritime crimes as shown in figure 4.63 above. However, a minority (17.1%) view these instruments as insufficient.

Table 4.76: Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? (Ports)

	"Frequency"	"Percent"
"Yes"	"29"	"82.9"
"No"	"6"	"17.1"
"Total"	"35"	"100.0"

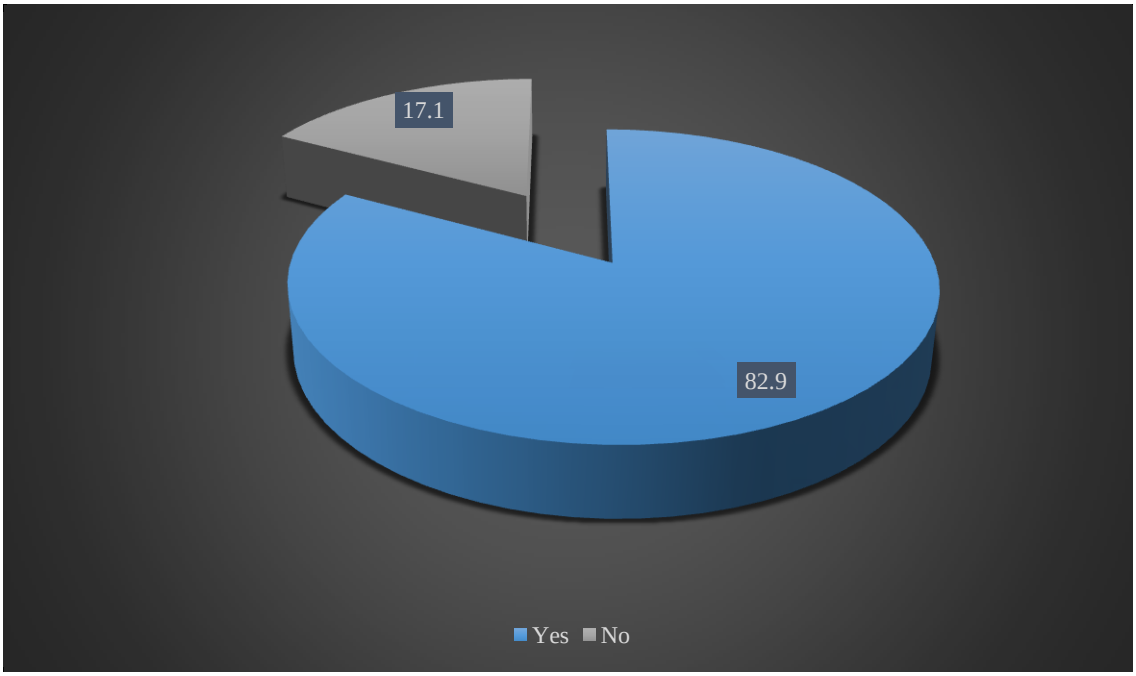


Figure 4.64: In the following maritime sector areas, is the technology mandated by various IMO instruments effective in promoting maritime security? (Ports)

As per the above Figure 4.64 shows that a substantial majority of respondents (82.9%) consider the technologies needed to effectively promote marine security in port regions as required by several IMO treaties. However, 17.1% of respondents feel the technology may not be fully effective,

Table 4.77: Does the technology mandated by several IMO instruments effectively promote marine security in the maritime industry listed below? (Ships)

	Frequency	Percent
Yes	29	82.9
No	6	17.1
Total	35	100.0

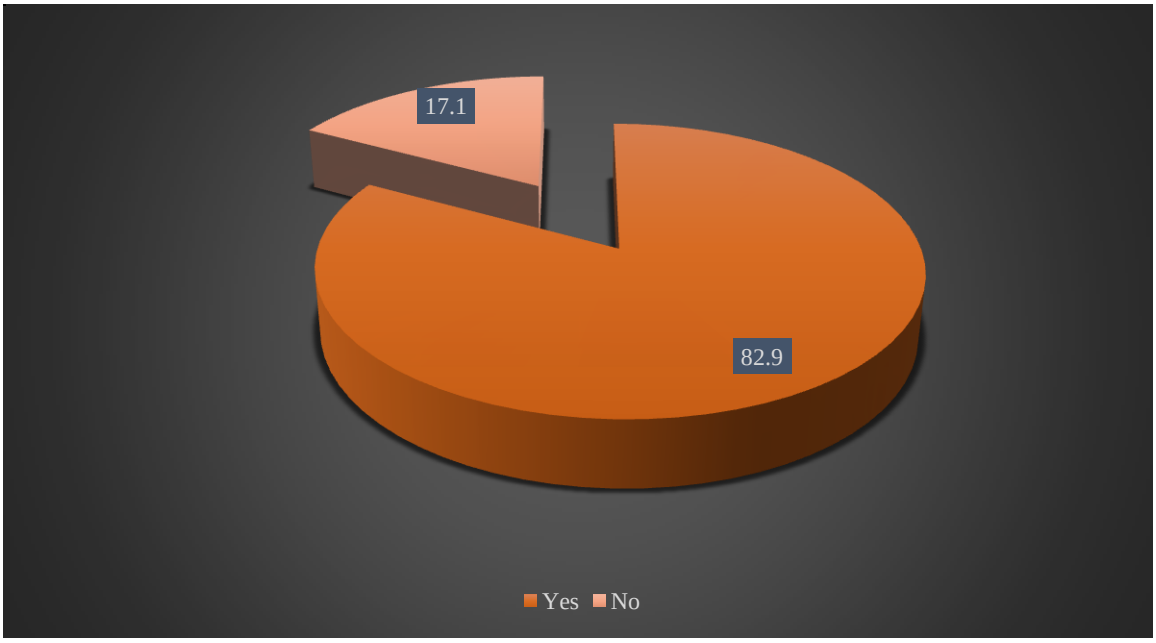


Figure 4.65: Does the marine sector's use of the technology mandated by several IMO instruments effectively promote maritime security listed below? (Ships)

The majority of respondents (82.9%) think that the technology mandated by IMO instruments is effective in enhancing maritime security on ships, as seen in Figure 4.65 above. 17.1% of respondents, however, believe that the technology is not entirely successful.

Table 4.78: Do the various IMO instruments' requirements for technology effectively promote maritime security in the maritime industry listed below? (Other Installations)

	“Frequency”	“Percent”
“Yes”	”28””	”80.0”
“No”	”7”	”20.0”
“Total”	”35”	”100.0”

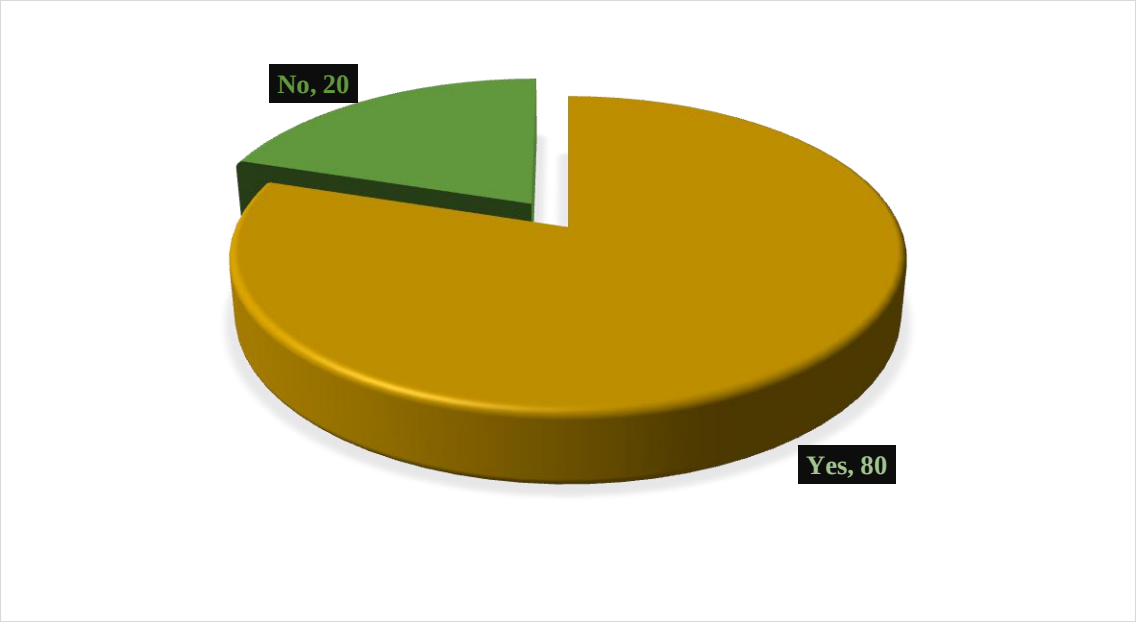


Figure 4.66: Does the maritime industry's use of the technology mandated by several IMO instruments effectively promote maritime security listed below? (Other Installations)

Eighty percent of respondents think that the technology mandated by IMO instruments is effective in improving maritime security in other facilities, as seen in Figure 4.66 above. However, 20% of respondents disagree.

Table 4.79: How does your company encourage employees to follow security policies?

	Frequency	Percent
"Financial incentives", such as "reward money"/"out-of-turn" giving certificates or promotion medals, etc.	19	54.3
Recognition in public, by insignia or than above	12	34.3
Other incentives Mentioned response	4	11.4
Total	35	100.0

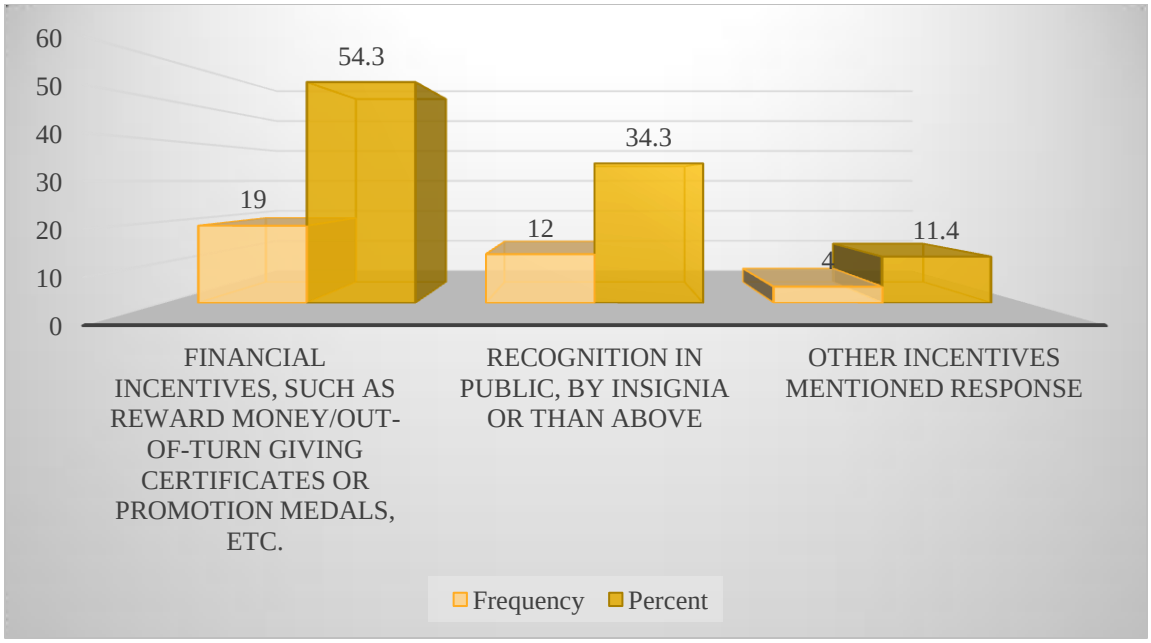


Figure 4.67: How does your company encourage employees to follow security protocols?

According to above Figure 4.67 shows that the most common method for motivating staff to comply with security guidelines is through financial incentives, such as reward money, certificates, or promotion medals, as indicated by 54.3% of respondents. Public recognition follows, with 34.3% of respondents identifying it as a key motivator. A smaller portion (11.4%) mentioned other unspecified incentives.

Table 4.80: Do your flagships currently have enough personnel on board to meet security requirements?

	Frequency	Percent
Yes	29	82.9
No	6	17.1
Total	35	100.0

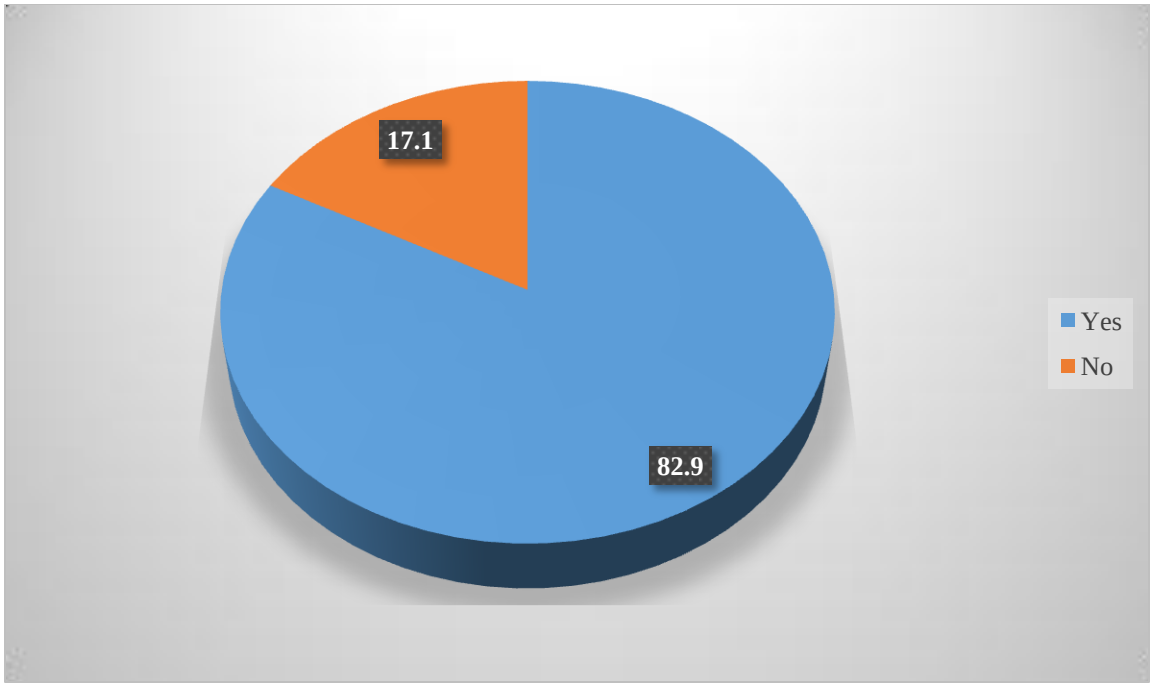


Figure 4.68: Are your flagships now manned at a sufficient degree to meet security requirements?

The majority of responders (82.9%) think that the current manning levels on their flagships are adequate to comply with security regulations, as seen in Figure 4.68 above. Still, 17.1% of those surveyed believe that there is not enough staff.

Table 4.81: As of right now, certain flag state administrations are issuing safe manning certifications without paying enough attention to the trading of vessels, onboard administrative tasks, and security standards. Considering the current global security situation,

	"Frequency"	"Percent"
"Yes"	30	85.7
"No"	5	14.3
"Total"	35	100.0

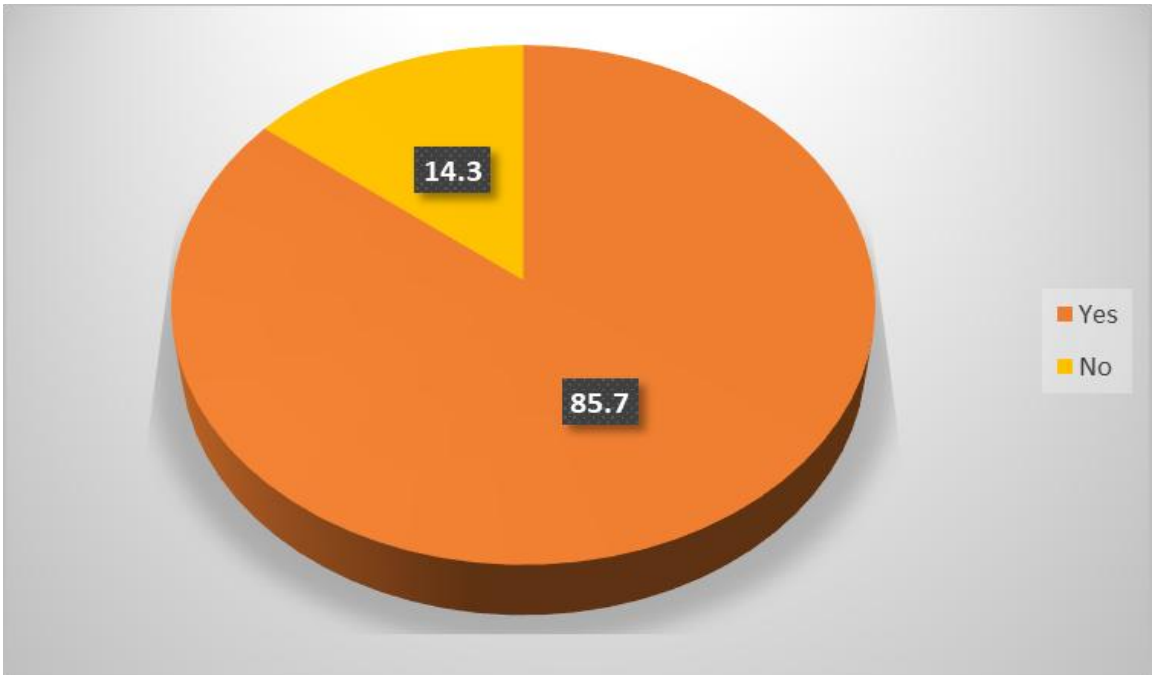


Figure 4.69: As of right now, certain flag state administrations are issuing safe manning certifications without paying enough attention to the trading of vessels, onboard administrative tasks, and security standards. Considering the current global security situation,

According to above Figure 4.69, Given the current state of international security, a sizable majority of respondents (85.7%) think that some flag state administrations issue safe manning certificates without giving enough thought to the trading, onboard administrative work, and security requirements of the vessels. 14.3%, however, disagree with this opinion.

Table 4.82: To what extent do you believe the Ship Security Alarm System (SSAS) contributes to maritime security?

	Frequency	Percent
"Effective"	25	71.4
"Not Effective"	10	28.6
Total	35	100.0

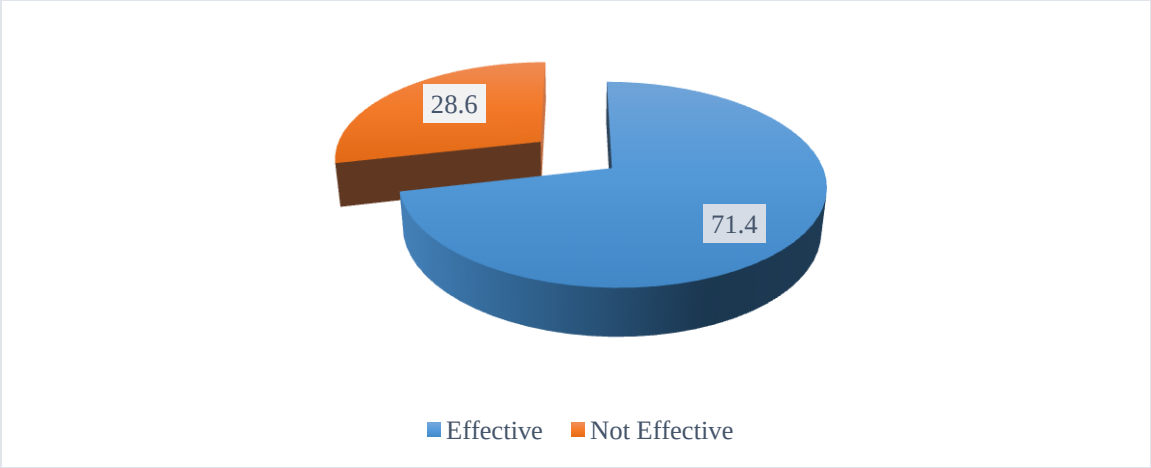


Figure 4.70: In your opinion, how successful is the Ship Security Alarm System's (SSAS) contribution to maritime security?

The "Ship Security Alarm System" (SSAS) in promoting "maritime security" in above figure 4.70, the majority of respondents (71.4%) consider as effective. However, 28.6% of respondents believe the system is not effective,

Table 4.83: Have you had to handle a security incident at work?

	Frequency	Percent
Yes	26	74.3
No	9	25.7
Total	35	100.0

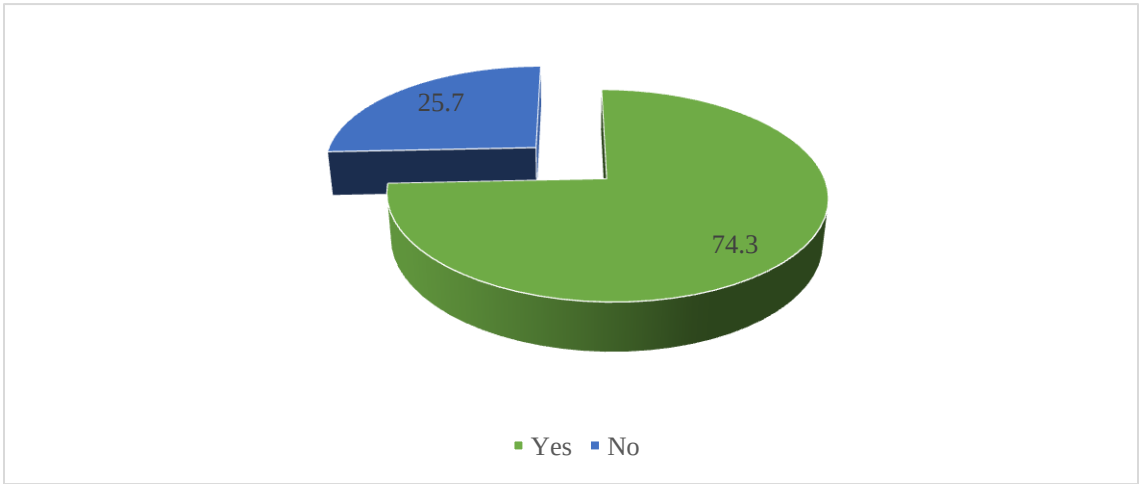


Figure 4.71: Have you handled any security-related issues at work?

The majority of respondents (74.3%) have dealt with a security incident in their place of work, as seen in Figure 4.71 above. However, 25.7% of those surveyed said they had never had a security incident.

Table 4.84: Regarding the aforementioned occurrence or incidents, how would you rank the response of the "Maritime Administration" and "maritime law enforcement agencies"?

	Frequency	Percent
"Effective"	26	74.3
"Inadequate"	9	25.7
Total	35	100.0

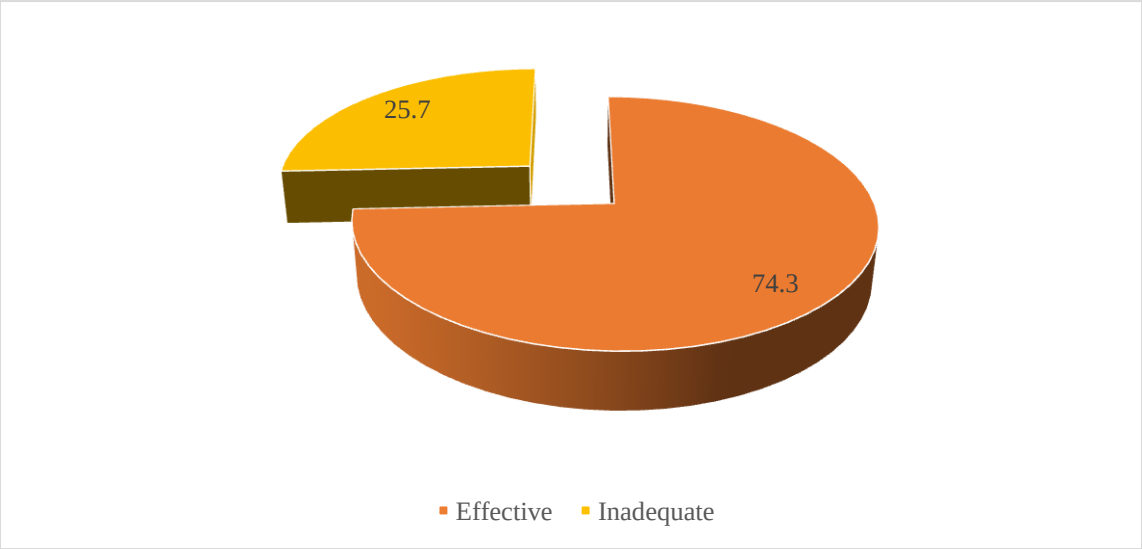


Figure 4.72: How would you rank the "Maritime Administration's" and Maritime Law Enforcement's response to the occurrence or incidents mentioned above?

The response of "Maritime Administration" and "maritime law enforcement agencies" is shown in above figure 4.72, the majority of respondents (74.3%) are effective. However, 25.7% of respondents consider the response to be inadequate.

Table 4.85: Does the Automatic Identification System (AIS) promote or hinder security?

	"Frequency"	"Percent
Effective for security	"25"	"71.4"

Hindrance for security	“10”	“28.6”
“Total”	“35”	“100.0”

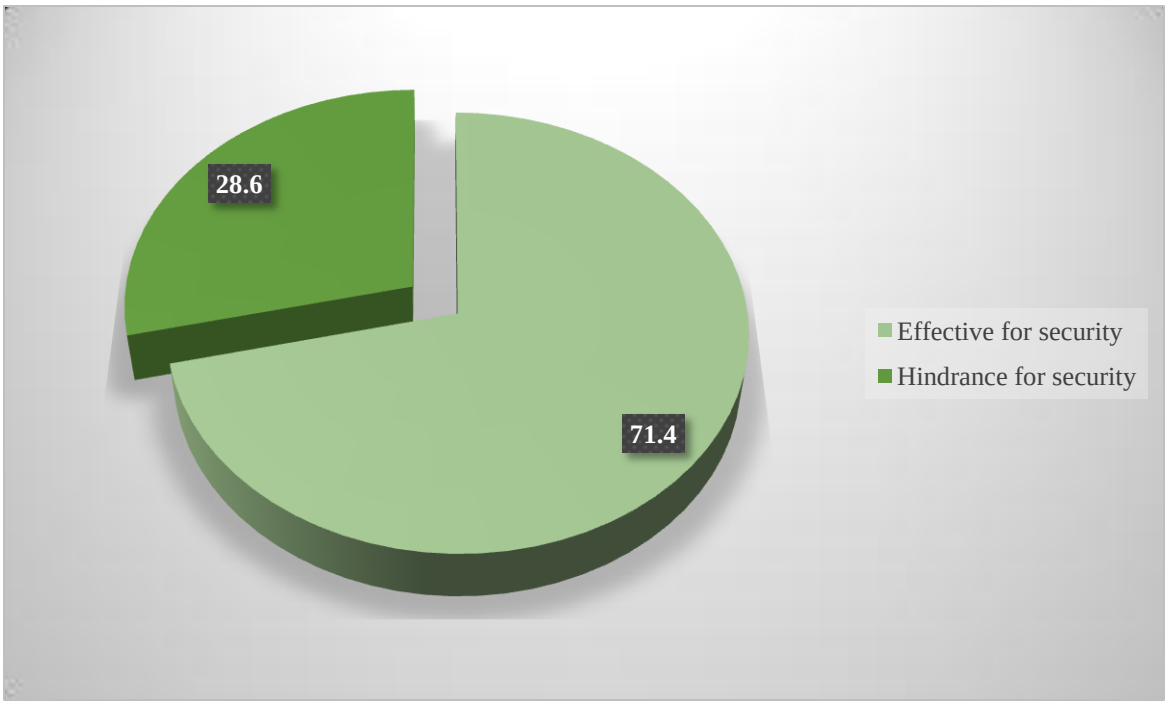


Figure 4.73: Does the Automatic Identification System (AIS) promote security or contribute to it?

The AIS is seen as effective for security by 71.4% of respondents, as shown in Figure 4.73 above. However, according to 28.6% of respondents, AIS is a hindrance to security.

Table 4.86: Does the Vessel Traffic System (VTS) promote security or hinder it?

	Frequency	Percent
Effective for security	23	65.7
Hindrance for security	12	34.3
Total	35	100.0

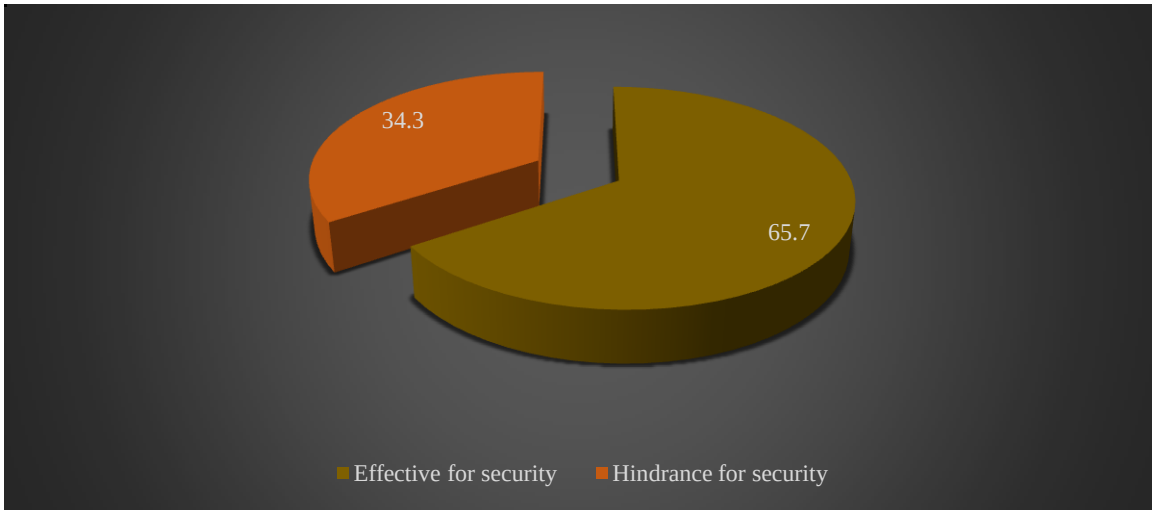


Figure 4.74: Does the Vessel Traffic System (VTS) promote or hinder security?

The Vessel Traffic System (VTS) above Figure 4.74 shows that 65.7% of respondents are effective for security. However, 34.3% of respondents consider VTS a hindrance to security.

Table 4.87: Is VTS an active security threat mitigation strategy or a deterrent?

	Frequency	Percent
"Deterrent"	22	62.9
"Active measure"	13	37.1
Total	35	100.0

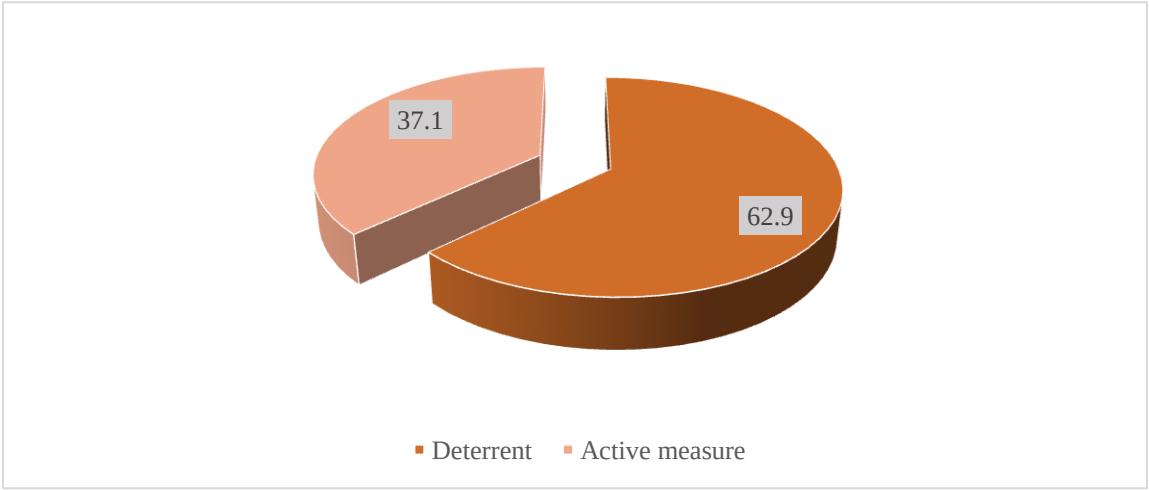


Figure 4.75: Does VTS actively mitigate security threats or is it merely a deterrent?

According to Figure 4.75 above, 62.9% of respondents believe that the VTS deterrents security concerns. VTS is seen by 37.1% of respondents as an active measure threat mitigation strategy.

Table 4.88: Will requiring reporting to the Vessel Traffic System (VTS) improve local security as a whole?

	Frequency	Percent
Yes	30	85.7
No	5	14.3
Total	35	100.0

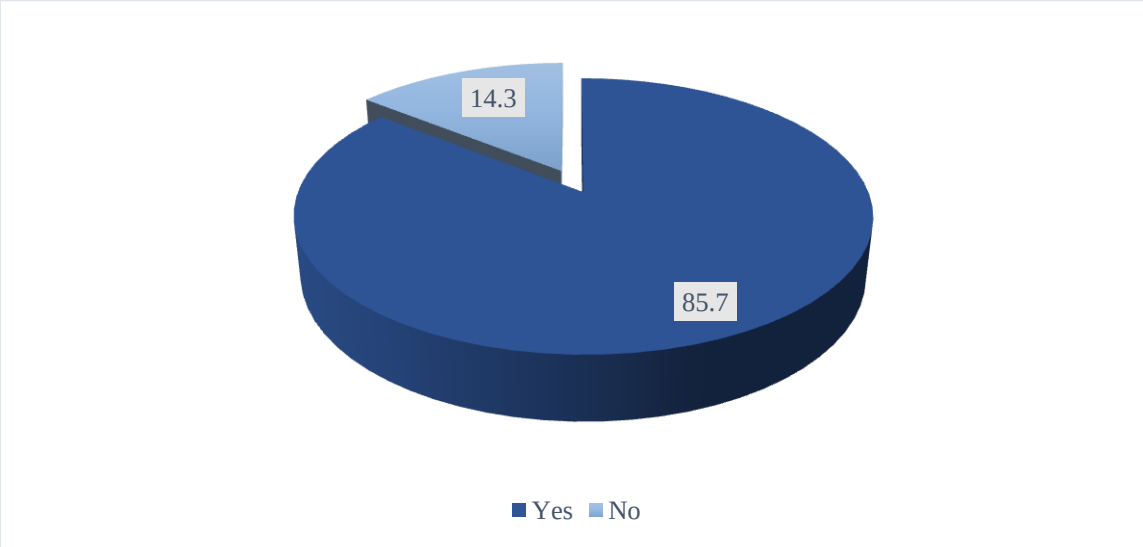


Figure 4.76: Will required Vessel Traffic System (VTS) reporting improve local security as a whole?

The above Figure 4.76 shows that a strong majority of respondents (85.7%) believe that mandatory reporting to VTS will enhance overall security in the area. In contrast, 14.3% of respondents disagree.

Table 4.89: Will the operator's efficiency in identifying and preventing security incidents be improved by radar-AIS interface?

	Frequency	Percent
Yes	25	71.4

No	10	28.6
Total	35	100.0

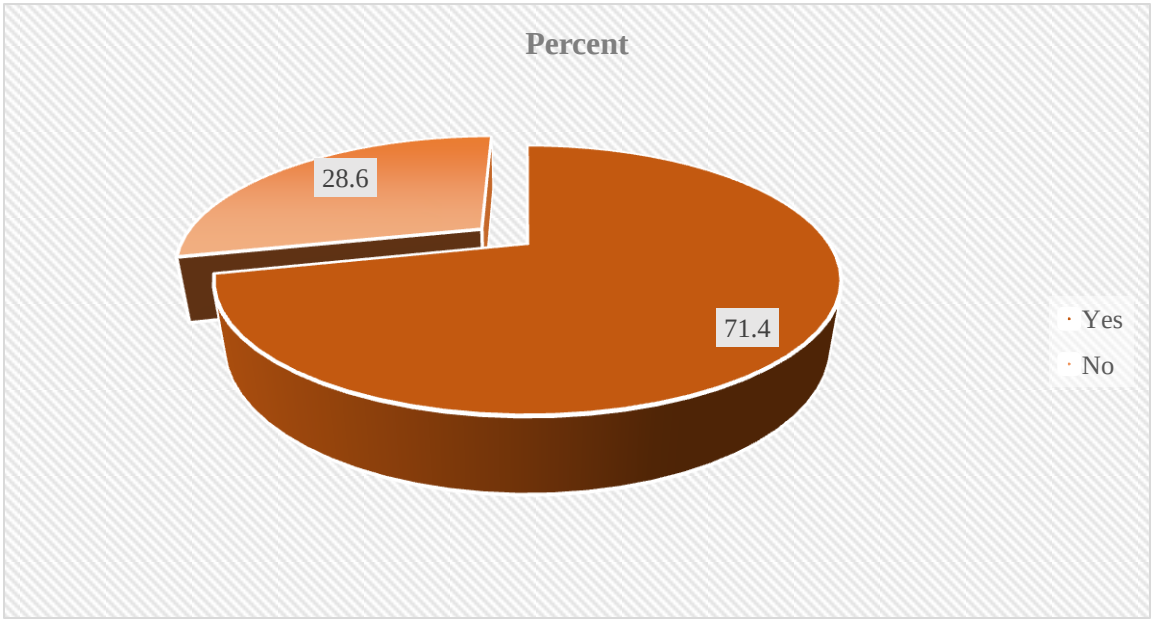


Figure 4.77: Will radar and AIS interface improve operator effectiveness in identifying threats early and averting security incidents?

According to 71.4% of respondents, integrating radar with the Automatic Identification System (AIS) will enhance operator efficiency in identifying and preventing security issues, as seen in Figure 4.77 above. However, according to 28.6% of respondents, efficiency might not be increased.

Table 4.90: Will the goal of safe transportation be aided or hindered by long-range identification and tracking of ships (LRIT)?

	Frequency	Percent
"Foster maritime security"	25	71.4
"Will be a hindrance"	10	28.6
Total	35	100.0

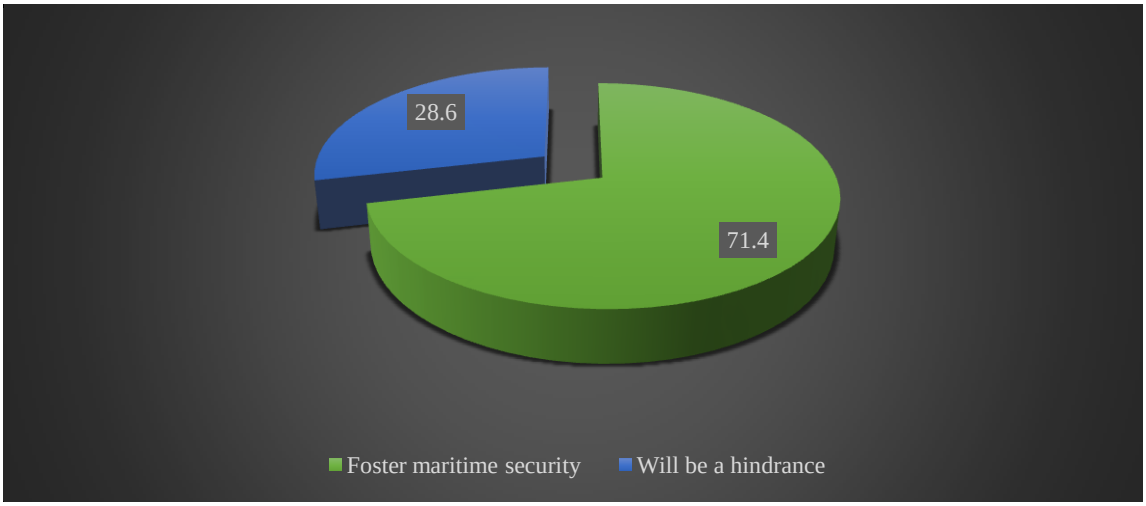


Figure 4.78: Is long-range identification and tracking of ships (LRIT) going to help or hurt the goal of safe shipping?

The LRIT will foster the objective of security the above Figure 4.78 shows that 71.4% Foster maritime security. However, 28.6% of respondents view it as a hindrance.

Table 4.91: Do you have any prior experience inspecting containers for security?

	Frequency	Percent
Yes	23	65.7
No	12	34.3
Total	35	100.0

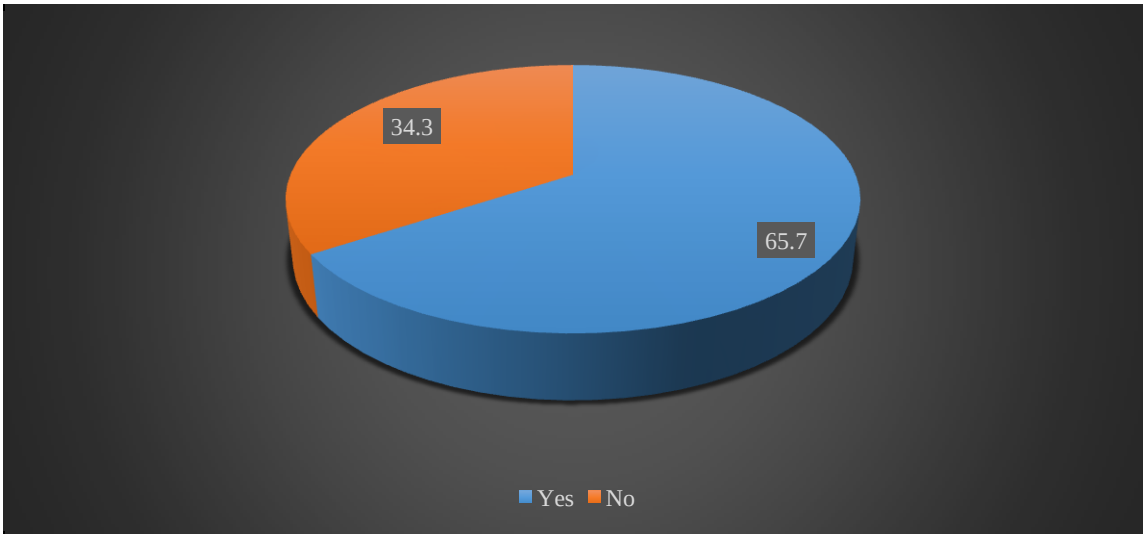


Figure 4.79: Do you have any prior container security screening experience?

According to above Figure 4.79 shows that 65.7% of respondents have experience in security scanning of containers. In contrast, 34.3% of respondents have not had such experience.

Table 4.92: What do you think would be the greatest way to improve maritime security, taking into account the trade commitment of ship owners and the security risk?

	Frequency	Percent
"Random scanning"	20	57.1
100% scanning	15	42.9
Total	35	100.0

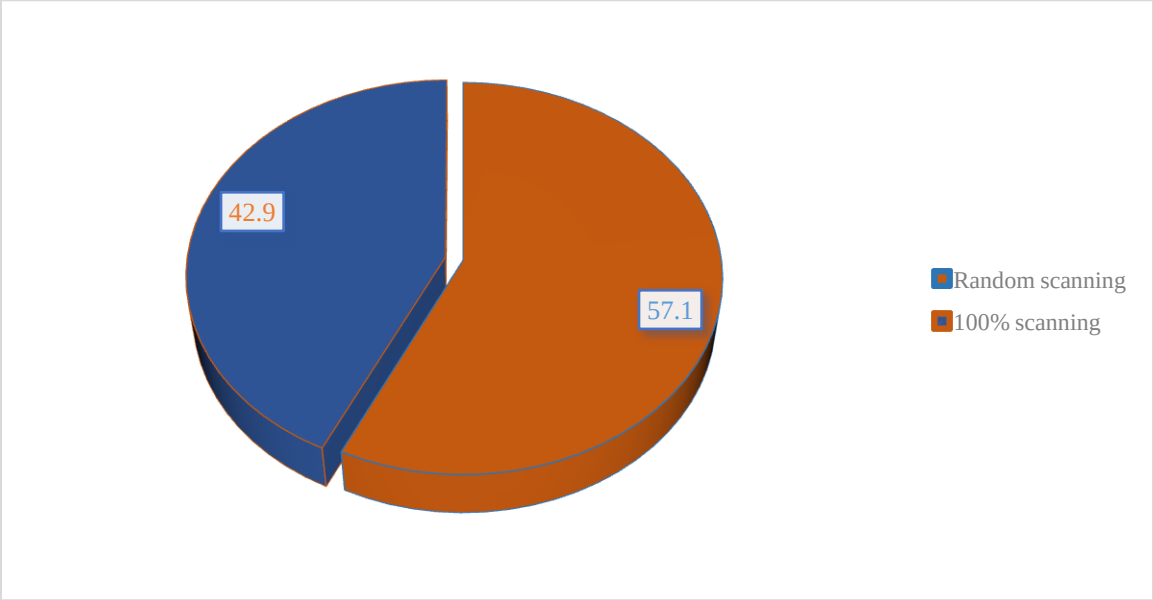


Figure 4.80: Which, in your opinion, would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment?

The best solution for enhancing maritime security, suggests that this approach strikes a balance between security risks and commercial commitments of ship owners as above Figure 4.20 shows that 57.1% of respondents are random scanning. On the other hand, 42.9% support 100% scanning.

Table 4.93: Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER).

	"Frequency"	"Percent"
"Yes"	30	85.7
"No"	5	14.3
"Total"	35	100.0

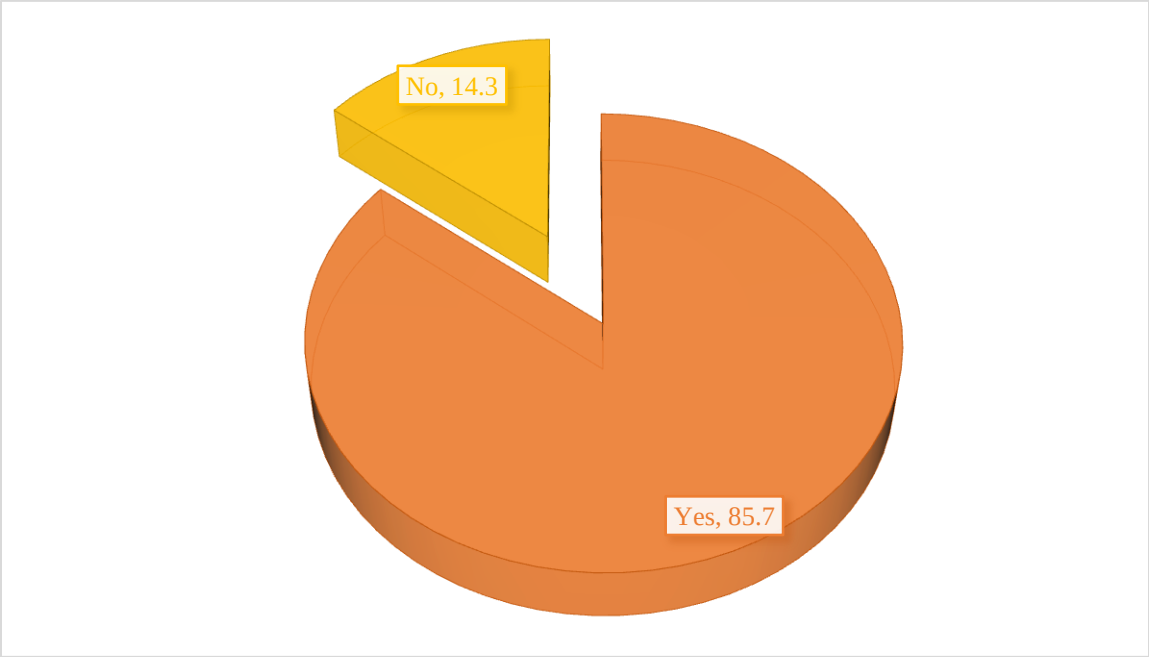


Figure 4.81: Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue system (AMVER).

The above figure 4.81 shows that 85.7% of respondents are aware of various ship reporting systems worldwide, such as AMVER, JASREP, and INDSAR. In contrast, 14.3% of respondents are not aware of these reporting systems.

Table 4.94: In the current security situation, would you rather have law enforcement keep an eye on your ship's location?

	Frequency	Percent

Yes	29	82.9
No	6	17.1
Total	35	100.0

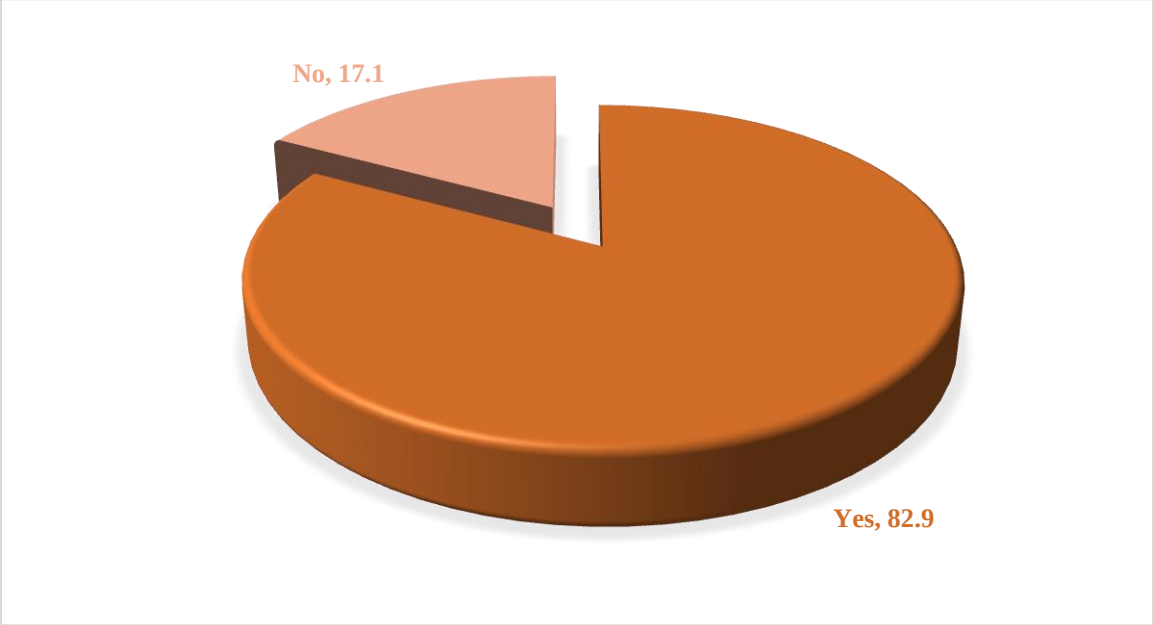


Figure 4.82: Which would you prefer—the position of your ship being tracked by law enforcement in the current security scenario?

According to the above figure 4.82 shows that a significant majority of respondents (82.9%) would prefer their ship's position to be monitored by "law enforcement agencies" in the current security scenario. However, 17.1% of respondents are not satisfied.

Table 4.95: Do you think all ships on international journeys should be required to report to one of the global ship reporting systems?

	Frequency	Percent
Yes	30	85.7
No	5	14.3
Total	35	100.0

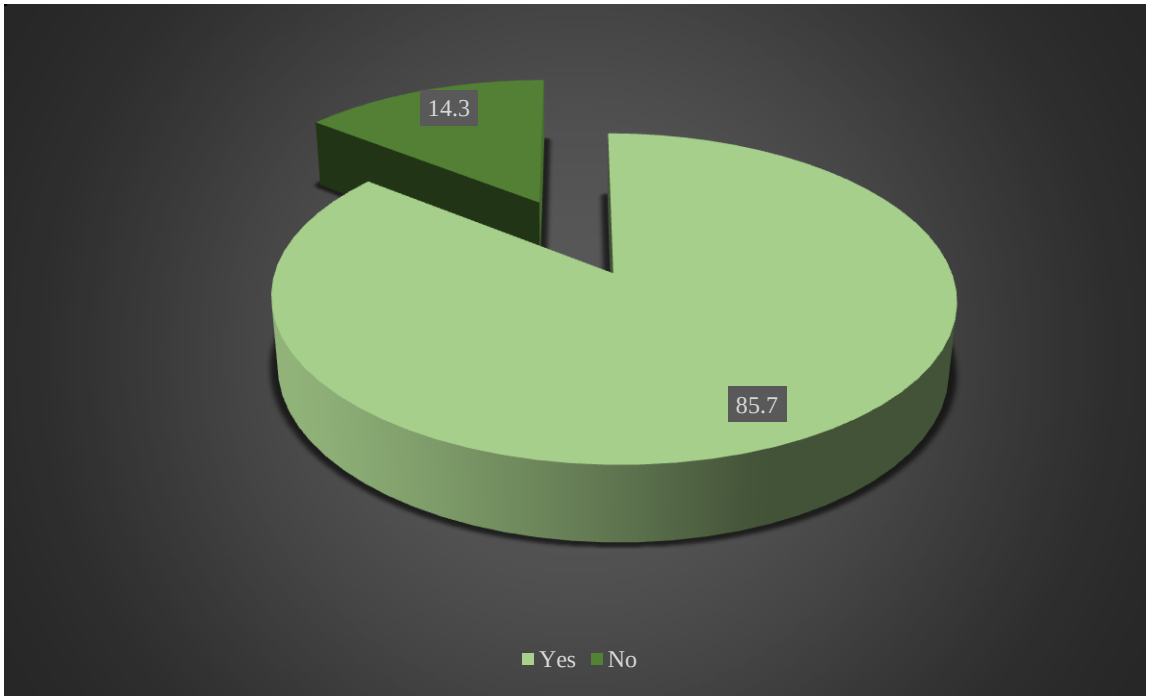


Figure 4.83: Should all ships on international journeys be required to report to one of the global ship reporting systems, in your opinion?

Since 85.7% of respondents are satisfied, it should be mandatory for all ships travelling internationally to use the global ship reporting systems (see Figure 4.83 above). 14.3% of respondents, however, express dissatisfaction.

Table 4.96: In terms of training, does the Vessel Data Recorder (VDR) improve maritime security?

	Frequency	Percent
Yes	28	80.0
No	7	20.0
Total	35	100.0

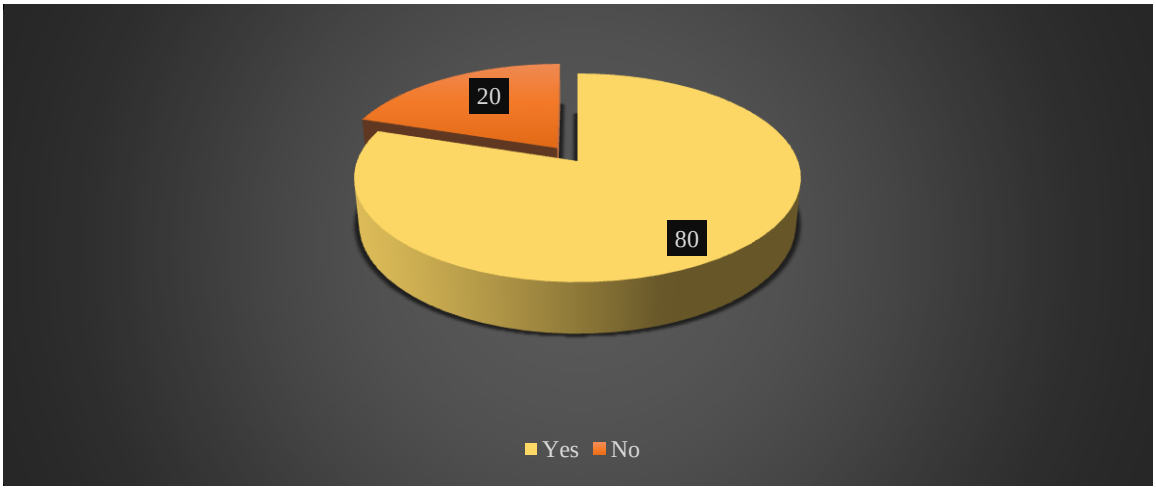


Figure 4.84: Does maritime security training benefit from the use of the Vessel Data Recorder (VDR)?

The VDR adds value to maritime security, the above Figure 4.84 shows that 80.0% of respondents believed. However, 20.0% of respondents are not them.

Table 4.97: In terms of analysis, does the Vessel Data Recorder (VDR) improve maritime security?

	Frequency	Percent
Yes	27	77.1
No	8	22.9
Total	35	100.0

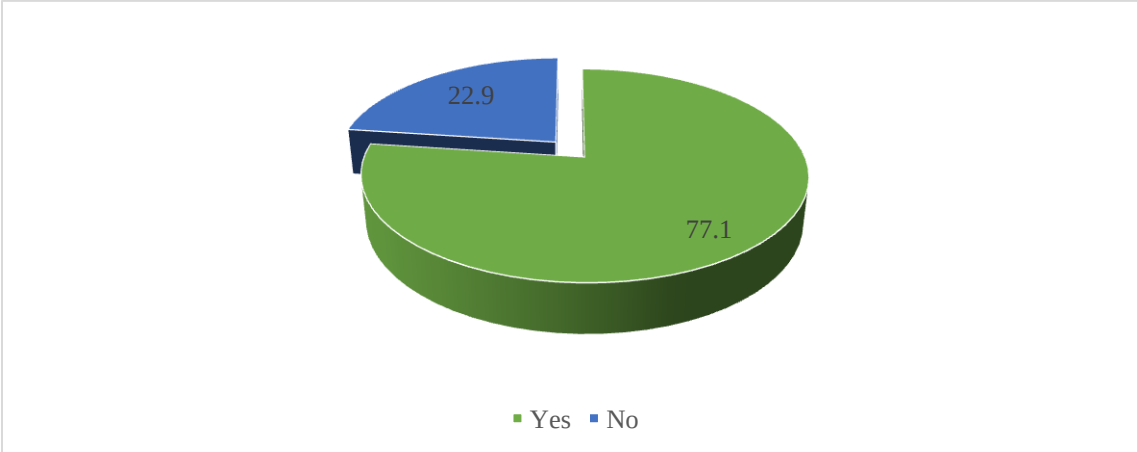


Figure 4.85: Is there an analytical benefit to maritime security from the Vessel Data Recorder (VDR)?

According to above Figure 4.85 shows that 77.1% of respondents believe the VDR adds value to maritime security in terms of analysis. However, 22.9% of respondents are not interested.

Nonparametric Tests

Table 4.98: "Hypothesis Test Summary"

	Null Hypothesis	Test	Test statistics	Sig.	Decision
1	Do you think that improving maritime security is necessary given the current situation? happen with equal odds.	"One-Sample Chi-Square Test"	24.029[a]	.000	"Reject the null hypothesis".
2	What do you think is the biggest threat to the marine industry? occur with equal odds.	"One-Sample Chi-Square Test"	9.057[a]	.107	Retain the null hypothesis.
3	Are the IMO's established tools sufficient to combat the aforementioned marine crimes, in your opinion? occur with equal odds.	"One-Sample Chi-Square Test"	15.114[a]	.000	"Reject the null hypothesis".
4	Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? Ports are equally likely to occur.	"One-Sample Chi-Square Test"	15.114[a]	.000	"Reject the null hypothesis".

5	Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? Ships are equally likely to occur.	“One-Sample Chi-Square Test”	15.114[a]	.000	“Reject the null hypothesis”.
6	Does the following maritime sector effectively promote maritime security with the technology mandated by various IMO instruments? The likelihood of (Other Installations) happening is equal.	“One-Sample Chi-Square Test”	15.114[a]	.000	“Reject the null hypothesis”.
7	How does your company encourage employees to follow security policies? happen with equal odds.	“One-Sample Chi-Square Test”	9.657[a]	.008	“Reject the null hypothesis”.
8	Are your flagships now manned at a sufficient degree to meet security requirements? occur with equal odds.	“One-Sample Chi-Square Test”	15.114[a]	.000	“Reject the null hypothesis”.
9	Current trends indicate that certain flag state administrations issue safe manning certifications	“One-Sample Chi-Square Test”	17.857[a]	.000	“Reject the null hypothesis”.

	without paying enough attention to security standards, onboard administrative tasks, and vessel trading. happen with equal odds, taking into account the current global security situation.				
10	To what extent do you believe the Ship Security Alarm System (SSAS) contributes to maritime security? happen with equal odds.	"One-Sample Chi-Square Test"	6.429[a]	.011	"Reject the null hypothesis".
11	Have you had to handle a security incident at work? happen with equal odds.	"One-Sample Chi-Square Test"	8.257[a]	.004	"Reject the null hypothesis".
12	Regarding the aforementioned occurrence or incidents, how would you rank the response of the "Maritime Administration" and "maritime law enforcement agencies"? happen with equal odds.	"One-Sample Chi-Square Test"	8.257[a]	.004	"Reject the null hypothesis".
13	Does the Automatic Identification System (AIS) promote or hinder security? happen with equal odds.	"One-Sample Chi-Square Test"	6.429[a]	.011	"Reject the null hypothesis".

14	Do the Vessel Traffic System (VTS) contribute to or detract from security? occur with equal odds.	“One-Sample Chi-Square Test”	3.457[a]	.063	Retain the null hypothesis.
15	Is VTS an active security threat mitigation strategy or a deterrent? happen with equal odds.	“One-Sample Chi-Square Test”	2.314[a]	.128	Retain the null hypothesis.
16	Will requiring reporting to the Vessel Traffic System (VTS) improve local security as a whole? happen with equal odds.	“One-Sample Chi-Square Test”	17.857[a]	.000	“Reject the null hypothesis”.
17	Will the operator's efficiency in identifying and preventing security incidents be improved by radar-AIS interface? happen with equal odds.	“One-Sample Chi-Square Test”	6.429[a]	.011	“Reject the null hypothesis”.
18	Will the goal of safe transportation be aided or hindered by long-range identification and tracking of ships (LRIT)? happen with equal odds.	“One-Sample Chi-Square Test”	6.429[a]	.011	“Reject the null hypothesis”.
19	Do you have any prior experience inspecting containers	“One-Sample Chi-Square Test”	3.457[a]	.063	Retain the null hypothesis.

	for security? happen with equal odds.				
20	What do you think would be the greatest way to improve maritime security, taking into account the security risk and ship owners' commercial commitment? happen with equal odds.	"One-Sample Chi-Square Test"	.714[a]	.398	Retain the null hypothesis.
21	Numerous ship reporting systems exist around the world, including the Indian (Maritime) Search and Rescue Computerised Ship Reporting System (INDSAR), the Japanese Ship Reporting System (JASREP), and the Automated Mutual-Assistance Vessel Rescue System (AMVER). occur in your o with equal chances.	"One-Sample Chi-Square Test"	17.857[a]	.000	"Reject the null hypothesis".
22	Would you rather have law enforcement keep an eye on your ship's whereabouts in the current security scenario?	"One-Sample Chi-Square Test"	15.114[a]	.000	"Reject the null hypothesis".

	happen with equal odds.				
23	Do you think all ships on international journeys should be required to report to one of the global ship reporting systems? happen with equal odds.	"One-Sample Chi-Square Test"	17.857[a]	.000	"Reject the null hypothesis".
24	In terms of training, does the Vessel Data Recorder (VDR) improve maritime security? happen with equal odds.	"One-Sample Chi-Square Test"	12.600[a]	.000	"Reject the null hypothesis".
25	Is there any analytical benefit to maritime security from the Vessel Data Recorder (VDR)? occur with equal odds.	"One-Sample Chi-Square Test"	10.314[a]	.001	"Reject the null hypothesis".

Asymptotic significances are displayed. The significance level is .050.

The results for the question, "Do you feel, in the present-day scenario, there is a need to enhance maritime security?" show a significant trend among responses. We were able to reject the null hypothesis of equal probability using a one-sample chi-square test with a p-value of.000 and a chi-square value of 24.029. This indicates that respondents from shipping companies do not view this need equally; rather, there is a strong consensus on the necessity of enhancing maritime security in today's environment.

For the question, "In your opinion, which crime poses the greatest threat to the maritime sector?" Regarding particular dangers, the one-sample chi-square test results show no discernible variation in responses. We maintain the null hypothesis in light of

the chi-square value of 9.057 and the p-value of.107, which indicate that respondents believe that different marine crimes pose an equivalent threat to the industry. This result reflects an absence of a clear consensus among participants on which specific crime is seen as the most significant threat.

For the question, "In your opinion, are the instruments adopted by IMO adequate to combat the above maritime crimes?" the one-sample chi-square test reveals a significant difference in responses. With a chi-square value of 15.114 and a p-value of .000, we reject the null hypothesis of equal probabilities, indicating that respondents do not equally view the adequacy of IMO's instruments. This suggests a strong perception among participants that the measures currently adopted by the IMO may not be sufficient to effectively address maritime crimes.

For the question, "Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ports)" the one-sample chi-square test reveals a significant disparity in responses. Because the chi-square value is 15.114 and the p-value is.000, we reject the null hypothesis that the probabilities are equal. This result suggests that respondents' views on the value of IMO-mandated technology in enhancing port security are not all in accord, suggesting that respondents have differing concerns or viewpoints regarding the ways in which these technologies impact maritime security in port areas.

For the question, "Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Ships)" the one-sample chi-square test shows significant variation in responses. The null hypothesis that the probabilities are equal is rejected with a chi-square value of 15.114 and a p-value of.000. This suggests that respondents do not equally view the effectiveness of IMO-mandated technologies in enhancing security on ships, indicating

diverse opinions or potential concerns about the adequacy of these technologies for improving ship-based maritime security.

For the question, "Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? (Other Installations)" the one-sample chi-square test results indicate significant differences in responses. With a p-value of.000 and a chi-square value of 15.114, we reject the null hypothesis that the probabilities are equal. This finding suggests that respondents have varied views on the effectiveness of IMO-mandated technologies in enhancing security across other maritime installations, reflecting a potential lack of consensus on whether these technologies adequately support security in these areas.

For the question, "How does your organization motivate its staff to comply with security guidelines?" the one-sample chi-square test shows a significant difference in responses. Because the chi-square value is 9.657 and the p-value is.008, we reject the null hypothesis that the probabilities are equal. This finding implies that companies use a variety of strategies to encourage employees to follow security policies, showing that no one strategy is more effective than another.

For the question, "Are the present manning levels onboard your flagships adequate to comply with security regulations?" the one-sample chi-square test shows a significant variation in responses. With a chi-square value of 15.114 and a p-value of .000, we reject the null hypothesis of equal probabilities. This indicates that respondents do not uniformly agree on the adequacy of current manning levels to meet security regulations, suggesting concerns or differing views regarding staffing sufficiency for compliance.

For the statement, "Present trend shows that certain flag state administration issue safe manning certificates without giving due attention to vessels trading, administrative

work onboard, and security requirements, keeping in mind the present security scenario in the world," the one-sample chi-square test reveals a significant difference in responses. With a chi-square value of 17.857 and a p-value of .000, we reject the null hypothesis of equal probabilities. This result indicates that respondents widely agree that certain flag state administrations may overlook critical operational and security factors when issuing safe manning certificates, highlighting concerns about the adequacy of manning standards under current global security conditions.

For the question, "How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security?" the one-sample chi-square test shows a significant difference in responses. Because the chi-square value is 6.429 and the p-value is.011, we reject the null hypothesis that the probabilities are equal. This suggests that different respondents had different opinions on how beneficial SSAS is for enhancing maritime security, exposing a range of opinions regarding the system's value and impact on enhancing ship security.

For the question, "Have you dealt with a security incident in your place of work?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.004 and a chi-square value of 8.257, we reject the null hypothesis that the probabilities are equal. This indicates that the respondents' experiences with security incidents in the workplace are not uniformly distributed, suggesting that a significant proportion have encountered such incidents, highlighting the relevance of security challenges in their work environments.

For the question, "How would you rate the response of “Maritime Administration” / “maritime law enforcement agencies” in the above incident(s)?" the one-sample chi-square test shows a significant difference in responses. The null hypothesis that the probabilities are equal is rejected with a chi-square value of 8.257 and

a p-value of.004. This suggests that respondents have differing perspectives about how well the “Maritime Administration” and law enforcement agencies handled security events, indicating that their viewpoints are not all the same.

For the question, "Is Automatic Identification System (AIS) fostering security or is it a hindrance?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.011 and a chi-square value of 6.429, we reject the null hypothesis that the probabilities are equal. This suggests varying ideas on whether AIS is advantageous for security or potentially detrimental, indicating that respondents' thoughts on the role of AIS in maritime security are not all the same.

For the question, "Is Vessel Traffic System (VTS) fostering security or is it a hindrance?" the one-sample chi-square test shows no significant difference in responses. We reject the null hypothesis that the probabilities are equal, as indicated by the chi-square value of 6.429 and the p-value of.011. This suggests that respondents had varying ideas about whether AIS is helpful for security or could be troublesome, indicating that their thoughts on the role of AIS in maritime security are not all the same.

For the question, "Is VTS a deterrent or an active measure for mitigating security threat?" the one-sample chi-square test shows no significant difference in responses. The null hypothesis of equal probabilities is upheld at a p-value of.128 and a chi-square value of 2.314. This implies that respondents have a balanced opinion of VTS's significance in reducing security concerns, viewing it as neither primarily an active measure nor as a significant deterrent.

For the question, "Will mandatory reporting to Vessel Traffic System (VTS) enhance overall security in the area?" the one-sample chi-square test shows a significant difference in responses. With a chi-square value of 17.857 and a p-value of .000, we reject the null hypothesis of equal probabilities. This indicates that respondents do not

view the impact of mandatory reporting to VTS as equally beneficial, suggesting a strong consensus that such reporting would indeed enhance overall security in the area.

For the question, " Will interfacing of radar with AIS enhance the operator efficiency in early identification and prevention security incident from occurring?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.011 and a chi-square value of 6.429, we reject the null hypothesis that the probabilities are equal. This shows a significant conviction in the efficacy of this integration for improving maritime security, as respondents largely concur that integrating radar with AIS will increase operator efficiency in detecting and averting security situations.

For the question, "Will long-range identification and tracking of ships (LRIT) foster the objective of secure shipping or will it be a hindrance?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.011 and a chi-square value of 6.429, we reject the null hypothesis that the probabilities are equal. This implies that respondents do not see LRIT to be a barrier or to promote safe shipping. indicating a strong belief that LRIT generally supports secure shipping but with some varied opinions on its effectiveness.

For the question, "Do you have any experience in security scanning of containers?" the one-sample chi-square test shows no significant difference in responses. Given the p-value of.063 and the chi-square value of 3.457, we maintain the null hypothesis of equal probability. This shows that there is no clear agreement or prevailing experience among participants, suggesting that respondents' experiences with security scanning of containers are evenly dispersed.

For the question, "Taking into consideration the security risk and commercial commitment of ship owners, what in your opinion would be the best solution for enhancing maritime security?" the one-sample chi-square test shows no significant

difference in responses. With a p-value of.398 and a chi-square value of.714, we maintain the null hypothesis that the probabilities are equal. This suggests a wide range of viewpoints on the most effective techniques taking into account both security issues and commercial factors, indicating that respondents do not have a common opinion on the best way to improve maritime security.

For the question, "There are different ship reporting systems worldwide, such as Automated Mutual-Assistance Vessel Rescue system (AMVER), Japanese Ship Reporting System (JASREP), Indian (Maritime) Search and Rescue Computerized Ship Reporting System (INDSAR) etc. In your opinion, do these systems foster maritime security?" the one-sample chi-square test shows a significant difference in responses. The null hypothesis that the probabilities are equal is rejected with a chi-square value of 17.857 and a p-value of.000. Although some respondents may have different views, this suggests that there is broad agreement that these ship reporting systems are effective in increasing maritime security. It also shows that respondents do not regard these systems as equally nurturing marine security.

For the question, "In the present security scenario, will you prefer that your ship's position be monitored by law enforcement agencies?" the one-sample chi-square test shows a significant difference in responses. With a chi-square value of 15.114 and a p-value of .000, we reject the null hypothesis of equal probabilities. This indicates that respondents do not have uniform views on whether their ship's position should be monitored by law enforcement agencies, suggesting a strong consensus in favor of monitoring, although some may still have concerns or differing opinions on the matter.

For the question, "In your opinion, should reporting to any one of the worldwide ship reporting systems be made mandatory for all ships on international voyages?" A significant difference in replies is revealed by the one-sample chi-square test. With a p-

value of.000 and a chi-square value of 17.857, we reject the null hypothesis that the probabilities are equal. This suggests that respondents' opinions on whether or not all ships on international voyages should be required to report to global ship reporting systems are not all the same. The result suggests a strong consensus in favor of making reporting mandatory, though some respondents may have differing opinions on the requirement.

For the question, "Does the Vessel Data Recorder (VDR) add value to maritime security with regard to training?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.000 and a chi-square value of 12.600, we reject the null hypothesis that the probabilities are equal. This suggests a strong consensus that the VDR is helpful for training, even though individual respondents may have different ideas on its effectiveness. It also shows that respondents do not share a common opinion on whether the VDR offers value to maritime security in terms of training.

For the question, "Does the Vessel Data Recorder (VDR) add value to maritime security with regard to analysis?" the one-sample chi-square test shows a significant difference in responses. With a p-value of.001 and a chi-square value of 10.314, we reject the null hypothesis that the probabilities are equal. This implies that respondents' thoughts on whether the VDR contributes to maritime security in terms of analysis are not all the same, showing that there is broad agreement that the VDR is useful for analysis, even though individual respondents may have different ideas.

CHAPTER V:

DISCUSSION

5.1 Discussion of Findings

The findings of this research illustrate that nature of security management, as well as practices, technologies, and regulations, are varied and tense within the maritime industry. The results show a common understanding of the necessity of the improvement of maritime security with more concrete concerns about certain risks such as piracy, terrorism, and cybercrime. Nevertheless, the answers speak about the same implementing International Maritime Organization (IMO) instruments means that while these standards are implemented, they may not meet modern maritime security needs.

Significant variability in responses was noted across regions regarding data-sharing practices and the accessibility of ship databases. Those with weak or near-non-existent systems for the exchange of important maritime data, especially in near real-time, have significant security issues. The respondents' satisfaction regarding technologies required by IMO was also somewhat varied; there were concerns where the respondent felt that the technologies were useful, but perhaps not as beneficial as expected in some other respects, for application on ports, vessels and installations or otherwise, these results imply that the effectiveness of technology may reduce with the extent of development in the ports, vessels and installations. Selective responses were received about the efficiency of tools like "Ship Security Alarm System" (SSAS), "Automatic Identification System" (AIS), and "Vessel Traffic System" (VTS). These divergent views show that even though such tools help contribute to safety, they can be ineffective in solving all security situations or are likely to experience operational constraints in some parts of the world. Also the divided reaction to mandatory reporting

to Vessel Traffic Systems and international reporting standards point to the difficulty in achieving the goal of providing operational excellence while maintaining security.

One of the key lessons learnt is identification of VDR as a solution, which may be utilised for security training and evaluation, underlining that data is an essential instrument in security risk mitigation as well as a tool used in training for crisis response.

In a nutshell, this work highlights the importance of a context-intelligent approach to maritime security with references to capabilities in the region, existing technological infrastructure, threat perception, etc., rather than a blueprint approach. On the same note, the approach will enhance a reactive and sustainable maritime security structure.

Discussion of Findings from the" Maritime Administration" Survey

The results of the survey conducted among the "Maritime Administration"s indicate the improvements and issues regarding maritime security and cooperation with the police. Survey participants from "Maritime Administration" overwhelmingly called for increased security, with diminished effectiveness of the IMO instruments appropriate to counter modern threats. This aligns with a study conducted by Karim (2022) which emphasizes the exponential growth of cybersecurity threats in the maritime industry. Due to the proliferation of cyberattacks, the security of offshore installations, ports, and ships is more and more at risk. Cyberattacks on the marine industry have recently increased in frequency and severity, coinciding with the sector's growing reliance on digital technologies amid the backdrop of the worldwide pandemic. Gaining a deeper comprehension of the IMO regulations about maritime cybersecurity was a consequence of this study. While "International marine Organization" (IMO) did pass certain cybersecurity-related laws and policies, the existing international legal framework is insufficient to address cybersecurity risks in the marine industry. The concern over the adequacy of IMO standards suggests that administrations feel existing frameworks may

lack the agility needed to adapt to rapidly evolving threats. A critical finding is the variability in data-sharing mechanisms between “Flag Administration”s and law enforcement agencies. Although some countries implement real-time, requirement-based data sharing, others lack such systems, which poses significant gaps in maritime security (UNODC, 2024).

Discussion of Findings from the Global Insights of Foreign Navies Survey

The survey results from the study of foreign navies also served to capture the ideas and perceptions set forth from the global maritime security perspective, as well as to reveal both commonalities and differences in foreign perception of security threats among various actors in the maritime domain. Several respondents believe that security should be increased involving threats such as piracy, smuggling, and cyber threats, which are considerate and ever-dynamic. A study conducted by Islam (2024) additionally brought out the fact that certain dangers associated with technological abuse, such invasions of privacy, unequal application of force, and the diminishment of human discretion and responsibility, are highlighted. Responsible and ethical use of technology in maritime security requires strong regulatory structures and international cooperation, and it is crucial to take a balanced approach that weighs the pros and downsides of technological progress. An interesting discovery is the kind of interaction that different foreign navies have with the countries’ “maritime law enforcement agencies”. While some administrations noted frequent interaction, some suggested that it was only occasional, implying inadequate coordinated maritime operations. These variations in frequency and mechanisms regarding the type of information exchanged between the “Flag Administration”s and the police also corroborate previous research which has also pointed out the need for common guidelines to facilitate efficient data sharing in emergency situations.

Discussion of Findings from the Shipping Companies Survey

The survey of the ship operators shows that, overall, they are highly supportive of measures to improve maritime security, and many of them identified shortcomings in the present IMO instruments and technology relevant to the security of ports, ships and other maritime facilities. A huge percentage of shipping firms responded that the current technologies are useful but enough to meet modern-day threats, including cyber threats, piracy and illegal business. The study also revealed that the shortage of seafarers is emerging as a growing complaint by shipping companies in relation to the proper security staffing on board vessels. Many respondents perceive manning levels as insufficient, a view echoed by scholars like Thai and Grewal, (2007); Delmas and Salsac, (2022); Jankowski *et al.,* (2022) argue that staffing issues can limit the effective implementation of security protocols. Furthermore, there is strong support for the role of Ship Security Alarm Systems (SSAS) and Vessel Data Recorders (VDR) in promoting security, but concerns remain about the consistent effectiveness of these systems in real-world incidents. Another key insight is the support for a mandatory recommendation based on the assessment of the level of support for the mandatory reporting procedure to vessel tracking systems including the Vessel Traffic System (VTS), which might have a positive impact on security monitoring and response.

5.2 Discussion of Research Question One

a) Administrative officers that will include officials responsible for overall administration and legal aspects.

Research Question One of this study explores the perspectives of administrative officers and highlights critical insights into the challenges and perceptions of those responsible for the management and legal aspects of maritime security. The study shows

that the administrative officers partly understand need for raising the security measures in maritime industry, referring to the existing deficiencies in the policy implementation as well as the current limitation of the technologies utilized in this sphere. Several respondents were not satisfied with the current International IMO guidelines for recommendations some of the findings are as follows: A study Safitra, Lubis and Fakhrurroja (2023) offers a thorough framework to influence cyber security in the years to come. In light of the complexity of today's cyber threats, this framework guides organizations to strengthen their defenses. The combination of resilience with capabilities is the main focus. Cyber security strategies that incorporate aspects can help organizations better prepare for, react to, and recover from cyber disasters.

Among the administrative officers, the legal systems are cited as supportive measures as well as constraints to efficient maritime security. A substantial number of interviewed experts agree that IMO norms are the foundation for security operations, but, at the same time, most of the respondents insist on the necessity to develop more detailed regional adaptations of these frameworks because the existing sets of rules are insufficient to protect ships and their crews from all types of threats In this sense, the (Ajagunna *et al.*, 2020; Renganayagalu, Mallam and Hernes, 2022) who pointed to the possibility to enhance the protection by regionally focused amendments to maritime law This view alleges that maritime security could be enhanced by harmonisation of international, regional and national frameworks. Administrative officers also expressed concerns about the communication and coordination between administrative bodies and law enforcement agencies, indicating a gap in collaborative efforts. Some administrative officers advocate for a streamlined data-sharing system between “Flag Administration”s and maritime law enforcement, a sentiment that underscores an industry-wide call for enhanced data transparency.

5.3 Discussion of Research Question Two

a) Officers responsible for enforcing National Maritime legislation in their respective Maritime zones like - coast guard, Navy, Maritime security agency, Marine police etc.

The second research question of this study revolves around the views of officers charged with the implementation of national maritime legislation, which includes Coast Guard, maritime security offices, navy, and marine police, on existing tools and frameworks for maritime security. These enforcement officers are important in overseeing, deterring, and handling maritime offenses in their regions of operation. The study establishes that a majority of these officers consider the present measures of maritime security, which are technological and legislative, as insufficient to meet the challenging and changing nature of security threats.

The first key finding emerging from this research work is that there is a need to develop better surveillance and monitoring techniques. From the responses of officers, it emerged that there's no real-time database integration of the current technologies supporting the VTS and SSAS. This complements the findings made by Hasan *et al.* (2021), that gaps in real-time information also limit operational readiness in response to enforcement agencies in high-risk zones. In addition, enforcement officers describe a requirement for enhanced information integration, since fast cooperation between agencies is crucial to respond to security threats promptly. Additionally, they discovered that cyber security preparation has a favorable effect on the security performance of organizations. (Simola and Pöyhönen, 2022).

The other major finding established is the cooperation between the teams. Police officers interviewed commented that while there may be a convergence of interests in

viewing maritime security, translation of this into effective communication between the various parties proved to be slow and disjointed. Additionally, officers raised concerns about resource limitations, particularly in terms of personnel and equipment, which they believe compromise the effectiveness of their operations.

5.4 Discussion of Research Question Three

a) Cast and crew present at the ship that includes ship masters, shipping organizations and companies, shipping associations, etc.

Research Question Three focuses on the opinions of shipboard personnel, including shipmasters, shipping companies, and shipping associations, pertaining to maritime security measures and the adequacy of existing rules and systems. Because these are the stakeholders who are on the frontline being affected by maritime security threats, they are useful in surmising the field's strengths and weaknesses as well as issues that require fixing.

A major observation arising from this study is how current security measures are considered beneficial, albeit not fully responsive to the demands of the shipboard environment. Some of the respondents offered social concerns that were focused on the AIS as well as the VTS, which they think are not very useful on certain occasions. This concurs with observations made by Bueger (2015); Mwango Charo (2021), who observed that mandatory security procedures usually entail generic security requirements without understanding local conditions on specific boats.

Other issues of concern are, of course, manning levels, which shipmasters and crews are deemed to meet security demands. They claim that reduced personnel on board present an inability to address security threats effectively, a concern observed by Akamangwa (2016), who established that the shortage of crews is a normal thing in commercial vessels and affects both the safety and security of the vessel. This was a

challenge pointed out by the respondents; they recommended that the firm increase its crew levels or conduct more training on onboard security to counter this challenge and improve its security management capacity. Another study by Hannaford and Van Hassel (2021) found that there is no correlation between the number of crew members and the reduction of onboard chores or weariness, and that growing shipboard automation and decreasing crew numbers may have detrimental consequences for the Licensed Deck Officer, such as greater complacency, decreased situational awareness, and over-reliance on sensors. The primary concern of maritime authorities should be the implementation of new regulations on navigation, crewing levels, and liability. Mariners will adjust to this unavoidable technology, even if the shipping business is notoriously resistant to change.

Also, there is a demand for more open and weaker security approaches. Some of the shipboard personnel commented that standard operating procedures, though necessary, can be a constraint to the smooth running of the operation. Finally, shipping companies and associations voiced concerns about the financial and operational costs of compliance, which they feel can strain their resources without necessarily yielding proportional security benefits.

CHAPTER VI:

SUMMARY, IMPLICATIONS, AND RECOMMENDATIONS

6.1 Summary

This study investigates the perceptions, challenges, and needs across various segments of the maritime industry regarding current maritime security practices, technologies, and regulations. Findings indicate a widespread understanding of the need to enhance maritime security, with participants highlighting specific concerns about growing threats such as piracy, terrorism, and cybercrime. A central theme emerging from the data is that while the International Maritime Organization (IMO) provides foundational standards for maritime security, these may not be adequately responsive to evolving security risks.

"Maritime Administration" respondents mainly called for enhanced security measures, spearheaded in the area of cyber security for ports, ships, and facilities. Some participants' view was that the currently guiding IMO guidelines are rigid and do not offer enough flexibility in responding to current threat in light of the growing digital risks. Also, there was a higher differentiation of attitudes and techniques for sharing the data depending on the availability of real-time data-sharing potential in different countries.

In this study, the various operational models of foreign navies imply different regional security organizations. When it comes to risk factors mentioned by the respondents, piracy, smuggling and cyber threats are among the most frequently cited factors; however, the degrees of concern, engagement with local offices of marshal's affairs and collaboration with local police departments do not seem to be cohesive. Some navies disclosed they regularly engaged in data sharing and cooperative operations with police or Coast Guard forces, while others said such cooperation was rare at most,

suggesting the need for internationally developed guidelines. Such disparity corresponds with earlier research discussing the need for consolidation of common security measures within the maritime domain.

Shipping companies support stricter security measures but express dissatisfaction with the efficacy of certain IMO-mandated technologies. While systems like the Ship Security Alarm System (SSAS) and Vessel Data Recorders (VDR) are beneficial, there are doubts about their reliability in real-world applications. Besides, the shortage of people remains an issue where businesses are certain that staff shortages threaten to undermine effective security measures. This study supports other studies recommending a larger number of staff and staff training in order to provide for security requirements.

In sum, the present research highlights the necessity to adopt a context-based approach to understanding the level of maritime security, that take into account the capacities of the regions, the development of technology and threat potential. Thus, it identifies considerable advantages in emphasising the need for adaptive, collaborative approaches to tackle systematically maritime security threats. These conclusions point to a desire for new regional-specific guidelines as well as enhanced cooperation systems for a stronger and better sustained worldwide maritime security.

6.2 Implications

From this study the following major implications arise for maritime policy, security measures and the use of technology. First of all, the outcomes portray that current IMO frame works and technologies as may be prototype can be inadequate to address current risks as cybercrimes, piracy, smuggling among others. This means that blue stakeholders involved in maritiime policymaking should start considering their efforts at envisioning new IMO requirements fit for purpose for fending of new age

security threats. It should be more about preparedness for new types of threats and new technologies more about updates.

Secondly, the work showed a number of crucial issues connected to the specifics of data-sharing and cooperation between “Maritime Administration”s, police agencies, and naval authorities. This implies to leaders of industries as well as regional players a need to develop a highly-coordinated system of rules of passing data while operating outside national frameworks. These protocols should focus as much as possible on the exchange of information in real, to improve response time and readiness levels of security. Policymakers and security agencies might explore creating a global maritime security data network, which could facilitate rapid information flow and coordinated response to threats.

Last, the conclusions stress the necessity of proper staffing, training, and equipment in pursuit of proper maritime security. The respondents in the shipping industry regard the small number of crew and resources as the major impediment to the implementation of efficient security management systems. This means that a large investment has to be made on the human part as a supplement to the technological aspect. In particular, more attention and funding should be paid to security training programs on the crew members’ side, and more permanent staff recruiting would add to the sector’s security protection against all security hazards. All these implications suggest further policy updates, the establishment of cooperation frameworks and increasing personnel support for a systematic and adaptive maritime security environment.

6.3 Recommendations for Future Research

Future research should delve deeper into regional differences in maritime security practices to uncover specific challenges and best practices in diverse geopolitical contexts. In the first instance, comparing regions with high-risk maritime environments,

such as piracy-prone areas, and those with low-risk maritime environments might facilitate an understanding of specifics of threats that develop in the given environment, hence influencing the security measures and technologies. This conclusion means that such research could help in designing more sensitive frameworks in IMO that would effectively correspond to the needs of certain regions.

Secondly, more research would be useful on how these new technologies, like AI and blockchain, will compound the existing maritime security challenges. Researching how these technologies can augment the insertion of real-time data processes and the decision-making process would be beneficial in bringing about changes to current security practices. Specifically, the investigation of AI-based predictive information gathering for threat identification may be useful in preventing risks and incidents.

Last, the research gaps include the lack of literature that analyses the impact of cybersecurity integration on maritime operations over the long run, as there is likely to be a rise in technological advancement of threats. Whether positive or negative, such changes in cost would be essential to decipher the practicality and viability of cybersecurity policies for diverse maritime actors. Thus, the studies that provide empirical evidence for more flexible, technological, and teamwork-based models would open a new era for growth in the field.

6.4 Conclusion

This study provides an in-depth analysis of maritime security practices, highlighting key areas where current approaches and technologies may fall short. The study establishes that although the IMO guidelines act as fundamental structures, they may not suffice the complex and dynamic security of the global maritime market. Lack of coordination in data sharing amongst the regions, variation in the level of cyber

readiness, and the differing levels of technology adoption also show there is a need for specific regional solutions that address the regional threats and operating environments.

The study also highlights the fact that all the stakeholders, such as the administrative officers, law enforcement agencies and shipping companies, appreciate the need to enhance security, but they are faced with challenges in managing the security system as well as in coordinating them and their efficiency with the technologies available to them. While technologies like the SSAS, AIS, and VTS are well supported, problems in practical use assert that ready-appropriate tools are not universal or effective enough.

In conclusion, this research underscores the importance of a context-aware approach to maritime security, advocating for adaptive, regionally informed strategies that address both current and emerging threats. By embracing a more collaborative and technology-integrated framework, maritime stakeholders can enhance security resilience and better safeguard global trade routes.

REFERENCES

Abbas, S. *et al.* (2022) ‘“‘Review of smart grid and nascent energy policies: Pakistan as a case study,’”’.

Ahn, S. Il and Kurt, R.E. (2020) ‘Application of a CREAM based framework to assess human reliability in emergency response to engine room fires on ships’, *Ocean Engineering*, 216, p. 108078. Available at: https://doi.org/10.1016/j.oceaneng.2020.108078.

Ajagunna, I. *et al.* (2020) ‘Reflections on the theme issue outcomes the fourth industrial revolution: What are the realities for maritime and tourism dependent countries?’, *Worldwide Hospitality and Tourism Themes* [Preprint]. Available at: https://doi.org/10.1108/WHATT-02-2020-089.

Akamangwa, N. (2016) ‘Working for the environment and against safety: How compliance affects health and safety on board ships’, *Safety Science*, 87, pp. 131–143. Available at: https://doi.org/10.1016/j.ssci.2016.03.027.

Akpan, F. *et al.* (2022) ‘Cybersecurity Challenges in the Maritime Sector’, *Network* [Preprint]. Available at: https://doi.org/10.3390/network2010009.

Ali, I. and Sidhu, J.S. (2023) ‘Strategic Dynamics of the Arms Race in South Asia’, *Journal of Asian and African Studies* [Preprint]. Available at: https://doi.org/10.1177/00219096231153150.

Ali, Z. *et al.* (2021) ‘“‘Fault management in DC microgrids: A review of challenges, countermeasures, and future research trends,’”’.

Ali, Z. *et al.* (2022) ‘“‘Fault detection and classification in hybrid shipboard microgrids,’”’.

Ali, Z. *et al.* (2023) ‘“‘A study of a generalized photovoltaic system with MPPT using perturb and observer algorithms under varying conditions,’”’.

Alqurashi, F.S. *et al.* (2023) ‘Maritime Communications: A Survey on Enabling Technologies, Opportunities, and Challenges’, *IEEE Internet of Things Journal*, 10(4), pp. 3525–3547. Available at: https://doi.org/10.1109/JIOT.2022.3219674.

Alsawalqa, R.O. and Venter, D. (2022) ‘Piracy and Maritime Security in the North-Western Indian Ocean: From the Gulf of Oman to the Waters off the Somali Coast’, *Insight on Africa* [Preprint]. Available at: https://doi.org/10.1177/09750878211049224.

Androjna, A. *et al.* (2020) ‘“‘Assessing cyber challenges of maritime navigation,””’.

Baig, M.Z., Lagdami, K. and Mejia Jr., M.Q. (2024) ‘Enhancing maritime safety: A comprehensive review of challenges and opportunities in the domestic ferry sector’, *Maritime Technology and Research*, 6(3), p. 268911. Available at: https://doi.org/10.33175/mtr.2024.268911.

Baird, A.J. (2000) ‘The Japan coastal ferry system’, *Maritime Policy & Management*, 27(1), pp. 3–16. Available at: https://doi.org/10.1080/030888300286644.

Baird, A.J. (2012) ‘Comparing the efficiency of public and private ferry services on the Pentland Firth between mainland Scotland and the Orkney Islands’, *Research in Transportation Business & Management*, 4, pp. 79–89. Available at: https://doi.org/10.1016/j.rtbm.2012.06.001.

Balakrishnan Nair, T.M. *et al.* (2023) ‘Advances in Ocean State Forecasting and Marine Fishery Advisory Services for the Indian Ocean Region’, in *Social and Economic Impact of Earth Sciences*. Singapore: Springer Nature Singapore, pp. 201–227. Available at: https://doi.org/10.1007/978-981-19-6929-4_11.

Baygi, F. *et al.* (2017) ‘Factors affecting health-promoting lifestyle profile in Iranian male seafarers working on tankers’, *International Maritime Health*, 68(1), pp. 1–6. Available at: https://doi.org/10.5603/IMH.2017.0001.

Beckman, R. and Page, M. (2014) 'Piracy and Armed Robbery Against Ships', in *The Handbook of Security*. London: Palgrave Macmillan UK, pp. 234–255. Available at: https://doi.org/10.1007/978-1-349-67284-4_11.

Bibby, L. and Dehe, B. (2018) 'Defining and assessing industry 4.0 maturity levels – case of the defence sector', *Production Planning & Control*, 29(12), pp. 1030–1043. Available at: https://doi.org/10.1080/09537287.2018.1503355.

BIMCO *et al.* (2011) 'Best management practices for Protection against Somalia Based Piracy'.

Borg, S., Attard, F.G. and Mallia Vella De Fremeaux, P. (2023) *Research Handbook on Ocean Governance Law, Research Handbook on Ocean Governance Law*. Edited by S. Borg, F.G. Attard, and P.M. Vella de Fremeaux. Edward Elgar Publishing. Available at: https://doi.org/10.4337/9781839107696.

Bothur, D., Zheng, G. and Valli, and C. (2017) '"'A critical analysis of security vulnerabilities and countermeasures in a smart ship system,'"'.

Bothur, Dennis, Zheng, G. and Valli, C. (2017) 'A critical analysis of security vulnerabilities and countermeasures in a smart ship system', in *Proceedings of the 15th Australian Information Security Management Conference, AISM 2017*.

Boutilier, J. (2005) 'The best of times, the worst of times: The global maritime outlook 2004', *Best of Times, the Worst of Times*, pp. 15–16.

Bradbury-Jones, C. *et al.* (2022) 'Scoping reviews: the PAGER framework for improving the quality of reporting', *International Journal of Social Research Methodology*, 25(4), pp. 457–470. Available at: https://doi.org/10.1080/13645579.2021.1899596.

Bronk, R. and Dewitte, P. (2020) 'Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor', in *Proceedings of the Annual Hawaii*

International Conference on System Sciences. Available at: https://doi.org/10.24251/HICSS.2020.240.

Brouer, B.D., Karsten, C.V. and Pisinger, D. (2016) 'Big Data Optimization in Maritime Logistics', *Studies in Big Data* [Preprint]. Available at: https://doi.org/10.1007/978-3-319-30265-2_14.

Brouer, B.D., Karsten, C.V. and Pisinger, D. (2017) 'Optimization in liner shipping', *4OR* [Preprint]. Available at: https://doi.org/10.1007/s10288-017-0342-6.

Bruzzone, A. (2012) *Guidelines for Ferry Transportation Services*. Washington, D.C.: National Academies Press. Available at: https://doi.org/10.17226/14644.

Bueger, C. (2015) 'What is maritime security?', *Marine Policy* [Preprint]. Available at: https://doi.org/10.1016/j.marpol.2014.12.005.

Bueger, C., Edmunds, T. and McCabe, R. (2020) 'Into the sea: capacity-building innovations and the maritime security challenge', *Third World Quarterly*, 41(2), pp. 228–246. Available at: https://doi.org/10.1080/01436597.2019.1660632.

Cantarelli, C.C. *et al.* (2018) 'Cost Overruns in Large-Scale Transport Infrastructure Projects', *Automation in Construction* [Preprint].

ÇETİN, O. and KÖSEOĞLU, M. (2020) 'A Study on the Classification of Maritime Security Threat Topics', *International Journal of Environment and Geoinformatics*, 7(3), pp. 365–371. Available at: https://doi.org/10.30897/ijegeo.742336.

Chamberlain, G. (2008) 'Pirate attacks around the world rise by 20pc'.

Chapsos, I. and Malcolm, J.A. (2017) 'Maritime security in Indonesia: Towards a comprehensive agenda?', *Marine Policy* [Preprint]. Available at: https://doi.org/10.1016/j.marpol.2016.11.033.

Cheemakurthy, H. and Garme, K. (2022) 'Fuzzy AHP-Based Design Performance Index

for Evaluation of Ferries', *Sustainability*, 14(6), p. 3680. Available at: https://doi.org/10.3390/su14063680.

Chowdhury, M.N. *et al.* (2024) 'Navigating Human Factors in Maritime Safety: A Review of Risks and Improvements in Engine Rooms of Ocean-Going Vessels', *International Journal of Safety and Security Engineering*, 14(1), pp. 1–14. Available at: https://doi.org/10.18280/ijsse.140101.

d'Amore, M., Baggio, R. and Valdani, E. (2015) 'A Practical Approach to Big Data in Tourism: A Low Cost Raspberry Pi Cluster', in *Information and Communication Technologies in Tourism 2015*. Cham: Springer International Publishing, pp. 169–181. Available at: https://doi.org/10.1007/978-3-319-14343-9_13.

Daniel Brown, J. *et al.* (2023) 'Anchoring Global Security: Autonomous Shipping with Mind Reading AI, GPT-core and MAMBA-core Agents, RAG-Fusion, AI Communities, Hive-AI, and the Human Psyche', (April 2024). Available at: https://doi.org/10.13140/RG.2.2.34188.90247.

Defence, M. of (2020) 'Defence equipment and Support'.

Delmas, M.C. and Salsac, K. (2022) 'Galileo Advanced Features for the Marine Domain: Breakthrough Applications for Safety and Security', in *35th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS+ 2022*. Available at: https://doi.org/10.33012/2022.18490.

DeSimone, R. (2008) 'Globalization Keeps Future Bright for Shipping', *Maritime Reporter \& Engineering News*, 16.

Etikan, I. (2016) 'Comparison of Convenience Sampling and Purposive Sampling', *American Journal of Theoretical and Applied Statistics* [Preprint]. Available at: https://doi.org/10.11648/j.ajtas.20160501.11.

Farah, M.A. Ben *et al.* (2022) '''Cyber security in the maritime industry: A systematic

survey of recent advances and future trends,'.

Ben Farah, M.A. *et al.* (2022) 'Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends', *Information*, 13(1), p. 22. Available at: https://doi.org/10.3390/info13010022.

Fellow, S. (2016) 'Pakistan Navy ' S Emerging', (July).

Fenstad, J., Dahl, Ø. and Kongsvik, T. (2016) 'Shipboard safety: exploring organizational and regulatory factors', *Maritime Policy & Management*, 43(5), pp. 552–568. Available at: https://doi.org/10.1080/03088839.2016.1154993.

Franks, B. (2012) *Taming The Big Data Tidal Wave: Finding Opportunities in Huge Data Streams with Advanced Analytics*, *Wiley and SAS Business Series*.

Freire, W.P. *et al.* (2022) 'Towards a Secure and Scalable Maritime Monitoring System Using Blockchain and Low-Cost IoT Technology', *Sensors*, 22(13), p. 4895. Available at: https://doi.org/10.3390/s22134895.

Frøystad, C., Bernsmed, K. and Meland, P.H. (2017) 'Protecting Future Maritime Communication', in *Proceedings of the 12th International Conference on Availability, Reliability and Security*. New York, NY, USA: ACM, pp. 1–10. Available at: https://doi.org/10.1145/3098954.3103169.

Fruth, M. and Teuteberg, F. (2017) 'Digitization in maritime logistics—What is there and what is missing?', *Cogent Business & Management*. Edited by S. Liu, 4(1), p. 1411066. Available at: https://doi.org/10.1080/23311975.2017.1411066.

Galinec, D., Možnik, D. and Guberina, B. (2017) 'Cybersecurity and cyber defence: national level strategic approach', *Automatika*, 58(3), pp. 273–286. Available at: https://doi.org/10.1080/00051144.2017.1407022.

Germond, B. (2015) 'The geopolitical dimension of maritime security', *Marine Policy*, 54, pp. 137–142. Available at: https://doi.org/10.1016/j.marpol.2014.12.013.

Germond, B. and Ha, F.W. (2019) 'Climate change and maritime security narrative: the case of the international maritime organisation', *Journal of Environmental Studies and Sciences*, 9(1), pp. 1–12. Available at: https://doi.org/10.1007/s13412-018-0509-2.

Germond, B. and Mazaris, A.D. (2019) 'Climate change and maritime security', *Marine Policy* [Preprint]. Available at: https://doi.org/10.1016/j.marpol.2018.10.010.

Global., A. (2021) 'Safety & Shipping.'

Graham, E. (2014) *Syphoning Confidence: Piracy and Fuel Theft in Southeast Asia*, *RSIS Commentary*.

Greig, M., & Ronald, W.M. (2005) 'The impact of ferry services on an Island Economy'.

H, K. (2020) 'India Vs China: a comparison of the Indian and Chinese (PLA) navies.'

Hannaford, E. and Van Hassel, E. (2021) 'Risks and benefits of crew reduction and/or removal with increased automation on the ship operator: A licensed deck officer's perspective', *Applied Sciences (Switzerland)* [Preprint]. Available at: https://doi.org/10.3390/app11083569.

Hanzu-Pazara and Arsenie, R.& P. (2010) 'New challenges in the maritime academics.'

Hareide, O.S. *et al.* (2018) '"Enhancing navigator competence by demonstrating maritime cyber security,"'.

Hasan, S. *et al.* (2021) 'Evaluating the cyber security readiness of organizations and its influence on performance', *Journal of Information Security and Applications* [Preprint]. Available at: https://doi.org/10.1016/j.jisa.2020.102726.

Hayes, C.R. (2016) 'MARITIME CYBERSECURITY: THE FUTURE OF NATIONAL SECURITY'.

Hjarnoe, L. and Leppin, A. (2013) 'Health promotion in the Danish maritime setting: challenges and possibilities for changing lifestyle behavior and health among

seafarers', *BMC Public Health*, 13(1), p. 1165. Available at: https://doi.org/10.1186/1471-2458-13-1165.

ICC International Maritime Buereu (2015) 'Piracy and Armed Robbery against Ships.'

IRS (2020) '"List of Active Works Approval for In Water Inspection"'.

Islam, M.S. (2024) 'Maritime Security in a Technological Era: Addressing Challenges in Balancing Technology and Ethics', *Mersin University Journal of Maritime Faculty*, 6(1), pp. 1–16. Available at: https://doi.org/10.47512/meujmaf.1418239.

Jankowski, D. *et al.* (2022) 'Decentralized Documentation of Maritime Traffic Incidents to Support Conflict Resolution', *Journal of Marine Science and Engineering* [Preprint]. Available at: https://doi.org/10.3390/jmse10122011.

Jensen, O.C. *et al.* (2006) 'Working conditions in international seafaring', *Occupational Medicine*, 56(6), pp. 393–397. Available at: https://doi.org/10.1093/occmed/kql038.

Jepsen, J.R. *et al.* (2016) 'International Maritime Health Association (IMHA) — expanding participation, coverage and service', *International Maritime Health*, 67(1), pp. 51–53. Available at: https://doi.org/10.5603/IMH.2016.0010.

Jones, S.S.A.P.G.P. (2006) 'Maritime Security: A Practical Guide Paperback'.

Joy, J. (2021) 'Maritime Security of India: Capabilities and Challenges', *Electronic Journal of Social and Strategic Studies* [Preprint]. Available at: https://doi.org/10.47362/ejsss.2021.2308.

Kabran, E. G., & Eguavoen, I. (2019) 'Ferry transportation in Abidijan: Establishment, operation and sustainability of a paratransit system.'

Kanehara, A. (2019) 'The Use of Force in Maritime Security and the Use of Arms in Law Enforcement under the Current Wide Understanding of Maritime Security', *Atsuko Kanehara 35 Japan Review*, 3(2), pp. 1–19.

Karim, M.S. (2022) ‘Maritime cybersecurity and the IMO legal instruments: Sluggish response to an escalating threat?’, *Marine Policy* [Preprint]. Available at: https://doi.org/10.1016/j.marpol.2022.105138.

Karunya, M.F. (2024) ‘An Analysis of the Indian Government’s Recent Initiatives Pertaining To Maritime Security’, *International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)*, 7(7). Available at: https://doi.org/10.15680/IJMRSET.2024.0707259.

Kasperson, J.X. *et al.* (2003) ‘The social amplification of risk: Assessing fifteen years of research and theory’, in *The Social Amplification of Risk*. Available at: https://doi.org/10.1017/CBO9780511550461.002.

Kavallieratos, G., Diamantopoulou, V. and Katsikas, and S.K. (2020) ‘Shipping 4.0: Security requirements for the cyber-enabled ship’,.

Khalid, M. (2021) ‘National Security Concerns and India’s Expanding Naval Presence in the Indian Ocean’, *Journal of Political Science and International Relations*, 4(3), p. 72. Available at: https://doi.org/10.11648/j.jpsir.20210403.11.

Kiger, M.E. and Varpio, L. (2020) ‘Thematic analysis of qualitative data: AMEE Guide No. 131’, *Medical Teacher*, 42(8), pp. 846–854. Available at: https://doi.org/10.1080/0142159X.2020.1755030.

Koh, L.Y. *et al.* (2024) ‘Key knowledge domains for maritime shipping executives in the digital era: a knowledge-based view approach’, *Technology Analysis and Strategic Management*, 36(7), pp. 1646–1663. Available at: https://doi.org/10.1080/09537325.2022.2106841.

Kotowska, I. (2015) ‘The Role of Ferry and Ro-Ro Shipping in Sustainable Development of Transport’, *Review of Economic Perspectives*, 15(1), pp. 35–48. Available at: https://doi.org/10.1515/revecp-2015-0010.

Kraska, J., Wilson, B. (2008) ‘Fighting Pirates: The Pen and the Sword.’

Kristensen, H.M. and Korda, M. (2022) ‘Indian nuclear weapons, 2022’, *Bulletin of the Atomic Scientists*, 78(4), pp. 224–236. Available at: https://doi.org/10.1080/00963402.2022.2087385.

Kumar, P. *et al.* (2023) ‘“‘DLTIF: Deep learning-driven cyber threat intelligence modeling and identification framework in IoT-enabled maritime transportation systems,””’.

Lan, D. *et al.* (2024) ‘Application of Artificial Intelligence Technology in Vulnerability Analysis of Intelligent Ship Network’, *International Journal of Computational Intelligence Systems*, 17(1), p. 147. Available at: https://doi.org/10.1007/s44196-024-00539-z.

Lane, A.D. (1999) ‘Crew Competence.’

Lane, T. (1997) ‘Globalization, deregulation and crew competence in world shipping in McConville, James (edit).’

Leach, P.T. (2011) *Piracy Costs Shipping Industry Billions*.

Lee, H.Y. and Leung, K.Y.K. (2022) ‘Island ferry travel during COVID-19: charting the recovery of local tourism in Hong Kong’, *Current Issues in Tourism*, 25(1), pp. 76–93. Available at: https://doi.org/10.1080/13683500.2021.1911964.

Lee, P.T.-W., Kwon, O.K. and Ruan, X. (2019) ‘Sustainability Challenges in Maritime Transport and Logistics Industry and Its Way Ahead’, *Sustainability*, 11(5), p. 1331. Available at: https://doi.org/10.3390/su11051331.

Liang, T.-P. and Liu, Y.-H. (2018) ‘Research Landscape of Business Intelligence and Big Data analytics: A bibliometrics study’, *Expert Systems with Applications*, 111, pp. 2–10. Available at: https://doi.org/10.1016/j.eswa.2018.05.018.

Liss, C. (2003) ‘MARITIME PIRACY IN SOUTHEAST ASIA’, pp. 52–68.

Liwång, H., Ringsberg, J.W. and Norsell, M. (2013) 'Quantitative risk analysis – Ship security analysis for effective risk control options', *Safety Science*, 58, pp. 98–112. Available at: https://doi.org/10.1016/j.ssci.2013.04.003.

Ljung, M. (2010) 'Function Based Manning and Aspects of Flexibility'.

Longo, G. *et al.* (2023) 'Attacking (and Defending) the Maritime Radar System', *IEEE Transactions on Information Forensics and Security* [Preprint]. Available at: https://doi.org/10.1109/TIFS.2023.3282132.

Magramo, M.& L.G. (2009) 'A Noble Profession Called Seafaring: the Making of an Officer.'

Mendas, Z. (2015) 'Tracing socio-economic impact of ferry provision in Zadar island archipelago', *Journal of Marine and Island Cultures*, 4(1), pp. 10–26. Available at: https://doi.org/10.1016/j.imic.2015.06.002.

Michaela Barnett, Issah Samori, Brandon Griffin, X.-L.P. and L.P. (2023) 'A Commentary and Exploration of Maritime Applications of Biosecurity and Cybersecurity Intersections'.

Millington, I., & Funge, J. (2009) 'Artificial intelligence for games: CRC Press.'

Ministry of External Affairs (2016) 'Address by Prime Minister, Shri Narendra Modi to the Joint Session of the US Congress'.

Mirović, M., Miličević, M. and Obradović, I. (2018) 'Veliki skupovi podataka u pomorskoj industriji', *Naše more*, 65(1), pp. 56–62. Available at: https://doi.org/10.17818/NM/2018/1.8.

Mitropoulos, E.E. (2004) 'Rising to new challenges.'

Mitsatsos, D.C. (2005) 'An industry perspective on ISPS Code implementation'.

Moroni, D. *et al.* (2022) 'A mobile crowdsensing app for improved maritime security and awareness', in *2022 IEEE International Conference on Pervasive Computing and*

Communications Workshops and other Affiliated Events (PerCom Workshops). IEEE, pp. 103–105. Available at: https://doi.org/10.1109/PerComWorkshops53856.2022.9767516.

Moseley, A. (2009) 'The Implementation of International Maritime Security Instruments in CARICOM States",'.

Mraković, I. and Vojinović, R. (2019) 'Maritime Cyber Security Analysis – How to Reduce Threats?', *Transactions on Maritime Science*, 8(1), pp. 132–139. Available at: https://doi.org/10.7225/toms.v08.n01.013.

Muhdar, A., Hamzah, M.Z. and Sofilda, E. (2022) 'Maritime Security Policy for Increasing National Economic Growth in Archipelagic Country', in *International Academic Symposium of Social Science 2022*. Basel Switzerland: MDPI, p. 86. Available at: https://doi.org/10.3390/proceedings2022082086.

Munim, Z.H. *et al.* (2020) 'Big data and artificial intelligence in the maritime industry: a bibliometric review and future research directions', *Maritime Policy & Management*, 47(5), pp. 577–597. Available at: https://doi.org/10.1080/03088839.2020.1788731.

Mwango Charo, A. (2021) 'Role of Maritime Policies and Strategies in Shaping the Maritime Security Threats in Kenya', *African Journal of Empirical Research* [Preprint]. Available at: https://doi.org/10.51867/ajer.v2i1.18.

Nath, A. (2023) 'Turnaround of Palash Logistics', *Asian Journal of Management Cases*, p. 097282012211468. Available at: https://doi.org/10.1177/09728201221146859.

Nik Nor Suhaida Ali, Anas Afandi Ahmad Apandi and Laila Suriya Ahmad Apandi (2016a) 'Securing Maritime Supply Chain: Threats and Challenges of Piracy and Armed Robbery in SEA waters', *The 6th International Conference on International Studies (ICIS 2016)* [Preprint].

Nik Nor Suhaida Ali, Anas Afandi Ahmad Apandi and Laila Suriya Ahmad Apandi (2016b) ‘Securing Maritime Supply Chain: Threats and Challenges of Piracy and Armed Robbery in SEA waters’, *The 6th International Conference on International Studies (ICIS 2016)*, (September), pp. 537–547.

Nurul Fadilah (2024) ‘Implementation of National Defense in the Era of Technology in Learning Citizenship Education’, *International Journal of Students Education*, 2(2), pp. 190–194. Available at: https://doi.org/10.62966/ijose.vi.762.

Nurwahyudy, A. (2014) ‘Contemporary issues in domestic Ro-Ro passenger ferry operation in developing countries’:

Of, P. *et al.* (2013) *the Impact of Ship Crews on*.

Okafor-Yarwood, I. *et al.* (2024) ‘Technology and maritime security in Africa: Opportunities and challenges in Gulf of Guinea’, *Marine Policy*, 160(November 2023), p. 105976. Available at: https://doi.org/10.1016/j.marpol.2023.105976.

Paladin, Z. *et al.* (2022) ‘A Maritime Big Data Framework Integration in a Common Information Sharing Environment’, in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology, MIPRO 2022 - Proceedings*. Available at: https://doi.org/10.23919/MIPRO55190.2022.9803777.

Palbar Misas, J.D. *et al.* (2024) ‘Future of maritime autonomy: cybersecurity, trust and mariner’s situational awareness’, *Journal of Marine Engineering & Technology*, 23(3), pp. 224–235. Available at: https://doi.org/10.1080/20464177.2024.2330176.

Park *et al.* (2018) ‘The Impact of Ferry Disasters on Operational Efficiency of the South Korean Coastal Ferry Industry: A DEA-Window Analysis’, *The Asian Journal of Shipping and Logistics*, 34(3), pp. 248–255. Available at:

https://doi.org/10.1016/j.ajsl.2018.09.009.

Patel, B.N., Malik, A.K. and Nunes, W. (2016) *Indian Ocean and Maritime Security*, *Indian Ocean and Maritime Security: Competition, Cooperation and Threat*. Edited by B.N. Patel, A. Kumar Malik, and W. Nunes. Routledge India. Available at: https://doi.org/10.4324/9781315439761.

Pratiwi, A.C. and Tarigan, H. (2023) 'The Impact of Advanced Technology on Indonesia's National Security Stability', *Jurnal Pertahanan: Media Informasi ttg Kajian & Strategi Pertahanan yang Mengedepankan Identity, Nasionalism & Integrity* [Preprint]. Available at: https://doi.org/10.33172/jp.v9i3.16858.

Premarathna, P.K.B.I. (2021) 'Maritime Security Challenges in the Indian Ocean: Special Reference to Sri Lanka', *International Journal of Research and Innovation in Social Science*, 05(01), pp. 158–173. Available at: https://doi.org/10.47772/IJRISS.2021.5107.

PTI (2021) 'India emphasises on maritime security in Indian Ocean region', *The Hindu*.

Pyne, R.& T.K. (2005) 'Methods and Means for Analysis of Crew Communication in the Maritime Domain'.

Qiao, Z., Zhang, Y. and Wang, and S. (2021) '"'A collision risk identification method for autonomous ships based on field theory,"'.

Renganayagalu, S.K., Mallam, S.C. and Hernes, M. (2022) 'Maritime Education and Training in the COVID-19 Era and Beyond', *TransNav* [Preprint]. Available at: https://doi.org/10.12716/1001.16.01.06.

Roberts, S.E. *et al.* (2014) 'Fatal accidents and injuries among merchant seafarers worldwide', *Occupational Medicine*, 64(4), pp. 259–266. Available at: https://doi.org/10.1093/occmed/kqu017.

S. Aslam, M. P. Michaelides, and H.H. (2020) '"'Internet of Ships: A survey on

architectures, emerging applications, and challenges,’’’’.

S. Tan, J. M. Guerrero, P. Xie, R. Han, and J.C.V. (2020) ‘Brief survey on attack detection methods for cyber-physical systems,’’’.

Sadiq, M. *et al.* (2021) ‘‘‘‘Future greener seaports: A review of new infrastructure, challenges, and energy efficiency measures,’’’’.

SADOVAYA, E. (2015) ‘Effective Management of Maritime Security in Shipping Companies’, *Dr.Ntu.Edu.Sg* [Preprint].

Safitra, M.F., Lubis, M. and Fakhrurroja, H. (2023) *Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity*, *Sustainability (Switzerland)*. Available at: https://doi.org/10.3390/su151813369.

Sahu, P. (2022) ‘India’s Maritime Security: Strategy and Challenges’, *RESEARCH REVIEW International Journal of Multidisciplinary* [Preprint]. Available at: https://doi.org/10.31305/rrijm.2022.v07.i10.012.

Sanchez-Gonzalez, P.-L. *et al.* (2019) ‘Toward Digitalization of Maritime Transport?’, *Sensors*, 19(4), p. 926. Available at: https://doi.org/10.3390/s19040926.

Sapiie, M.A. (2016) ‘Indonesia to start joint sea patrols with Malaysia,philippines’.

Sarjito, A. (2024) ‘Enhancing National Security: Strategic Policy Development in Defense Management’, 2(1), pp. 56–68.

Scarlat, C., Ioanid, A. and Andrei, N. (2023a) ‘Innovative Technologies for Ports and Logistics Towards a Sustainable Resilient Future" MARLOG 12 USE OF THE GEOSPATIAL TECHNOLOGIES AND ITS IMPLICATIONS IN THE MARITIME TRANSPORT AND LOGISTICS’, *Arab Academy for Science, Technology, and Maritime Transport* [Preprint], (March).

Scarlat, C., Ioanid, A. and Andrei, N. (2023b) ‘Use of the geospatial technologies and its implications in the maritime transport and logistics’, *The International Maritime*

Transport and Logistic Journal, 12, p. 19. Available at: https://doi.org/10.21622/MARLOG.2023.12.663.

Sharad Raghvan (2015) 'High-risk area boundary shifted from India's coastline', *The Hindu*.

Shrestha, C.G. (2024) 'Contribution of Science and Technology to the Country's National Security', 5, pp. 33–40.

Silos *et al.* (2012) 'Trends in the global market for crews: A case study.'

Simola, J. *et al.* (2024) 'The Impact of Operational Technology Requirements in Maritime Industries', *European Conference on Cyber Warfare and Security*, 23(1), pp. 516–525. Available at: https://doi.org/10.34190/eccws.23.1.2357.

Simola, J. and Pöyhönen, J. (2022) 'Emerging Cyber risk Challenges in Maritime Transportation', *International Conference on Cyber Warfare and Security* [Preprint]. Available at: https://doi.org/10.34190/iccws.17.1.46.

Sirimanne *et al.* (2019) 'Review of maritime transport 2019.'

Skjong, E. *et al.* (2016) 'Past, present, and future challenges of the marine Vessel's electrical power system,'''.

Skjong, R. (2009) 'Risk-Based Ship Design – Methods, Tools and Applications'.

Sklet, S. (2006) 'Safety barriers: Definition, classification, and performance', *Journal of Loss Prevention in the Process Industries* [Preprint]. Available at: https://doi.org/10.1016/j.jlp.2005.12.004.

Tabish, N. and Chaur-Luh, T. (2024) 'Maritime Autonomous Surface Ships: A Review of Cybersecurity Challenges, Countermeasures, and Future Perspectives', *IEEE Access*, 12(February), pp. 17114–17136. Available at: https://doi.org/10.1109/ACCESS.2024.3357082.

Thai, V. V. and Grewal, D. (2007) 'The maritime security management system:

Perceptions of the international shipping community', *Maritime Economics and Logistics* [Preprint]. Available at: https://doi.org/10.1057/palgrave.mel.9100175.

Treves, T. (2009) 'Piracy, law of the sea, and use of force: Developments off the coast of somalia', *European Journal of International Law* [Preprint]. Available at: https://doi.org/10.1093/ejil/chp027.

UNCTAD. (2018) 'Review of Maritime Transoprt.'

UNODC (2024) *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud , Underground Banking and Technological Innovation in Southeast Asia : A Shifting Threat Landscape October 2024*, *UNITED NATIONS OFFICE ON DRUGS AND CRIME*.

Upadhyaya, S. (2018) 'Maritime Security Cooperation in the Indian Ocean Region: Assessment of India's Maritime Strategy to be the Regional "Net Security Provider"'.

USLUER, H.B. (2022) 'The effect of the developing and changing Electronic Bridge Equipment and Electronic Navigation Charts on Intelligent Maritime Transportation Systems', *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi*, 5(1), pp. 116–125. Available at: https://doi.org/10.51513/jitsa.1097807.

Wang, J. *et al.* (2020) '"'A survey of technologies for unmanned merchant ships,"'".

Wengelin, M. (2012) 'Service, regulations, and ports.'

Wirawan, D. (2022) 'MARITIME SECURITY INCREASES DEFENSE DIPLOMACY IN THE WORLD MARITIME AXIS FRAMEWORK', 8(1).

Wisdom, T., & Kamanga, T. (2002) 'Development and implementation of uniform safety standards for inland waterways vessels and non-convention craft in Africa: The case of the Southern African Development Community (SADC)'.

Yang, D. *et al.* (2019) 'How big data enriches maritime research – a critical review of

Automatic Identification System (AIS) data applications', *Transport Reviews*, 39(6), pp. 755–773. Available at: https://doi.org/10.1080/01441647.2019.1649315.

Zarzuelo, I. de la P., Soeane, M.J.F. and Bermúdez, and B.L. (2020) ""'Industry 4.0 in the port and maritime industry: A literature review,"".

Zhang, Y. *et al.* (2022) 'Design and Development of Maritime Data Security Management Platform', *Applied Sciences*, 12(2), p. 800. Available at: https://doi.org/10.3390/app12020800.

Zhong, M. and Meng, F. (2019) 'A YOLOv3-based non-helmet-use detection for seafarer safety aboard merchant ships', *Journal of Physics: Conference Series*, 1325(1), p. 012096. Available at: https://doi.org/10.1088/1742-6596/1325/1/012096.

APPENDIX A:

DATASET

	A	B	C	D	E	F
1	Is your country signatory to? (UN	Is your country signatory to? (S	Is your country signatory to?	Is your country signatory to? (S	Is your country signatory to? (ILO Co	Do you feel, in the present day scena
2	1	1	1	1	1	1
3	1	1	1	1	1	1
4	1	2	2	1	2	1
5	1	1	1	1	1	1
6	1	1	1	1	1	1
7	1	1	1	1	2	1
8	1	1	1	1	1	1
9	2	1	2	1	2	1
10	1	1	1	1	1	1
11	1	1	1	1	1	1
12	1	1	1	1	1	1
13	1	1	1	1	1	1
14	1	1	1	1	1	1
15	1	2	2	1	1	1
16	1	1	1	1	2	1
17	1	1	1	1	1	1
18	1	1	1	1	2	1
19	1	2	1	2	1	2
20	1	1	1	1	1	1
21	1	2	1	1	1	1
22	1	1	1	1	1	1
23	1	2	1	1	2	1
24	1	1	1	1	1	1
25	1	1	1	1	1	1

	G	H	I	J	K
1	In your opinion, which crime poses th	In your opinion, are the instruments a	In your Flag Administration is the san	How frequently does the maritime ad	How are the data listed below being s
2	1	1	2	1	1
3	2	1	1	4	1
4	2	1	2	2	2
5	3	1	2	6	2
6	1	1	1	3	1
7	2	1	1	3	1
8	1	1	1	2	2
9	2	2	1	3	2
10	6	1	1	3	2
11	2	1	2	3	1
12	1	1	1	1	1
13	2	1	1	1	1
14	1	2	1	5	3
15	3	1	1	3	2
16	3	1	1	3	1
17	2	1	1	2	2
18	3	1	1	3	1
19	2	1	2	2	1
20	3	1	1	3	1
21	4	1	2	3	1
22	1	2	1	2	1
23	4	1	1	2	1
24	1	1	1	1	1
25	1	1	1	4	1

	L	M	N	O	P
1	How are the data listed below being s	How are the data listed below being s	How are the data listed below being s	Is the tech2logy required under differ	Is the tech2logy required under differ
2	3	3	1	2	1
3	1	1	1	1	1
4	1	3	2	1	1
5	1	2	3	2	1
6	2	3	1	1	1
7	3	2	1	1	1
8	3	3	3	1	1
9	3	2	2	2	1
10	1	2	1	1	1
11	3	1	2	1	2
12	1	1	1	1	1
13	1	1	1	1	1
14	1	2	1	1	2
15	3	1	3	1	2
16	1	1	1	1	1
17	2	1	2	1	2
18	2	2	1	1	1
19	2	1	1	2	1
20	2	1	3	1	1
21	1	2	2	1	1
22	1	1	1	1	1
23	3	2	2	1	1
24	1	1	1	1	1
25	1	1	1	1	1

	Q	R	S	T	U
1	Is the tech2logy required under diffe	How does your organization motivate	Are the present manning levels onbc	Present trend shows that certain flag	How effective do you think the role of
2	2	1	2	1	2
3	1	2	1	1	1
4	1	2	1	2	1
5	1	1	1	1	2
6	1	1	1	1	1
7	1	1	2	2	1
8	2	2	1	2	2
9	2	1	2	2	1
10	1	2	2	1	1
11	1	2	1	2	2
12	1	1	1	1	1
13	1	1	1	1	1
14	2	2	2	1	1
15	1	2	2	1	2
16	1	1	1	1	1
17	1	2	2	2	1
18	1	2	1	1	1
19	2	1	1	2	2
20	1	2	1	1	1
21	1	1	1	2	1
22	1	1	1	1	1
23	1	2	1	1	1
24	1	1	1	1	1
25	1	1	1	1	1

	V	W	X	Y	Z
1	Have you dealt with a security incider	How would you rate the response of	Is Vessel Traffic System (VTS) foster	Is VTS a deterrent or an active measu	Will interfacing of radar with AIS enha
2	1	2	2	2	1
3	1	1	1	1	1
4	1	2	1	2	1
5	2	1	2	2	1
6	1	1	1	2	1
7	2	2	1	1	1
8	2	2	1	2	2
9	2	2	1	2	2
10	1	2	1	1	1
11	1	2	1	1	1
12	1	1	2	1	1
13	1	1	1	2	1
14	2	2	1	1	1
15	1	1	2	1	2
16	1	1	1	1	1
17	1	2	2	2	1
18	1	1	1	1	1
19	1	2	1	2	1
20	1	1	1	1	1
21	1	2	1	1	1
22	1	1	1	1	1
23	2	1	1	1	1
24	1	1	1	1	1
25	1	1	1	1	1

	AA	AB	AC	AD	AE
1	Will long -range identification and trac	Do you have any experience in securi	Taking into consideration the securit	There are different ship reporting sy	In your opinion should reporting to ar
2	1	1	2	2	1
3	1	1	1	1	1
4	1	2	2	1	2
5	1	2	1	1	2
6	1	1	2	1	1
7	1	1	1	1	1
8	1	1	2	2	2
9	1	1	1	2	2
10	1	2	2	2	2
11	2	1	2	1	1
12	1	1	1	1	1
13	1	2	2	1	2
14	1	2	2	1	1
15	1	2	1	2	2
16	1	1	1	1	1
17	1	1	1	2	1
18	2	1	1	1	1
19	1	1	1	1	1
20	1	1	1	1	1
21	1	1	1	1	1
22	1	1	1	1	1
23	2	1	2	1	1
24	1	1	1	1	1
25	1	1	2	1	1

	A	B	C	D	E
1	Do you feel, in the present-day scena	In your opinion, which crime poses th	In your opinion, are the instruments a	How frequently does the maritime ad	How are the data listed below being s
2	2	3	1	3	1
3	1	4	2	2	2
4	1	2	1	5	2
5	1	4	2	4	3
6	1	1	1	2	3
7	1	4	1	4	1
8	1	2	1	3	2
9	1	1	1	4	1
10	1	4	2	4	1
11	1	1	1	4	2
12	1	1	1	2	1
13	1	1	1	2	1
14	1	1	1	4	3
15	2	3	2	2	3
16	2	7	1	2	1
17	1	1	1	1	1
18	1	3	1	2	1
19	1	3	1	1	2
20	1	1	1	1	1
21	1	1	1	1	1
22	1	4	1	5	1
23	1	2	1	2	2
24	1	2	1	3	2
25	1	3	1	4	1
26	1	2	1	4	1

	F	G	H	I	J
1	How are the data listed below being s	How are the data listed below being s	How are the data listed below being s	Is the tech2logy required under diffe	Is the tech2logy required under diffe
2	1	3	1	1	1
3	3	1	1	1	2
4	2	2	2	2	2
5	2	3	1	2	1
6	3	2	1	1	2
7	1	1	3	2	1
8	2	3	1	2	1
9	1	1	1	1	1
10	2	1	2	2	1
11	1	3	1	2	1
12	1	1	2	1	1
13	1	1	2	1	1
14	2	1	2	2	1
15	1	2	2	1	2
16	2	1	2	2	1
17	1	1	1	1	1
18	1	1	1	1	1
19	1	3	2	1	1
20	1	1	1	1	1
21	1	1	1	1	1
22	1	1	3	1	1
23	1	2	3	2	1
24	3	1	2	1	1
25	2	1	2	1	1
26	2	1	3	1	1

	K	L	M	N	O
1	Is the tech2logy required under diffe	As a maritime law enforcement agen	How effective do you think the role of	Have you dealt with a security incider	How would you rate the response of
2	1	1	2	2	1
3	1	1	2	1	1
4	2	2	2	2	2
5	1	2	1	2	2
6	2	2	1	1	2
7	2	2	1	1	1
8	2	2	2	1	1
9	1	1	1	1	1
10	1	2	2	1	1
11	2	1	2	1	1
12	1	1	1	1	1
13	1	1	1	2	1
14	2	2	1	2	2
15	1	2	1	2	1
16	1	1	2	1	1
17	1	1	1	1	1
18	1	1	1	1	1
19	1	1	1	1	1
20	1	1	1	1	1
21	1	2	1	1	1
22	1	1	1	1	1
23	1	2	2	1	1
24	1	1	1	1	1
25	2	1	1	2	2
26	1	1	1	1	1

	P	Q	R	S	T
1	Is Automatic Identification System (2)	Is Vessel Traffic System (VTS) foster	Is VTS a deterrent or an active measu	Will mandatory reporting to Vessel T	Will interfacing of radar with 2 enhanc
2	2	1	2	2	1
3	2	1	1	1	2
4	2	2	2	2	2
5	2	2	1	1	1
6	2	1	2	1	1
7	2	1	2	2	1
8	2	2	1	1	1
9	1	1	2	1	1
10	2	1	2	1	2
11	2	1	1	2	1
12	1	1	2	1	1
13	1	1	2	1	1
14	2	1	1	1	2
15	2	1	2	2	1
16	1	2	1	1	1
17	1	1	1	1	1
18	1	1	1	1	1
19	1	1	1	1	1
20	1	1	2	1	1
21	1	2	2	1	1
22	1	1	1	1	1
23	1	2	2	1	1
24	1	2	1	2	1
25	1	1	1	2	1
26	2	1	1	1	2

	U	V	W	X	Y
1	Will long-range identification and trac	Do you have any experience in securi	Taking into consideration the securit	There are different 1 systems worldv	In your opinion should reporting to a
2	2	2	1	2	1
3	1	2	1	1	2
4	2	2	2	2	2
5	1	2	1	2	2
6	2	2	2	1	2
7	1	2	1	2	2
8	1	1	1	1	1
9	1	1	1	1	1
10	1	1	1	2	2
11	1	1	2	1	1
12	1	1	1	1	1
13	1	1	1	2	1
14	1	2	2	1	1
15	2	1	2	1	1
16	1	1	2	1	1
17	1	1	1	1	1
18	1	1	2	1	1
19	1	1	1	1	1
20	1	1	2	1	1
21	1	2	1	1	1
22	1	1	1	1	2
23	2	1	1	1	1
24	1	2	2	2	2
25	2	1	2	1	1
26	1	1	1	2	1

	A	B	C	D	E
1	Do you feel, in the present-day scena	In your opinion, which crime poses th	In your opinion, are the instruments a	Is the tech2logy required under diffe	Is the tech2logy required under diffe
2	1	2	2	2	1
3	1	4	2	2	2
4	1	3	1	2	1
5	1	4	1	1	1
6	2	3	1	2	2
7	1	3	1	1	2
8	1	4	1	2	2
9	1	5	1	1	1
10	1	2	1	1	1
11	1	1	1	1	1
12	1	1	1	1	1
13	2	2	1	2	1
14	2	1	2	1	1
15	1	6	1	1	1
16	1	1	1	1	1
17	1	5	1	1	1
18	1	5	1	1	1
19	1	2	1	1	2
20	1	2	1	1	1
21	1	1	1	1	1
22	1	2	1	1	1
23	1	2	1	1	1
24	1	1	1	1	1
25	1	1	1	1	1
26	1	3	1	1	2

	F	G	H	I	J
1	Is the tech2logy required under diffe	How does your organization motivate	Are the present manning levels onbc	Present trend shows that certain flag	How effective do you think the role of
2	1	1	1	1	2
3	1	2	2	1	1
4	2	3	1	1	1
5	2	2	2	1	1
6	1	2	2	1	2
7	1	3	1	1	2
8	1	2	1	1	2
9	1	2	1	1	2
10	1	1	1	1	1
11	1	1	1	1	1
12	1	1	1	1	1
13	2	2	1	2	1
14	2	3	1	1	2
15	1	1	1	1	1
16	1	2	1	1	1
17	1	1	1	1	1
18	1	2	1	1	1
19	1	1	2	1	1
20	1	1	1	1	1
21	1	1	1	1	1
22	1	2	1	1	1
23	1	1	1	1	1
24	1	1	1	1	1
25	1	1	1	1	1
26	2	3	1	2	2

	K	L	M	N	O
1	Have you dealt with a security incider	How would you rate the response of	Is Automatic Identification System (A	Is Vessel Traffic System (VTS) foster	Is VTS a deterrent or an active measu
2	1	1	2	1	1
3	2	2	2	2	1
4	1	1	1	2	2
5	2	1	1	1	1
6	1	2	1	2	1
7	2	2	2	2	2
8	1	2	1	2	2
9	1	1	2	1	2
10	1	1	1	1	2
11	1	1	1	2	2
12	1	1	1	2	1
13	2	1	2	2	1
14	2	1	2	1	1
15	1	1	1	1	2
16	1	1	1	1	1
17	1	1	1	1	1
18	1	1	1	1	2
19	1	2	1	1	1
20	1	1	1	1	1
21	1	1	2	1	1
22	1	1	1	1	1
23	1	1	2	1	2
24	1	1	1	1	1
25	1	1	1	1	1
26	2	1	1	1	2

	P	Q	R	S	T
1	Will mandatory reporting to Vessel T	Will interfacing of radar with AIS enha	Will long-range identification and trac	Do you have any experience in securi	Taking into consideration the securit
2	1	1	1	2	1
3	1	1	1	1	1
4	1	2	1	2	2
5	1	2	1	1	1
6	1	2	2	2	2
7	2	1	2	1	2
8	1	1	2	2	2
9	1	2	1	1	1
10	1	1	1	1	2
11	1	1	1	1	1
12	1	1	2	2	2
13	2	1	2	2	1
14	1	2	1	2	1
15	1	1	1	1	1
16	1	1	1	1	2
17	1	1	1	1	1
18	1	1	1	1	2
19	1	1	1	1	2
20	1	1	2	1	2
21	1	1	1	1	2
22	1	2	1	1	1
23	1	1	1	2	2
24	1	1	1	1	1
25	1	1	1	1	1
26	1	2	2	1	2

	U	V	W	X	Y
1	There are different ship reporting sy	In the present security scenario, will	In your opinion should reporting to a	Does the Vessel Data Recorder (VDR)	Does the Vessel Data Recorder (VDR)
2	1	1	1	1	1
3	1	1	2	2	2
4	2	1	1	2	1
5	1	2	2	1	2
6	1	1	2	2	2
7	1	2	1	2	1
8	1	2	1	1	2
9	1	1	1	1	1
10	1	1	1	1	1
11	1	1	1	1	1
12	1	1	1	1	1
13	2	2	1	2	2
14	2	1	1	2	2
15	1	1	1	1	1
16	1	1	1	1	1
17	1	1	1	1	1
18	1	1	1	1	1
19	1	2	1	1	1
20	1	1	1	1	1
21	1	1	1	1	1
22	1	1	1	1	1
23	1	1	1	1	1
24	1	1	1	1	1
25	1	1	1	1	1
26	2	1	2	1	1