10-31-2022

Threats and challenges to maritime autonomous surface ships (MASS): role of law enforcement agencies

Muhammad Adil Bajwa

WORLD MARITIME UNIVERSITY
Malmö, Sweden

THREATS AND CHALLENGES TO MARITIME AUTONOMOUS SURFACE SHIPS (MASS) – ROLE OF LAW ENFORCEMENT AGENCIES

By

MUHAMMAD ADIL BAJWA
PAKISTAN

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

MASTER OF SCIENCE
in
MARITIME AFFAIRS

(MARITIME SAFETY AND ENVIRONMENTAL ADMINISTRATION)

2022

Declaration

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

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

(Signature): ______________

(Date): 9 September 2022

Supervised by: Dr Chong Ju Chae

Supervisor's affiliation: Assistant Professor at
World Maritime University (WMU), Malmo, Sweden

Acknowledgement

It is an honor and a privilege for me to be a part of WMU. I would like to extend my deep appreciation to all the professors and staff of WMU who made it possible for me to achieve my desired goals. It would never have been possible without them.

I also extend my heartiest thanks to my supervisor; Assistant Professor Dr. Chong Ju Chae from South Korea; who has been guiding me throughout my writing and giving the desired guidelines through his professional skills. With his keen interest, vision and sound knowledge on the same subject, I was able to render my views into a logical and reasonable manner.

I would also like to thank my esteemed organization Pakistan Navy for providing me an opportunity to attend the Master’s degree programme. A very special thanks to Australian Maritime Safety Authority (AMSA) for providing me full fellowship at WMU. My honest recognition for admin staff who facilitated me in every way and made my stay at HSR very comfortable. Here I would not miss the opportunity to say special thanks to the Library staff and the World Bistro team who have taken care of our needs while being at the WMU.

In the end, I pay tribute to my parents, wife Saira, daughter Azmay and my twins (Aanzay and Muhammad Mustafa Bajwa) for their support, love and prayers during my entire Master’s degree program. Indeed, during fatigue and hard time, their encouragement played an important role to boost my moral for continuity and determination at WMU.

Abstract

Title of Dissertation: **Threats and Challenges to Maritime Autonomous Surface Ships – Role of Law Enforcement Agencies**

Degree: **Master of Science**

MASS will be the future of shipping industry. Technology has proven that machines and high tech systems can replace men presence onboard at sea, which is considered a devastating development in the human race. MASS is also being widely accepted in the world and has also proven itself as the future for sustainable shipping. With this great advancement, shipping industry may also face bigger challenges related to maritime security.

In maritime security the major threat includes, terrorism, piracy, cyber threats and armed robbery. Considering all these, IMO has formulated many regulations for implementation. The fear of transformation of ship into a weapon was always there. However, with the arrival of MASS, this fear has increased and may also be a threat to maritime security. Furthermore, the ultra-technological variations will have definite consequences in the implementation scheme too. The notion of independent, unmanned vessels upsets the complete maritime regulatory setup and interrupts the fundamental ideas of law.

Based on these challenges and threats posed by MASS, this dissertation deliberates upon the threats and challenges to MASS and role of law enforcement agencies (LEA's). The technological shift when crewless ships operate at sea will witness higher security challenges. For this reason, there is a need of possible mitigation measures to be investigated. On MASS and SCC, threat like cyber-attack and physical attack are more as compared to other conventional ships. To overcome these threats, shipping industry, manufacturers and LEA's have to think, coordinate and develop global strategy for the safety and security of MASS and SCC. There is also a need to impose and implement regulations related to new emerging security risks by IMO. Port security measures need to be enhanced and required to undertake risk assessment. Stringent security measures must be taken against cyber and physical threats to MASS/SCC. Subsequently, the dissertation deliberates upon the necessity for applicable solutions for dealing and avoiding these two security threats.

Keywords: Maritime Autonomous Surface Ships (MASS), Unmanned Ships, Autonomous ships, Shore Control Centers (SCC), Maritime Security, Piracy, Cyber-piracy/attack, Maritime law enforcement.

Table of Contents

Table of Figures

List of Tables

List of Abbreviations

AAWA:	Advance Autonomous Waterborne Application Initiative
AIS:	Automatic Identification System
AI:	Artificial Intelligence
AS:	Autonomous Ships
CCS:	China Classification Society
CPS:	Cyber Physical Systems
CSI:	Container Security Initiatives
CSO:	Company Security Officer
CTF:	Combined Task Forces
DNV:	Det Norske Veritas
ECDIS:	Electronic Chart Display and Information System
EU:	European Union
GDMSS:	Global Maritime Distress and Safety System
GPS:	Global Positioning System
GoO:	Gulf of Oman
HD:	High Definition
HF:	High Frequency
ICT:	Information Communication Technology
IMO:	International Maritime Organization
INS:	Inertial Navigation System
IR:	Infra-Red
ISSC:	International Ship Security Certificate
IoT:	Internet of Things
ISPS:	International Ship and Port Facility Security
IT:	Information Technology

JNCPT:	Jawaharlal Nehru Container Port Terminal
LEAs:	Law Enforcement Agencies
LIDAR:	Light Detection and Ranging
LR:	Lloyd's Register
MASS:	Maritime Autonomous Surface Ships
MIS:	Management Information System
MSC:	Maritime Safety Committee
MUNIN:	Maritime Unmanned Navigation through Intelligence Networks
NSA:	Non-State Actors
OT:	Operations Technology
PFSA:	Port Facility Security Assessment
PFSO:	Port Facility Security Officer
PFSP:	Port Facility Security Plan
PoLA:	Port of Los Angeles
RADAR:	Radio Direction and Ranging
RCC:	Remote Control Centre
RSE:	Regulatory Scoping Exercise
RQ:	Research Question
SCC:	Shore Control Centers
SME:	Subject Matter Experts
SOLAS:	Safety of Life at Sea
SSA:	Ship Security Assessments
SSO:	Ship Security Officer
SSP:	Ship Security Plan
SUA:	Suppression of Unlawful Acts
SVAN:	Saver Vessel with Autonomous Navigation
UHF:	Ultra High Frequency

UKMTO:	United Kingdom Maritime Trade Operations
UNCLOS:	United Nation Convention on the Law of the Sea
UNCTAD:	United Nations Conference on Trade and Development
US:	United States
VHF:	Very High Frequency
VTS:	Vessel Tracking System
WMU:	World Maritime University

Chapter 1 - Introduction

1.1 Background

Shipping industry is the backbone of international economy and almost 90% of the worldwide trade is being passed through international transport industry (UNCTAD, 2020). In 2011 Germany introduced the expression “Industry 4.0” which is recognized as the fourth Industry technology/revolution. According to Imran and Kantola, Industry 4.0 revolution was introduced due to rapid growth of contemporary technologies, which comprises of Internet of Things (IoT), cloud computing, Artificial Intelligence (AI), hyper-connectivity, automation, big datas and analytic advanced, smart and hyper-connected technologies (2018). In addition to this, it is highlighted that shipping industry has also revolutionized itself in respect of new technology, digitalization and automation (ICS, 2021). Therefore, in shipping sector, Shipping 4.0 revolution/uprising has been known as Autonomous Ships (AS) or Maritime Autonomous Surface Ships (MASS) which are being operated/handled from a Remote Control Centers (RCCs) also called Shore Control Centers (SCCs) by an automatic program and decision-making systems (Emad et al, 2020; Sakhi et al, 2019).

1.2 Definitions of MASS

There are many definitions of MASS, in recent past many research institutes, organizations and governments have conducted a number of researches on MASS. MASS is however still is in the phase of research, development and testing. Therefore, MASS has no official and defined definition. However, in many MASS studies, the European Union Maritime Unmanned Navigation through Intelligence Networks (MUNIN) project, DET NORSKE VERITAS (DNV), Lloyd's Register (LR), and China Classification Society (CCS) provides MASS’s descriptive definition.

MASS is defined by CCS as:

> *“It refers to a vessel using different forms of communications, sensors, IoTs and other ways for obtaining and perceiving information in an automatic manner. It also uses technology and automation to gather data*

> *of various elements such as the marine environment, port and logistics.*" (CCS, 2015)

According to DNV, MASS is defined as:

> "*These vessels are based on self-governance as well as automation to different extent." (Rødseth & Nordahl, 2017)*

MASS defined by IMO, as:

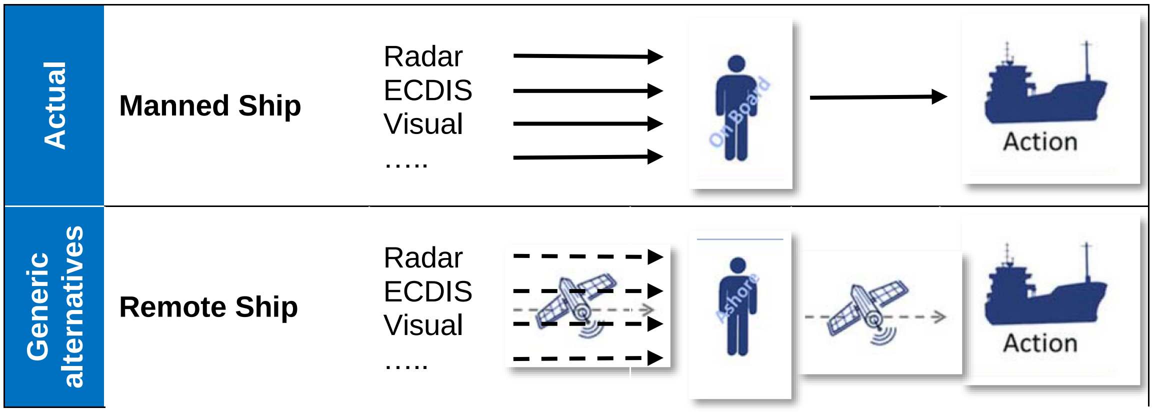
> "A *vessel that is capable to operate without human interaction to various degrees*." (IMO, 2018)

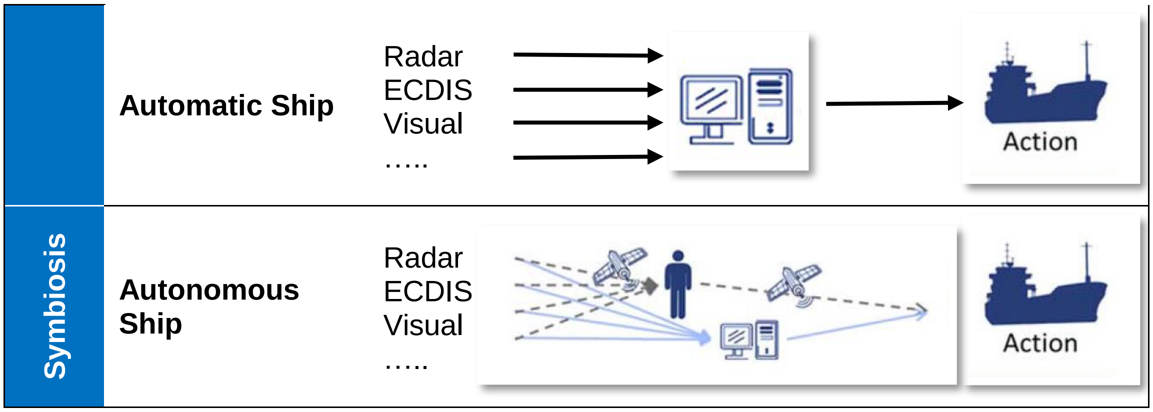
According to MUNIN MASS is defined as:

> "*It is regarded as vessel possessing communication based technology and control systems of next generation. This enables remote monitoring and controlling as it has advanced support systems for effective decision making and the ability to operate through full or partial autonomous control* " As shown in the figure 1. (Fraunhofer, 2015; Munin, 2019, p.3).

Figure 1

Envisaged Ship Control Methods



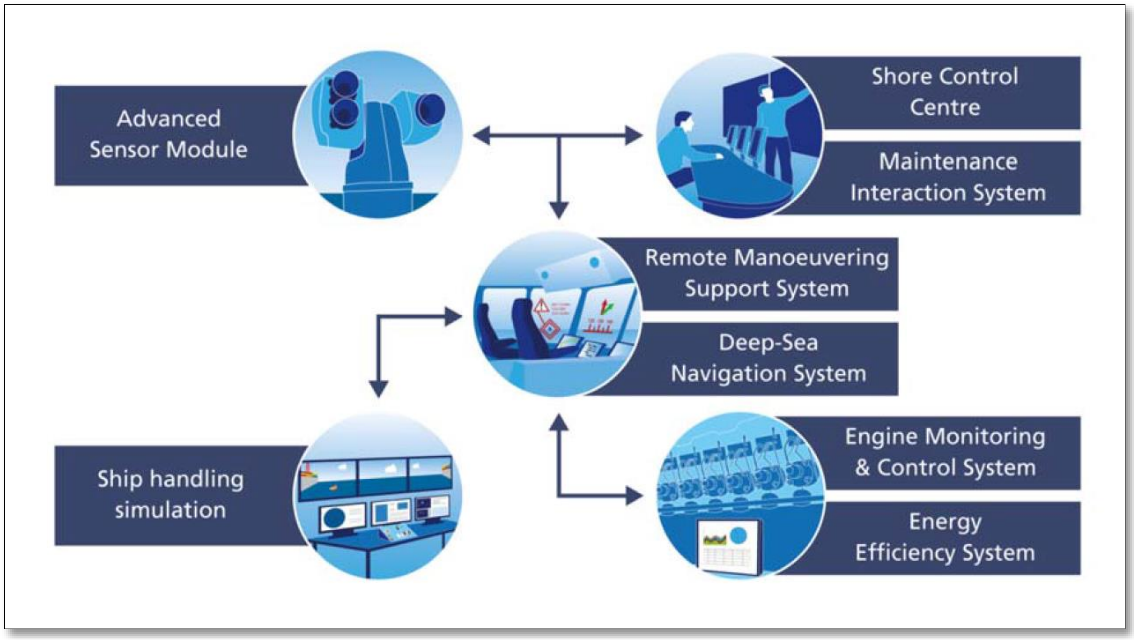


Note. Adapted from "SWOT-AHP Analysis of Autonomous Shipping," by Şenol, Y., Gokcek, V., & Seyhan, A. 2017, Paper presented at the 4th International Multidisciplinary Congress of Eurasia Proceedings, p. 58-69.

The project of MUNIN explains that, computers onboard ships have been programed in such a way that sailing will be done automatically at high seas through these computer systems. However, an operator who is on shore will control and monitor the ship movement from Shore Control Center (SCC) (Rødseth et al, 2012), which is shown in figure 2. Therefore, whenever the ship need intervention, it can be done through communication with Vessel Tracking System (VTS) or with another unit which is operating in that vicinity (MUNIN, 2016).

Figure 2

MUNIN Network


Advanced Sensor Module
Shore Control Centre
Maintenance Interaction System
Remote Manoeuvering Support System
Deep-Sea Navigation System
Ship handling simulation
Engine Monitoring & Control System
Energy Efficiency System

Note. *Adapted from "Research in maritime autonomous systems project results and technology potentials (final brochure) & nbsp," by Maritime Unmanned Navigation through Intelligence in Network MUNIN, 2016, (http://www.unmannedship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf).*

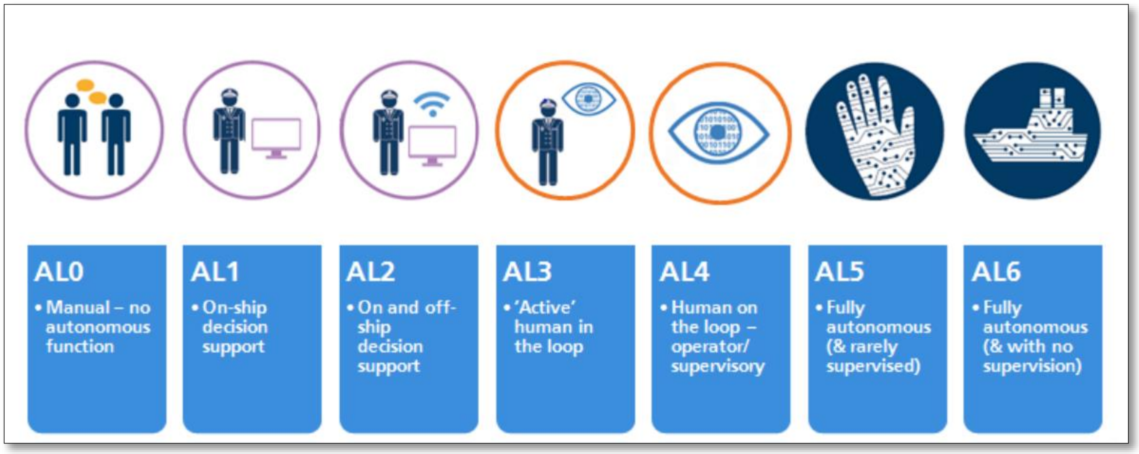
Keeping in view the, above definitions and researches, MASS can be referred ship with high tech sensors, automated digital navigation and auxiliary propulsion systems, self-automated decision logics to follow plans, automated/digital environment sensors, automatically adjustable mission execution considering the environmental conditions and actually operate without human involvement.

1.3 **Levels/Degrees of Autonomy**

Globally there are various agencies/organizations who have discussed in detail upon the different level of autonomy for autonomous ships. There are more than six authorities have defined the categories for degrees of autonomy (Zhou et al, 2019). According to Llyod, seven different levels of autonomy are there which is shown in figure 3 (2016).

Figure 3

Seven Levels of Autonomy

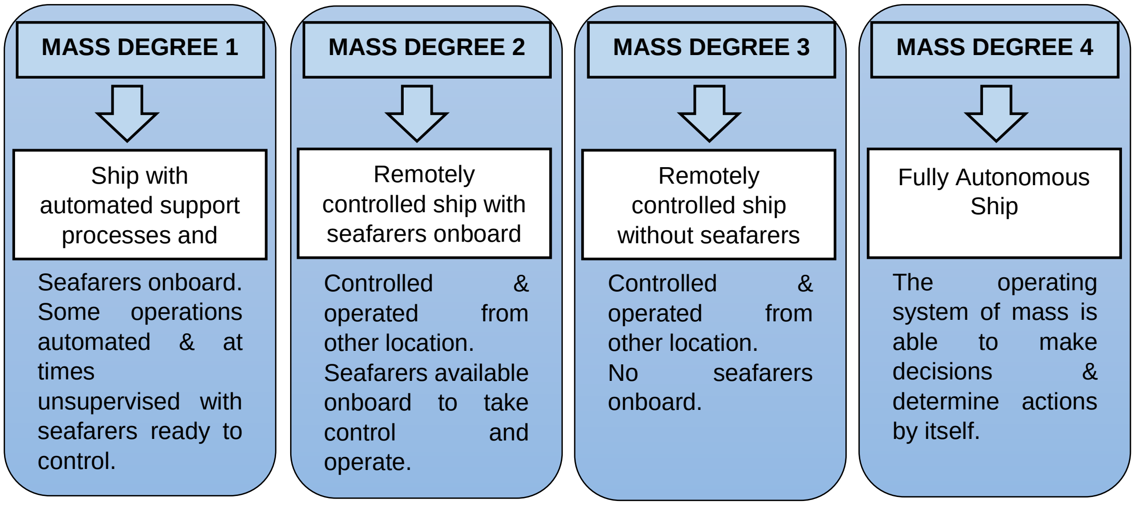

AL0
• Manual – no autonomous function
AL1
• On-ship decision support
AL2
• On and off-ship decision support
AL3
• 'Active' human in the loop
AL4
• Human on the loop – operator/ supervisory
AL5
• Fully autonomous (& rarely supervised)
AL6
• Fully autonomous (& with no supervision)

Note. Adapted from "Cyber-enabled ships Ship Right Procedure. LR defines 'autonomy levels' for ship design and operation," by Lloyd's Register Group Services Limited, 2016, (https://www.lr.org/en/latest-news/lr-defines-autonomy-levels-for-ship-design-and-operation/).

The autonomy level which is suggested by Danish Maritime Authority is adopted by IMO as shown in figure 3 (Zhou et al, 2021). There are four degrees of ship automation identified by IMO in Regulatory Scoping Exercise (RSE) as shown in figure 4 (IMO, 2018a).

Figure 4

Degrees of Automation

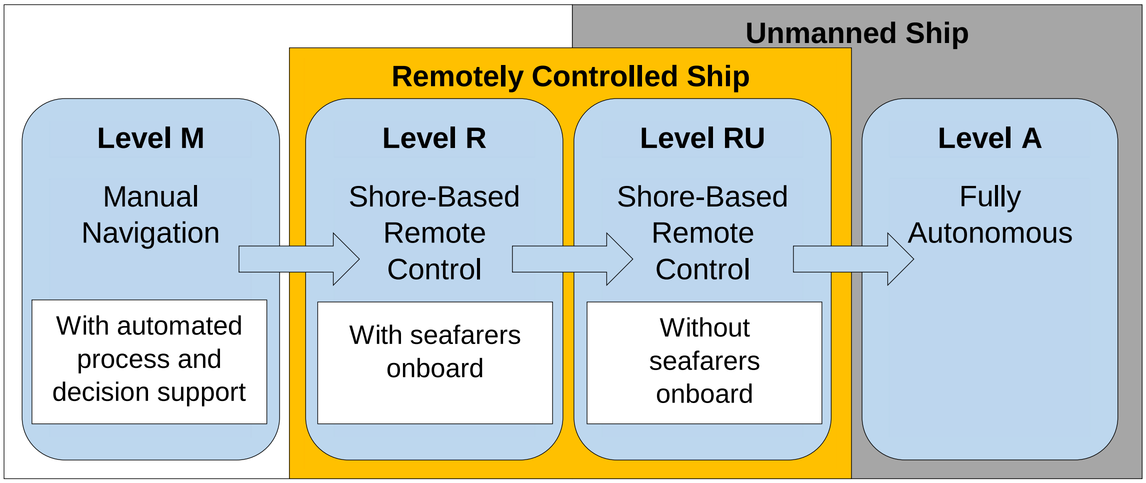

MASS DEGREE 1
Ship with automated support processes and
Seafarers onboard. Some operations automated & at times unsupervised with seafarers ready to control.
MASS DEGREE 2
Remotely controlled ship with seafarers onboard
Controlled & operated from other location. Seafarers available onboard to take control and operate.
MASS DEGREE 3
Remotely controlled ship without seafarers
Controlled & operated from other location. No seafarers onboard.
MASS DEGREE 4
Fully Autonomous Ship
The operating system of mass is able to make decisions & determine actions by itself.

Note. Prepared from "Maritime Safety Committee 100th Session MSC 100/ WP.8," by International Maritime Organization, 2018a, Working group report in 100th session of IMO MSC for the RSE for the use of MASS.

At degree three and four i.e. at levels "RU" and "A" as shown in figure 5, there will be no seafarer onboard ship. Ships will be controlled from shore remotely/fully autonomous with no human involvement (Klein, 2019; Şenol et al, 2017). Degree of MASS autonomy is however not essentially linear or hierarchical. During any single passage MASS can work more than one degrees of autonomy (Chae et al, 2020).

Figure 5

MASS – Taxonomy of Autonomy Level



Note. Adapted from "A system-theoretic approach to safety and security co-analysis of autonomous ships," by Zhou, X., Liu, Z., Wang, F., & Wu, Z. 2021, Ocean Engineering, 222, 108569.

1.4 **Progress/Timeline/Development in MASS**

The concept of automation is not very old old. Since the advent of computer technology, the self-steered autonomous robots are available and working all around in every part of the world in different forms and ways. With the passage of time there have been major improvements in the field of automation and technology, as a result smart ships have caught the attention of maritime sector (Chae et al, 2020). The very first cargo autonomous ship in the world is the *Yara Birkeland*, Norway (WMU, 2019). EU flagship-project MUNIN are the first to conduct study on a crewless and autonomous merchant ship, which led other companies and organizations to launch other concept ships in Europe as shown in 1 (Rødseth et al., 2021; Wariishi, 2019).

Table 1

European Initiatives in Development of Autonomous Ships

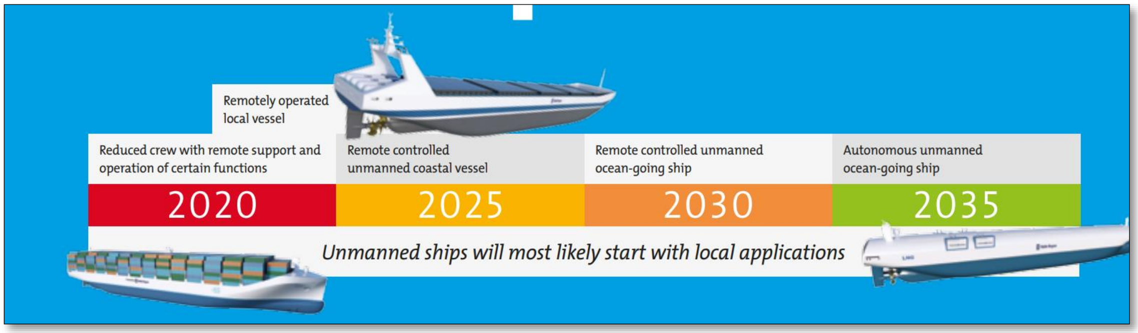
Projects with Industry- Government-Academia Collaboration		
MUNIN	Maritime Unmanned Navigation through Intelligence in Network	• Implemented from 2012-2015. • With the support of EU, the Fraunhofer Institute took the lead in developing the concept of unmanned vessels and conducting pilot program. • Announced the effect of fueling efficiency by 10% or more and reducing the risk of collision and sinking.
AAWA	Advance Autonomous Waterborne Application Initiative	• Implemented from 2015-2018. • Lead by Rolls-Royce, with the support of government of Finland. • Examined legal regulations and technical elements necessary for the realization of autonomous ships, and conducted research based on conceptual studies.
Efforts by Companies (primarily efforts towards practical applications)		
Yara International	Major Norwegian fertilizers maker	• Unmanned electronic container ship “Yara Birkeland” scheduled to be put into service in 2022. • Development is supported by a subsidy from the Norwegian government.
Kongsberg	Maritime division of a Norwegian public-private enterprise	
Rolls-Royce Commercial Marines	Now part of Kongsberg	• Under the SVAN (Saver Vessel with Autonomous Navigation) project, demonstrated autonomous operation of a freight and passenger ferry (coastal ship). • Owned by Finland’s Finferries in December 2018.
Wartsila	Finnish marine engine manufacturer	• Demonstrated autonomous operations of a freight and passenger ferry (coastal ship). • Owned by Norway’s Noried in November 2018.

Note. *Adapted from “Maritime Autonomous Surface Ships: Development Trends and Prospects-how Digitalization Drives Changes in Maritime Industry,” by Mitsui & Co.Global Strategic Studies Institute, 2019.*

The conclusion on crewless and autonomous ships of the MUNIN project is that they can only be used if they are safe and economical (Felski & Zwolak, 2020; Rødseth et al, 2018). Initially, crewless MASS will be used only for transport activity at smaller scale (Szelangiewicz & Żelazny, 2020). With the improvement in the technology and with the development in the legal regulations/reforms, sea going autonomous ships will emerge in fifteen to twenty years (Szelangiewicz & Żelazny, 2020). World leading companies/organizations have assured and planned to bring crewless MASS by 2025 and by 2035 it is expected that fully automated MASS will be functioning in the oceans as shown figure 6 (Emad et al., 2020; UNCTAD, 2018).

Figure 6

Autonomous Ship Future Development Timeline


Remotely operated local vessel
Reduced crew with remote support and operation of certain functions
Remote controlled unmanned coastal vessel
Remote controlled unmanned ocean-going ship
Autonomous unmanned ocean-going ship
2020
2025
2030
2035
Unmanned ships will most likely start with local applications

Note. Adapted from "Shipping 4.0 and training seafarers for the future autonomous and unmanned ships," by Emad, G. R., Khabir, M., & Shahbakhsh, M. 2020, Paper presented at the Proceedings of the 21st Marine Industries Conference (MIC2019), Qeshm Island, Iran, p. 1-2.

1.5 Threats and Challenges - MASS

According to Chang and colleagues, in shipping industry there are numerous reasoning to squeeze MASS (2021). There are however issues with this new technology such as the need to be recognized/adopted by the governments. In addition to this, the outdated maritime industry has numerous valid issues of safety, security and reliability of MASS operations (UNCTAD, 2018). According to Trump, with the technological advancement in the maritime sector, 4.0 ships still lacks in heftiness as well as rigidity against various dangers which includes both cyber and physical attacks (2020).

In addition to this, at sea, hazards, like collision/grounding along with security threats which includes piracy are always present. In this regard, Liwang stated that ship characterize excessive financial and illustrative worth and hence be a target of acts like robbery, piracy activity or terrorist attack (2016). Those who are involved in the maritime sector/transport, security issue is a continuous alarm. Over the years, the maritime stakeholders have strengthened the legal procedures and administrative instruments to uphold the maximum security for ships, people working on ships and the cargo onboard (Herbert-Burns et al, 2019). Nowadays, the biggest challenge for MASS is the threats like terrorist attacks and cyber-pirates. Hence, MASS requires a strong communication system with robust and multiple systems capable of dealing with these threats (Sakhi et al, 2019).

1.6 IMO Regulatory Scoping Exercise (RSE)

Advancement in the field of technology and digitalization, maritime industry is also continuously developing itself and testing these technologies to conduct safe autonomous vessel operations. International Maritime Organization's (IMO) Maritime Safety Committee (MSC) has started a RSE in 2017 with the goal for identifying ways for safe and secure MASS operations. Basically, this exercise includes two steps in which the first step is to determine that MASS is safe and environmentally feasible within current IMO conventions and future/upcoming goals. The second step is to analyse how MASS operations can be addressed keeping in view the human, technology and operational factors (IMO 2018). The first step has been completed by MSC at its 103rd session, as high-priority issues were figured out with extended multiple instruments, and at policy level these are required to be addressed in order to define future work. Further to address MASS in IMO, there is a need to design a goal based instrument related to MASS in a broader way through a regulatory framework (IMO, 2021). Therefore, the development of goal-based instrument work has been commenced after the 105th session of MSC meeting in April 2022. It was decided that, at the very first stage, a non-mandatory code will be developed and may be adopted during the second half of year 2024. After getting experienced in the use of non-mandatory MASS Code, a mandatory MASS Code will be shaped and will enter into force on 1st January 2028 (IMO, 2022).

1.7 Problem Statement

Considering the new advancement in technology especially in the field of shipping, these conventional ships are prone to maritime threats. MASS is an emerging technology, therefore there may be chances that Non-State Actors (NSAs), criminals/ terrorists could use the weakness of autonomous ships to carry out maritime crimes. There is a dire need to review the threats and challenges to MASS which may impact the maritime security. This is especially for threat of piracy in the form of cyber-attack which may lead to any terrorist activity. Hence, it is important to pursue the most appropriate measures to address this threat. In year 2021, maritime and logistics industry came under cyber-attack many times which affected the shipping industry very badly. These attacks targeted the ships with an increased frequency of 33% as compared to 2020 (Cyberstar, 2022). The top eight cyber-attacks of year 2021 which wedged the maritime and logistics industry the most are highlighted in table 3.

Table 2

Cyber-Attack Incidents 2021

S. No	Incidents on Maritime Companies	Date	Remarks
1.	Two Attacks on Japan's "K" line.	Mar 21 Jul 21	• Hackers get into the company's IT network system. • It contain around for ten days. • The system then bring online in steps. • Second attack was of interference called "unauthorized access to overseas subsidiary systems."

2.	Breach on a South Korean Shipping Company HMM.	Jun 21	• Hackers target HMM's email servers. • System remain offline for several days. • Company was able to restore the system and all the functionalities of the email system within days. • However it's not that fast recovery as the company is considered as a well-organized and well reliance company.
3.	Attack on Transnet (Rail and port operator of a major South African logistics).	Jul 21	• Attack happened on a container terminal and many terminals were non-operational for about a week including the main operational systems which was completely disconnected. • In result many vessels neglect to enter port and the terminal was stated force majeure.
4.	Breach in a port of Houston, Taxes, USA.	Aug 21	• Hackers subjugated a weakness in a password manager, in order to crack the port's network system and subsequently get access to other systems also. • IT team immediately sensed the breach and took necessary measures against the breach. • No delicate data was collected with no systems became upset.
5.	CMA CGM, the French container shipping company	Sep 21	• Hackers breached in company's system and get the customer data. • There was only data leakage, no disturbance observed in any main systems of the company. • The leaked data included sensitive information (customer names and contact information).
6.	Breach on a Singapore based shipping company - Pacific Offshore.	Nov 21	• There was an unauthorized access to the IT systems and the breach was limited to the data exposure. • There was a loss of sensitive registered commercial information and is considered a serious breach.

7.	Attack on a consulting firm Danaos Management Consultants.	Nov 21	• Hacker breach the IT network of the multiple shipping companies. • The breach was in the Supply chain. • Many shipping companies do business with the firm. • 10% of the customers were effected in that.
8.	Attack on Hellmann Worldwide Logistics, Germany.	Dec 21	• Consider as a ransom attack which halt only day to day operations. • All the connections of the system were removed from the central data center. • This impact their business operations.

Note. Prepared from "How Bad Was Maritime Cyber Security in 2021? Consider These 8 Incidents," by Cyberstar, 2022, (https://www.zkcyberstar.com/2022/03/15/how-bad-was-maritime-cyber-security-in-2021-consider-these-8-incidents/#:~:text=On%20the%20cyber%20security%20front,and%20port%20systems%20in%202020).

These threats and challenges are being overcome through frequent patrolling, deployments and conduct of maritime actions in different maritime zones by Law Enforcement Agencies LEA's, Navy, Maritime Security Agencies and Coast Guard (CG), plus the Combined Maritime Forces (CTF-151 & CTF-150) and navigational rules mentioned in the UNCLOS Article 11012 (Kraska, 2010). The piracy on any MASS might lead to a terrorist activity. Hence, it is important to determine which actions will be taken to counter that threat considering the state's right to engage based on its sovereign rights over its maritime zones (Klein et al, 2020). There are numerous reasons for which Combined Task Forces (CTF) commenced boarding operations on foreign-flagged vessels under the umbrella of United Nations and same is the case with the LEA's. Port of Los Angeles (PoLA) developed an unmanned autonomous fast boat for the security of the port which is capable of providing information of the target through its sensors above water as well as under water (Galdorisi, 2022). MASS may create practical challenges in the maritime domain for LEA's. In order to maintain/preserve governance out at sea, LEA's are working on behalf of respective coastal states. Thus, the role of LEA's in this regard is considered very important.

1.8 Research Questions

The research questions are as under:

- What are the different security threats and challenges to MASS and its impact on maritime security?
- What is the role of law enforcement agencies in order to address the security threats and challenges related to MASS?

The aim of this research is to highlight the security threats and challenges to MASS which may cause damage to International organizations, ship building companies, ship owners and Port/coastal states in respect of safety, environmental and economic risk. Moreover, if these threats particularly cyber, piracy and terrorism activity will be carried out on MASS/SCC, what will be the consequences and how they can be mitigated. The objectives of the study is to identify different security threats and challenges to MASS and its impacts on maritime security. Moreover, to make out the way forward to deal with these security threats and challenges.

Based on the research questions and keeping in view the aim and objectives the expected outcomes of the research is a better understanding of security threats and challenges to MASS, to establish the role of LEA's at sea, to familiarize states and organizations w.r.t vulnerabilities of MASS, to deal with different security challenges to MASS by the port/ coastal state in future, to develop effective strategies for safe and secure maritime transportation (MASS) and to identify possible implications of MASS for maritime security.

Chapter 2 – Literature Review

2.1 Introduction

The United Nation Convention on the Law of the Sea (UNCLOS), is considered all over the world as the "constitution for the ocean", which institutes a lawful structure that every country party to it must act, but this constitution doesn't define maritime security (Cook, 2020). In this regard, IMO is working hard to present higher safety and security standards in the shipping industry. Maritime safety in this regard, is considered as a major push back for businessmen to finance more in the field of MASS as it is considered as the future and is also reinforced by the transformational technology (Komianos, 2018; Kretschmann et al., 2017). However, to operate MASS as compared to commercial ships, it will be very different because of the risk profiles, responsibilities and accountability (Kim & Mallam, 2020). Keeping in this view, MASS will definitely change the entire operational concepts of shipping with new emerging hazards, risks and security issues. These issues may only be eliminated through new means and measures. It is perceived that MASS may face higher boarding and robbery threat with regards to the physical security (Honekamp, 2018). MASS as a crewless ship, creates a major security gap and requires a risk mitigation strategy. Therefore, in future there will be security teams deployed at pre-defined geographical areas/zones which may inspect and ensure smooth sailing of MASS or entry/leave at ports (Komianos, 2018). Furthermore, there will also be a risk of cyber threat to MASS in that, connectivity and cyber security is identified as the likely gaps by RSE for MASS operations (IMO, 2021b). Hence to enhance the understanding of MASS, the following sections explores advantages and disadvantages of MASS, fundamentals of MASS, introduction to maritime security, threats and challenges to MASS, role of law enforcement and cyber security/physical incident (scenarios) identification.

2.2 Advantages and Dis-advantages of MASS

It is very important to know the advantages and disadvantages of MASS in order to identify gaps and different threats and challenges to MASS. MASS may become a security threat to maritime sector while keeping in view the different dis-advantages of MASS.

2.2.1 **Advantages**. MASS is considered as one of the future step towards sustainability. Therefore many developers are investing in it and this concept is also consider as a potential answer to many shipping issues (de Klerk et al., 2021). Around 75-96% marine incidents occurred at sea are caused by some form of human errors (Rothblum, 2006). MASS will have reduced the number of navigation-related incidents, like collision or grounding, as compared to the conventional ships (Wróbel et al., 2017). Therefore, new technology and automation when applied on MASS degrees 1 and 2 (seafarer onboard) will definitely reduce these human related errors and marine incidents like collision. However, it cannot be applied on MASS degree 3 and 4 (no seafarer onboard) which will be operated from SCC. Therefore, there is a requirement to have that type of technology which is capable of making decisions automatically in order to avoid collision incidents and handle emergency situations (Chae et al., 2020). In situations like COVID-19 pandemic, MASS might reduce the probability of infection. It upsurge the safety of aquatic life and increases fuel efficiency (Innovation, 2020). Moreover, it will also support and reduce tiresome and risky maritime activities at sea (Porathe et al., 2018). In addition, MUNIN forecasted that over a period of 25 years this technology will save over $7m per MASS in terms of consumption of fuel, crew salaries and supplies (Callum, 2018). It has also been learnt that there is a drastic decline in the seafaring profession and people are not very much interested in this profession. There are very selected/limited labour supplying countries which are providing man power for this particular sector (Pribyl & Weigel, 2018). MASS while operating in a High Risk Area (HRA) will definitely reduce the risk of piracy, hostage's situation and cut short the insurance coverage cost (Carey, 2017; Kobyliński, 2018). As per the report of State of Maritime Piracy, total of 18 incidents were reported off the coast of West Africa and 21 incidents in Asia of kidnaping for ransom (EMERJ, 2022). Hull structure (closed structure and streamlined exterior) of MASS also have potential impact on decrease of wind resistance (aerodynamic profile) and prevent/stoppage of piracy for crew and cargo

(Chae et al., 2020). Moreover, deckhouse would no longer be required (no crew and bridge) and provide more space for cargo and easy to load the cargo (EMERJ, 2022).

2.2.2 **Dis-advantages.** There are many risks and uncertainties which may also come along with the benefits of MASS (Komianos, 2018). In case of new technology, safety of navigation of autonomous navigation systems may increase complexities and new hazards and unexpected system interdependencies (Utne et al., 2017; Chae et al., 2020). Initially or at the primary phase of setup of SCC and building MASS, a huge amount is required on capitalizing in the field of technology (Callum, 2018). MASS will be controlled through SCC which is considered as the third dimension for controlling the ship other than ship itself and ports. Handling MASS in harbor will be a challenging task (Pribyl & Weigel, 2018). In this regard, Van Hooydonk (2014) identified different drawbacks of technology while consideting that the shore controllers inside SCC are indulged in handling other ships along with assessing different situations at sea. Due of lack of crew, maintenance of moving parts of MASS will be difficult on long voyages and failures might cause significant delays (Callum, 2018). Cyber security is considered as one of the biggest threat to MASS and is expected to be increased with the increase in the mode/levels of autonomy (Kobyliński, 2018; Tam & Jones, 2018). According to Kobylinski (2018) and Habdank (2019) there is a risk of hacking MASS by the hackers (pirates) and taking complete control of ship. In result, hackers (pirates) will be able to remotely maneuver the ship towards their desired destination and transfer all valuable cargo. Pirates or so-called terrorists now a days may also use that ship as a bargaining chip for their own interest like asking for money or make demands to free their men etc. Furthermore, threaten coastal states by blocking port entrances, grounding, collusion, transport contraband items and carryout any kind of terrorist activity at any military installation/ assets. Table 3 below summarized these advantages and disadvantages.

Table 3

Advantages and Dis-advantages of MASS

S. No	Advantages	Dis-advantages
1.	Curtailed number of navigation-related incidents, like collision or grounding (Wróbel et al., 2017).	Increase complexities, new hazards and unexpected system interdependencies (Utne et al., 2017).
2.	Reduction in human related errors therefore bringing down costs related to accidents and insurance (Chae et al., 2020).	Handling MASS in harbor will be a challenging task (Pribyl & Weigel, 2018).
3.	Reduce tiresome and risky maritime activities at sea (Porathe et al., 2018).	Shore operators inside SCC are indulge in handling other ships along with assessing different situations at sea (Van Hooydonk, 2014).
4.	Reduces the manning cost (Pribyl & Weigel, 2018).	Cyber security one of the biggest threat to MASS and is expected to be increased with the increase in the levels of autonomy (Kobyliński, 2018; Tam & Jones, 2018).
5.	Increase safety of life (Pribyl & Weigel, 2018).	Cyber-pirates may hack MASS and took complete control of ship (Kobylinski, 2018 & Habdank, 2019).
6.	Cut short the insurance coverage cost (Carey, 2017; Kobyliński, 2018).	Maintenance of moving parts will be difficult on long voyages which cause significant delay (Callum, 2018).
7.	Capable of operating in a High Risk Area (HRA) will definitely reduce the risk of piracy and hostage's situation (Carey, 2017; Kobyliński, 2018).	Initially huge amount of investment on both SCC & MASS is required for the development of the technology (Callum, 2018).
8.	Hull structure of MASS have the potential impact in reduction of wind resistance and prevention of piracy for crew and cargo (Chae et al., 2020).	
9.	Environmental free operations/ voyages.	

10.	Situation like COVID-19, MASS diminishing the likelihood of infection (Innovation, 2020).	
11.	Upsurges the safety of aquatic life (Innovation, 2020).	
12.	Increases fuel efficiency (Callum, 2018).	

2.3 Background - Maritime Security

To make the maritime industry stronger, it is important to look into the matters related to maritime security. Considering the above mentioned threats to MASS, they may have direct influence, visible implications and effect on maritime sector. Since the start of 1990s, maritime security is considered as an important aspect and remain focus amongst many significant global security players (Bueger & Edmunds, 2017). Coastal states face many challenges like piracy activities, drug/human trafficking and environmental crimes. These are not considered as threat to a particular state but to the worldwide trade and energy security (Bueger et al., 2020). Presently, states' emphasis and the point of discussion at different levels is piracy, terrorism, arm/human trafficking and illicit activities at sea (Bueger et al., 2020). The level of maritime security differs from one area to another. However, it is relatively easy for the developed countries to implement global measures with an effective maritime administration. Most of the developing countries face issues/problems related to physical security of the ships, port and surrounding areas of their coast because of lack of resources and funds (Herbert-Burns et al., 2019). Considering all these ongoing challenges, the advent of MASS technology in maritime sector will become a new challenge for the maritime nations and will also raise question related to existing ocean governance structure (Klein, 2019).

2.4 Define - Maritime Security

As the research is basically focused on threats and challenges to MASS in maritime domain, it is important to discuss maritime security in detail as the above mentioned threats are very relevant to MASS as well. In that cyber threat is now become more prominent threat to MASS. There are many definitions, meanings and understandings of world "*Security*" and "*Maritime Security*". According to Andritsos:

> *"It refers to set of actions or means for ensuring safety specifically against the international threats. It also comprises of all the systems, measures or actions that have the aim to present such threats so that they do not compromise the security"* (Andritsos, 2013).

> *"Maritime security also refers to different preventive measures which have the purpose of protecting the port and shipping from the threats of unlawful acts which are intentional"* (Andritsos, 2013).

It is mentioned earlier that the word security and maritime security have different connotations for different actors like military and shipping industry (Natalie Klein, 2011).

According to military point of view, US Navy operational concept explains that:

> *"It refers to ensuring of smooth flow of commerce, freedom to navigate and to protect the different resources of ocean. It also focuses on ensuring that the maritime domain is secured from different threats at national and international levels such as drug trafficking, environmental destruction or illegal immigration through sea"* (Klein, 2011, p.8).

Ship owners on the other hand explain that:

> "*It is considered as a system of transportation along with relating to the safe logistics of cargo without being subject to any form of criminal activity*" (Klein, 2011).

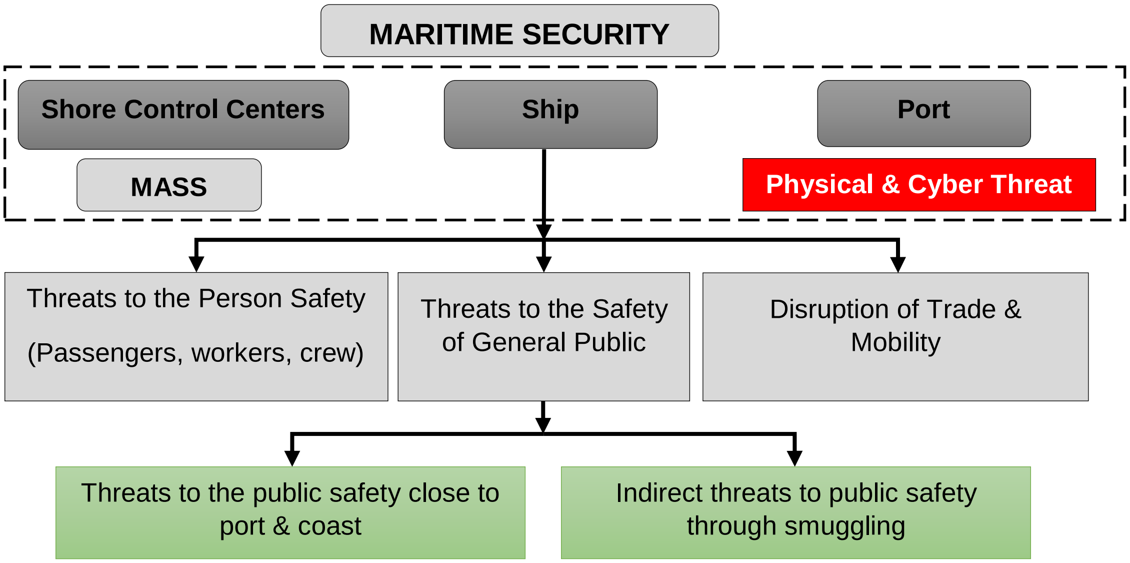
Jones (2006) describes ship owner's point of view and acknowledges the idea of maritime security as:

> "*It is regarded as the state of vessel/port/crew in terms of being secured as well as the safety from different threats such as piracy and terrorism*."

Keeping in view all the concepts and definitions of maritime security, it can be said that there is no fixed definition for it and it is an eye catching word which mostly draw attention to upcoming threats and make provision for rule to address them. According to Bueger (2015), maritime security is aiming towards 'threats' which prevails in the maritime domain. In the new era of technology and digitalization, revolution in form of automation and digitalization in the field of maritime industry has also evolved. MASS is considered as an important revolution which is risk free and purely environment friendly (Emad et al., 2020; Sakhi et al., 2019). It is considered that in future for sustainable shipping, MASS is the future of shipping. The future is of technology and with the integration of Information Technology (IT) and Operations Technology (OP), all the systems will combine into one called Cyber Physical Systems (CPS). Through this one can operate and maneuver the ship safely in future (Kavallieratos et al., 2020). MASS in future will be controlled from shore based center called SCC as these ships will be crewless. Therefore, MASS along with SCC and the present transport system (ships and ports) are considered as the main actors which form a new structure for maritime security as shown in figure 7.

Figure 7

Block diagram of Maritime Security in the framework of MASS


MARITIME SECURITY
Shore Control Centers
Ship
Port
MASS
Physical & Cyber Threat
Threats to the Person Safety
(Passengers, workers, crew)
Threats to the Safety of General Public
Disruption of Trade & Mobility
Threats to the public safety close to port & coast
Indirect threats to public safety through smuggling

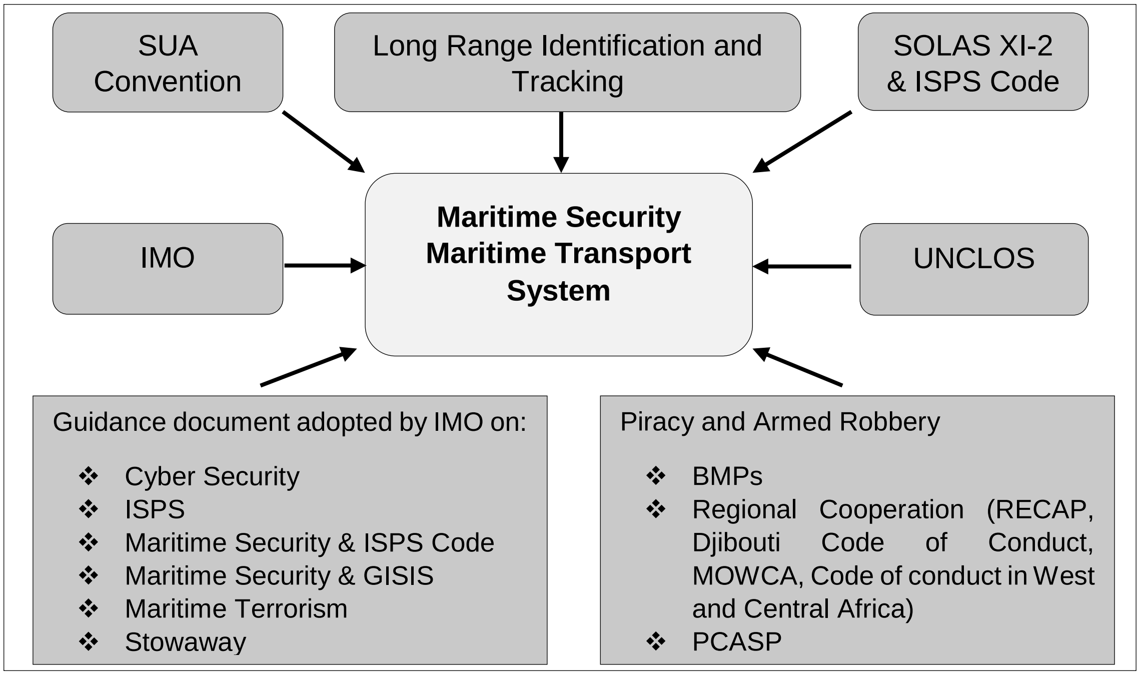
Note. Adapted from "EU port security & growth," by Andritsos, F. 2013, Paper presented at the proceedings of the 8th Future Security Research Conference, p. 267-274.

2.5 Instruments for Maritime Security

Accidents related to maritime happened in the past, they happen today and will also continue in future. Due to these accidents, the important elements which are most effected are men's life, material loss and environment. Once an accident occurs, the worldwide communal attempts to make some more stringent rules and do legislation changes or somewhat adopt new rules. In case of any security incident happened, it aided and became as a grounding in the maritime industry for developing any security instruments. The current security measures of maritime sector are offered at the international, regional, and national levels (Herbert-Burns et al., 2019; Metaparti, 2010). The most important IMO instruments (figure 8) related to maritime security are explained in the following paragraphs.

Figure 8

Maritime Security - IMO and global measures


SUA Convention
Long Range Identification and Tracking
SOLAS XI-2 & ISPS Code
IMO
Maritime Security Maritime Transport System
UNCLOS
Guidance document adopted by IMO on:
❖ Cyber Security
❖ ISPS
❖ Maritime Security & ISPS Code
❖ Maritime Security & GISIS
❖ Maritime Terrorism
❖ Stowaway
Piracy and Armed Robbery
❖ BMPs
❖ Regional Cooperation (RECAP, Djibouti Code of Conduct, MOWCA, Code of conduct in West and Central Africa)
❖ PCASP

Note. Prepared from "The International Ship and Port Facility (ISPS) Code," by International Maritime Organization 2021a, (https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx).

2.5.1 Suppression of Unlawful Acts (SUA) Convention 1988 and 2005 SUA Protocol

IMO passed one resolution A.584(14)17 trailed by circular number MSC/Circ.44318 in reaction to hijacking of an Italian cruise ship, Achille Lauro in 1985. A resolution 40/61 was then adopted by UNGA to “eliminate the issue of international terrorism by taking quick and necessary actions at the national level, like synchronization of domestic legislation with present international conventions and execution of presumed international obligations”. IMO adopted the convention called Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) in 1988 and was later revised in 2005 and finally implemented in form of Protocols to the SUA treaties called as 2005 protocols (Attard, 2014; Cook, 2020).

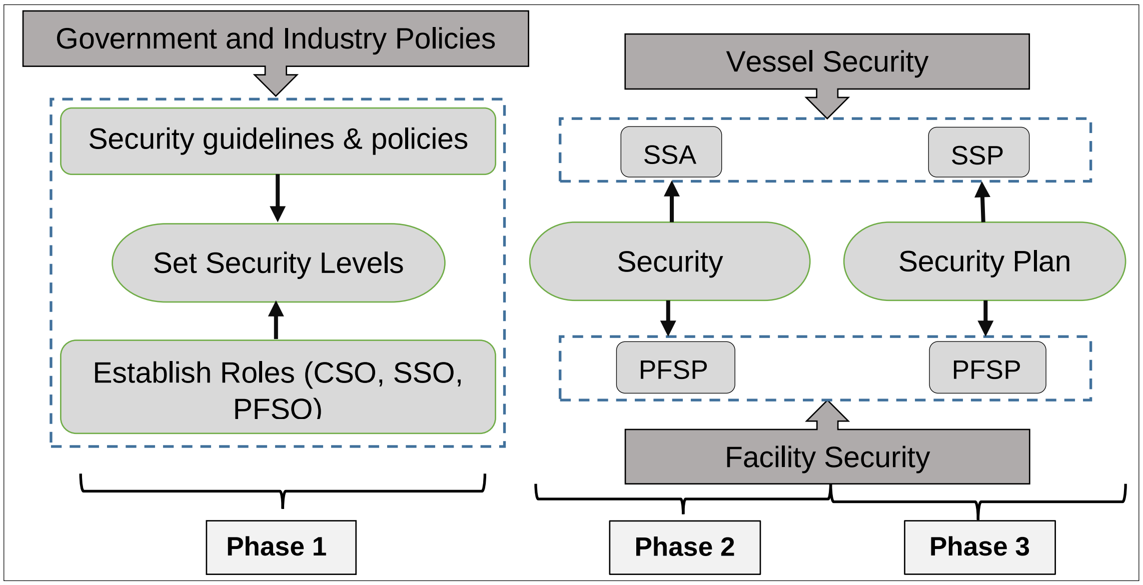
2.5.2 International Ship and Port Facility Security (ISPS) Code

In United States (US), 9/11 terrorist activity occurred which triggered a significant change related to security and encouraged controlling authorities to examine shipping in detail. Hence, International Ship and Port Facility Security (ISPS) Code was recommended and accepted in 2004. The main aim of this code was to protect shipping from terrorists which may be used as weapons for mass distruction (Metaparti, 2010). In order to augment maritime security, a new maritime security system was integrated in Safety of Life at Sea (SOLAS), chapter XI-2 on special methods, including the ISPS code. Mandatory part is “Part A”, whereas guidelines are in “Part B”. The regulation in this chapter says that ship security alert system must be installed on all sea going ships (Komianos, 2018).

The main and important objective of this code is to ascertain security threats and to adopt and enforce them and further make it mandatory for all the stake holders at a national and international level (Dalaklis, 2017). Therefore, to accomplish these objective, there must be a Company Security Officer (CSO) along with Ship Security Officer (SSO) onboard nominated by the ship operator. Furthermore, a ship must have a Ship Security Plan and after having Ship Security Assessments (SSAs) it must get an International Ship Security Certificate (ISSC) as well. This procedure is also required from ports to be complied. There are three phases for application of the ISPS code as shown in figure 9 (Komianos, 2018; Progoulakis & Nikitakos, 2019).

Figure 9

ISPS Code Process Phase



Note. Prepared from "Risk Assessment Framework for the Security of Offshore Oil and Gas Assets," by Progoulakis, I. & Nikitakos, N. 2019, IAME 2019 conference.

According to many researchers it is recommended that, it is hard to apply the present regulations related to security measures present in ISPS code on MASS, therefore it must be amended to take into consideration the crewless autonomous ships (Dalaklis, 2017; Kim & Yang, 2019). As MASS will be crewless, there will be no security officer present onboard which is considered as a challenge for technical, institutional and international organs and requires greater consideration to strengthen the security system onboard such as vessels (Komianos, 2018). For this reason, there is a RSE being conducted at IMO which concludes that all the high priority IMO instruments including SOLAS Chapter XI-2 will be addressed on priority basis (IMO, 2021a). ISPS code defines security occurrences, which mostly link to the ships. The ship's security valuation would eventually calculate all probable threats, allowing to part "B" of ISPS code. The different security incidents are shown in table 4 (IMO, 2021a).

Table 4

List of Security Incidents

S. No	Security Incidents
1.	Damage to, or destruction of, the ship or of a port facility
2.	Hijacking or seizure of the ship or persons on board
3.	Tampering with cargo, essential ship equipment or system or ship stores
4.	Unauthorized access or use, including presence of stowaways
5.	Smuggling weapons or equipment, including weapons of mass destruction
6.	Use of ship to carry those intending to cause a security incidents
7.	Use of ship itself as a weapon or as a means to cause damage to destruction
8.	Attacks from seawards whilst at berth or at anchor
9.	Attacks while at sea

Note. Prepared from "The International Ship and Port Facility (ISPS) Code," by International Maritime Organization 2021a, (https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx).

2.6 Maritime Security in non-IMO Treaties

On 10 December 1982, the 3rd UN conference on law of the sea was held in Montego Bay, Jamaica which was basically based on maritime security counting the desecration of territorial rights and piracy. In that, UNCLOS classified three significant navigational rules which include "innocent passage applies in the territorial and archipelagic waters, transit passage applies to straits used for international navigation, and archipelagic sea lanes passage applies to archipelagic waters". For economic and security reasons, each of these rules attempts to pursuit a balance between two opposing benefits of a coastal states, the second is the interest of states who struggle to keep freedom of navigation and over flight. Part VII of UNCLOS particularly article 8820, encompasses active requirements related to maritime security. For every maritime nation, maritime security is considered as common concern. Furthermore, article 100 of UNCLOS provides the provisioning to fight with piracy, and allow cooperation among states to clash with piracy activity at high seas or outside the jurisdiction of any particular state (Attard, 2014). In this regard, questions have been raised by Osinuga (2020) that cyber-pirates may target MASS who are probably operating and are present on land and therefore may not be reflected as pirates in a traditional way. He suggested that UNCLOS may be re-looked in a manner that to cover, integrate and engage the piracy aspect in respect of cyber pirates.

2.7 Threats and Challenges to MASS and SCC (Security Scenarios)

In future, MASS will likely alter the configuration, shape, and ways and means of pirates, terrorist and criminal activities. With crewless vessels, keeping in mind the levels of autonomy the number of hostage situations will likely reduce to minimum. However, no person onboard may cause and increase in number of attempts to seize that ship for valuable cargo.

Keeping in view all the traditional security threats to the conventional shipping, with the advent of MASS there will be new emerging threat of cyber threat. MASS at sea and SCCs on land are vulnerable to cyber-attacks. Once MASS will be in the hands of cyber-pirates, there may be various scenarios related to security incidents. Researcher deliberate that once cyber and physical attack on SCCs/MASS happened, the expected results/outcome are shown in table 5. In subsequent sections, a complete evaluation has been carried out on Cyber Security threat in the background of MASS.

Table 5

Expected Situations – Cyber Attack

S. No	Expected Situations after MASS and SCC will be Hijacked
1.	Diversion to-wards vital military installation/ warships in the ports (Kobylinski, 2018)
2.	Collision with vital cargo vessel (Habdank, 2019)
3.	Grounding and blocking the channels (Chae et al., 2020)
4.	Collision with oil tankers for environmental pollution (Chae et al., 2020)
5.	Conduct of terrorist activity by exploding MASS in other's country ports (Kobylinski, 2018)
6.	Blocking the world trade routes (SLOCS) by grounding and collusions (Chae et al., 2020)
7.	Use MASS as a bargaining chip to make deals to make their men free

8.	Make demands for money from shipping companies/ owners
9.	Make SCC personal hostage and ask government to fulfill their demands
10.	MASS itself use as a weapon of mass distraction

2.7.1 **Cyber-Security Threats**

With the advancement in the field of technology and development of autonomy levels in MASS, cyber security has become threat to MASS and is also being the most frequently asked question. It is a type of soft threat which is in hidden form (virus) where the hackers are able to attain, access and get control of MASS system and change its operation according to hackers' objectives. This may cause severe consequences for maritime transport industry. In recent past, IMO has addressed this cyber security problem and issued guidelines on how to manage cyber risk (IMO, 2017b). The guidelines help in managing to protect ships from present developing threats. The systems which are exposed to this threat and are highlighted in the guideline are shown in the table 6:

Table 6

Systems Exposed to Cyber Threat

S. No	Systems
1.	Bridge Systems
2.	Cargo handling and management Systems
3.	Machinery and propulsion Systems
4.	Control Systems
5.	Passenger service and management Systems
6.	Passenger public network
7.	Crew Welfare Systems
8.	Communication Systems

Note. Prepared from "Maritime Cyber Risk Management in Safety Management Systems Resolution MSC. 428 (98)," by International Maritime Organization (IMO), Maritime Safety Committee, 2017c.

2.7.2 Physical Threat to SCC - Connectivity between MASS and SCC

In order to operate, MASS connectivity between SCC and MASS is essential and can be called shore to ship connection. For that there must be a strong link of wire-less communication either through satellite or UHF/VHF/HF transmissions. These communication links may be compromised which are used to maneuver and control MASS from far distances through cyber-attacks (Tam & Jones, 2018). According to RSE, cyber-security is also considered as a potential gap in MASS operations (IMO, 2021b). Honekamp explains that communication and IT systems of MASS are the two main security issues which need to be addressed and controlled, considering the cyber-attack as a source of great concern (2018).

A study was conducted on use of robotics and AI by Kunz and Ó hÉigeartaigh, which concluded that these things would affect the world safety and security sectors of aviation, shipping, transportation and automobiles (2020). It further explains that development in the field of MASS will be the most robot related threat to the world. It may be in the shape of transport of terrorists, drone carrying explosives, biological, chemical and radio-active materials. The cyber-attack would not only affect MASS but also SCC infrastructure. SCC play a significant role for MASS and is considered as the hub of operation (Rylander & Man, 2016). For navigators these centers will have contemporary virtual bridge and machinery control rooms and these cyber-physical ships will be operated by the virtual captains/ engineers. The only requirement to operate MASS is of a secure and reliable connectivity and setup (Kutsuna et al., 2019). SCCs will be installed with safe and secure communication system through terrestrial and satellite, strong unbreakable link between sea/land-based actors, sensor related to weather and sea, and presence of human to act as operator (Wróbel et al., 2020). In RSE's conclusion, gaps related to SCC has given high priority against many IMO instruments. However, Chapter XI-2 to SOLAS has not included and considered them as probable gaps for SCC (IMO, 2021b). SCC at one time can handle several MASS at a time. Therefore, cyber-pirates or criminals may attack on SCC-MASS communication or SCC itself to meet their agendas.

2.8 Cyber-Security Incidents in Maritime Industry and Other Industries

There was a cyber-attack; called NotPetya which occurred in June 2017; on Maersk's system the world's largest transport of seaborne freight. Global trade of 15 per cent is transported through containers of this company. After the cyber-attack occurred, the container ships of Maersk's mounted motionless at sea and 76 port terminals around the globe went on halt, port terminals working stopped. The retrieval of the entire system was fast, however in that brief recovery period the organization suffered $300m losses (Safety, 2018). Similarly, in year 2022, there was another cyber-attack on JNCPT container terminal in Mumbai in that hacker distract the container ship to other terminal at the Jawaharlal Nehru Port using port Management Information System (MIS) near Mumbai (Cyberstar, 2022).

Considering the above situations, the revealing gaps in MASS systems may also become a favorable zone for cyber-attacks. Similarly, there are chances of cyber threat when MASS is remotely operated and managed. If compared with driverless cars and computer system controlled oil pipe lines, the consequences/impact of cyber-attacks directing at MASS will be far more devastating and dangerous. Similarly, hacking of the one of the giant maritime company of the world came under cyber-attack and its ship's and operations in port were halted which resulted in financial loss and diversion of container ship in port of Mumbai from one terminal to another is a fruit for thought. Consider an unmanned oil tanker hijacked by a non-state actors group/terrorist which may be used to attack the buzziest port of a country.

2.9 Define – Cyber Risk

IMO defined Cyber risk as:

"*Measuring the level of threat faced by a technological asset by any potential situation that might lead to operational or safety/security related failures. This will be due to the system or information being compromised, lost or corrupted*" (IMO, 2017a).

2.10 Communication System and Cyber Security of MASS

Safe, secure and proficient operations of MASS through wireless communication systems is very crucial. Therefore, it is very essential to have a smooth and error free communication link between MASS and SCC. The required communication system for MASS are mentioned in the table 7. These communication needs to be bi-directional, strongly encrypted, correct and sustained by various systems, without producing any redundancy and diminishing the risk factor (Laurinen, 2016).

Table 7

Communication Systems used for MASS

S. No	Communication Systems	Usage
1.	Navigation Systems	Related to positioning and route-setting
2.	Marine Satellite System	For information related to navigation and safety between ships at sea and infrastructure onshore (e.g. SCC, Ports).
3.	Data Communication Stems	
4.	Remote monitoring and control Systems	
5.	Satellite Communication System	
6.	Terrestrial Communication System	

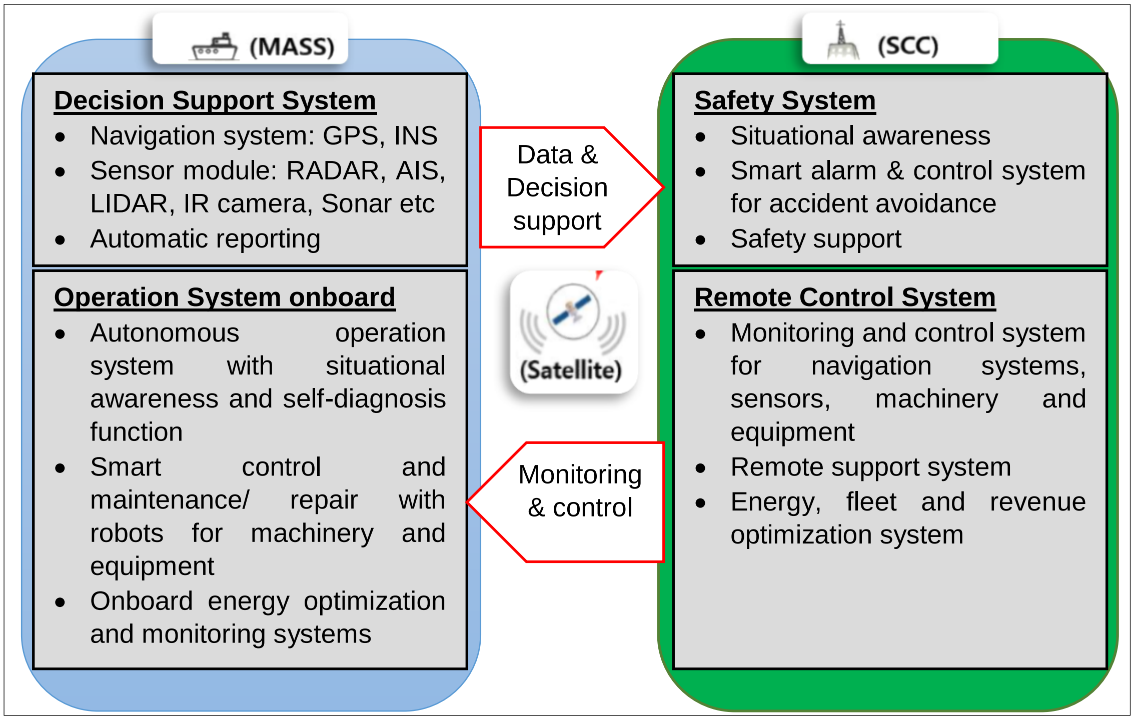
Note. Prepared from "The Next Steps; AAWA: Advanced Autonomous Waterborne Applications," by Laurinen, M, 2016, Remote and Autonomous Ships London, UK.

The above communication systems must be reliable, provide better performances and must be secured and capable of dealing with cyber-attacks. In addition, issues related to satellite or terrestrial communication systems need to be improved and tackled in such a way that the system performance, cyber-security and system reliability must not be compromised. MASS likely requires different types of sensors and systems like Light Detection and Ranging (LIDAR), Radio Direction and Ranging (RADAR) , Global Positioning System (GPS), Inertial Navigation System (INS), Global Maritime Distress and Safety System (GDMSS), High Definition (HD) video, optical and Infra-Red (IR) cameras, Electronic Chart Display and Information System (ECDIS), Automatic Identification System (AIS), microphones, wind and pressure sensors. All above sensors and systems will be controlled through SCC from shore and requires transmission of data (both ways) to regulate MASS systems/functions and to make real-time decisions (Seif et al, 2016).

In emergency situation, MASS should be remotely controlled from SCC through the operator. All the important information/communication is done through satellite in a short span of time. Therefore, high data transmission rate is required, including the data reliability, smooth real-time communication, true authentication of the data transfer, toughness, and security aspect must be the prime concern for effective communication between MASS and SCC. Vis-à-vis cyber-security, if a cyber-attack occurs on MASS main control system, it may become reason for causing an incident like grounding, collision, and stationary at sea and environmental pollution (Chae et al, 2020). Figure 10 shows relationship between systems of MASS and SCC through satellite.

Figure 10

Relationship b/w MASS and SCC


(MASS)
Decision Support System
Navigation system: GPS, INS
Sensor module: RADAR, AIS, LIDAR, IR camera, Sonar etc
Automatic reporting
Operation System onboard
Autonomous operation system with situational awareness and self-diagnosis function
Smart control and maintenance/ repair with robots for machinery and equipment
Onboard energy optimization and monitoring systems
Data & Decision support
(Satellite)
Monitoring & control
(SCC)
Safety System
Situational awareness
Smart alarm & control system for accident avoidance
Safety support
Remote Control System
Monitoring and control system for navigation systems, sensors, machinery and equipment
Remote support system
Energy, fleet and revenue optimization system

Note. *Adapted from "A Study on Identification of Development Status of MASS Technologies and Directions* *of Improvement," by Chae, C.-J., Kim, M., & Kim, H.-J. 2020, Applied Sciences, p.10(13), 4564, (https://doi.org/10.3390/app10134564).*

2.11 Law Enforcement at Sea

To maintain maritime security and law and order situation; out at sea within the jurisdiction of any coast state; Maritime law enforcement is very important. Every coastal state has its own maritime strategy to deal with maritime security. This strategy is derived from government level and implemented at local level. LEA's are the one who are responsible to enforce government orders and at the same time prevent and suppress all illegal activities out at sea. In that operations conducted are surveillance through air, boarding operations, detail inspections, through search, persons arrest, seizure of vessels, after detention of a ship imposition of sanctions (Galani & Evans, 2020). The real gloom of MASS is an actual apprehension to the experts of maritime security. The law enforcement community reflects that for criminals, MASS may become a strength or a threat route to evade their detection of misusing this technology (Allen, 2018).

At high seas, article 110 of UNCLOS administer the Visit Board Search Seizure (VBSS) operations which states that if there are realistic evidence of a vessel indulge in piracy activity or any type of slavery trade and without nationality. As per the article 110(3) the LEA's may "send a boat lead by an officer towards the doubted vessel" and this boarding team can inspect and check the ships documents and if required may also conduct the physical search in case of any doubt (Guilfoyle, 2017; Klein, 2019). Klein (2019) judgmentally debates the case of doubtful MASS, where the condition to define the MASS is a "ship" which is owned by a flag state and, if this is the case, that State's approval must be required for conduct of likely boarding operation. However, she contemplates it to be challenging (Klein, 2019). Furthermore, states who ratified UNCLOS are to cooperate with each other in order to overwhelm unlawful traffic involved in narcotic, drugs and substances like psychotropic in the high seas. Drug convention of 1988 explained this cooperation for the purposes of law enforcement. As per the article 17 of drug convention, those vessels which are involved in any type of illicit trafficking the right of visit be implemented by law enforcers on that particular vessel (Klein, 2019).

2.12 **Literature Review Summary**

As MASS is the future of maritime sector, it is concluded that MASS has many advantages like free of human error, better navigation safety, environment friendly, capable of operating in a High Risk Area (HRA) with less risk of piracy and hostage's situation, reduce tiresome and risky maritime activities and fuel efficient. However, from among the various disadvantages, cyber security and physical attack is the main threat to MASS and SCC. Moreover, MASS along with SCC will form a new structure for maritime security in that MASS at sea and SCCs on land both are considered as vulnerable to cyber-attacks. Furthermore, it is also established that, if the cyber-pirates attacked MASS and SCC, there will be precarious outcome and depraved situations for any flag/coastal state in general and LEA's in particular and is considered to be unsafe for the future of maritime industry. It can be determined that connectivity and cyber security threat have a great effect on MASS which may lead to many dangerous situations and may also cause implications on maritime security and increase the role of LEA's. However, precise statements cannot be accumulated since in the maritime field there is no historical or accidental data available in the past. Therefore, researcher in next chapter deliberate upon the methodology the impacts of MASS which is under Cyber-attack on this aspect which is then analyzed in chapter 4.

Chapter 3 – Methodology

3.1 Introduction

In this chapter, researcher gives a framework of working methodology of the research. In the following sections researcher tried to provide and explain in detail about the methodology being used, the reasons for its selection, research approach being followed, the entire process, data collection methods, ethical issues being faced, validity/ reliability and limitations faced.

3.2 Structure of the Study

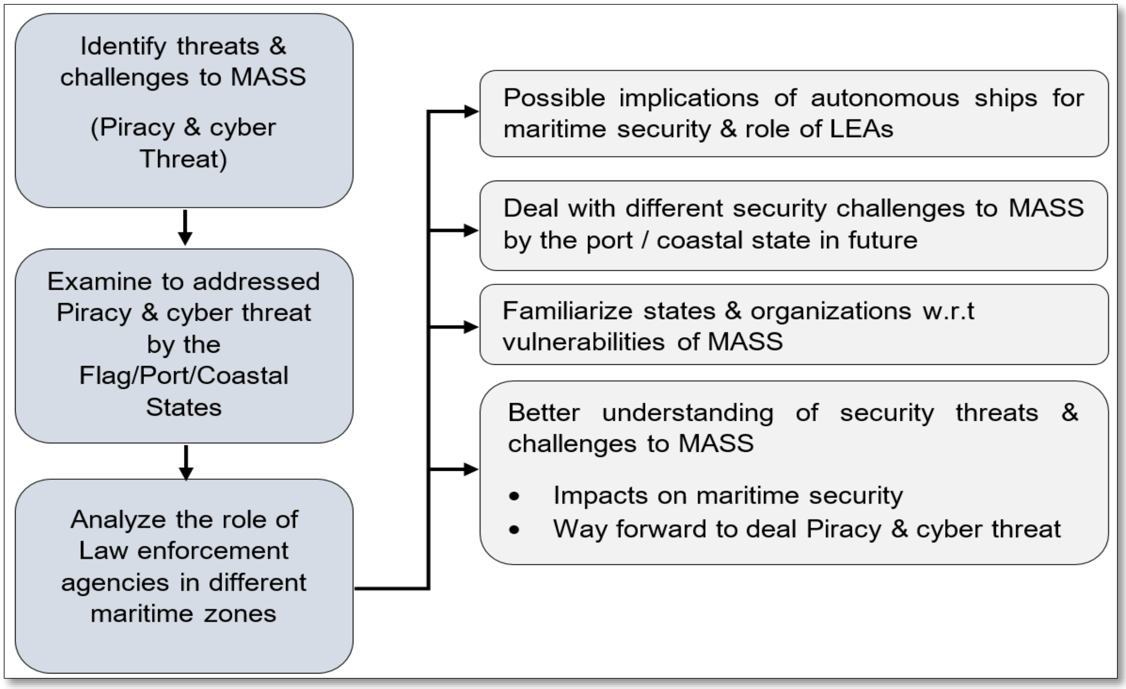
This dissertation is divided into five different chapters where chapter one provides the introduction to MASS, problem statement, aim, objectives, research questions, the expected outcome and limitations faced during the research. Chapter two covers the literature review focused on threats and challenges being faced to MASS and options to address/cater these threats and the role of LEA's. Chapter three covers the methodology and briefly explains the approach, the questionnaires survey along with the given scenario. Chapter four covers the findings and analyses of the scenario related to piracy threat in form of cyber threat. In chapter five there will be the conclusion and recommendations.

3.3 Research Methodology

This research is related to the MASS and what are the different types of threats and challenges faced by the MASS. As there is no historical data available w.r.t the incident happened in the history, therefore the plan is to answer the already structured research question through hypothetical scenarios. In response to the research questions, quantitative approach will be used in which inputs from experts through surveys will be used in addition to review of available research material. Figure 11 shows the procedure being followed for the research to get the expected outcome:

Figure 11

Process of Research Methodology (Author)


Identify threats & challenges to MASS
(Piracy & cyber Threat)
Examine to addressed Piracy & cyber threat by the Flag/Port/Coastal States
Analyze the role of Law enforcement agencies in different maritime zones
Possible implications of autonomous ships for maritime security & role of LEAs
Deal with different security challenges to MASS by the port / coastal state in future
Familiarize states & organizations w.r.t vulnerabilities of MASS
Better understanding of security threats & challenges to MASS
• Impacts on maritime security
• Way forward to deal Piracy & cyber threat

3.3.1 **Explanation**

Research is basically a complex activity to be carried out. It includes various methods in order to achieve the aim and objectives of a particular research (Verschuren et al., 2010). In this research a quantitative approach is chosen, mentioning the uniqueness of the research about threats and challenges to MASS and role of LEA's. The researcher practically used open-ended (quantitative) data collection method (Creswell, 2021).

3.3.2 **Reasoning**

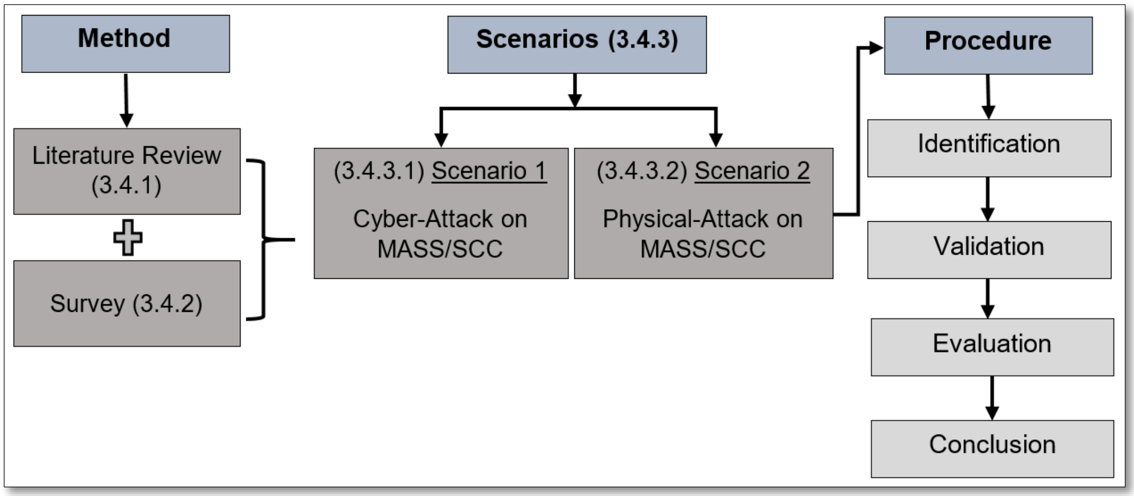
The choice of using and putting on the best techniques, irrespective of their standards, in more multifarious conditions is a foremost advantage of a particular approach. Particular research topics permit examination/exploration by numerous techniques extent through various models. Therefore, the selected approach are the one which probably provide and gives such liberty and flexibility (Kumar, 2018). The technology in the field of automation especially in maritime sector is evolving rapidly. Its effects/impacts on various maritime disciplines are on a very early stages and is very difficult to envisage.

3.3.3 **Approach**

The researcher has formulated two security scenarios related to MASS after going through the literature review and validated/analyzed through surveys. It in opinioned that survey is the option to get information from experts and relevant persons in the form of anonymity in a very quick manner and without any expense. Moreover, because of the non-availability of historical data on MASS (incidents) the formulation of two scenarios and authentication are considered as a suitable tool for establishing the basis of threats and challenges to MASS and role of LEA's. Figure 12 explains the process of the research by using two different scenarios creating methods that might be quantitative, qualitative, or mixed approach (Star et al., 2016).

Figure 12

Research Process Methodology



3.4 Research Process

3.4.1 Literature Review

Aim and objective of the literature review is to explore, discovery and identify the threats and challenges to MASS and analyze the role of LEAS's. Moreover to analyze and examine the data gathered from the reviewed literature. The literature review identifies certain weaknesses related to threats and challenges to MASS (maritime security) and role of LEA's. Security threats like cyber and physical attack are noticed in the form of scenario and tested to address research objectives.

3.4.2 Survey - Questionnaire Form and Data Collection

Data collection through questionnaire surveys began on 26 July 2022 and was completed on 10 Aug 2022. The questionnaire survey form has been formulated on the basis of security threats (cyber and piracy) to achieve research objectives. The survey form purpose is to make best use of the involvement of all maritime stakeholders. There are two parts of the questionnaire. In section II, questions are made after the detail literature review (Chapter 2) keeping in view the gaps while section-I contains total of seven questions focused on the personal information of the participants. Moreover, Section-II contains Twenty Three questions, including five questions fixated on responders understanding with the MASS's concept, maritime security, threats and challenges to MASS and role of law enforcement, was acquired. Following questions collected views/thoughts on cyber-attack and piracy attack and role of law enforcement agencies linking MASS. The questionnaire survey template is placed in Appendix A.

To best capture the varied point of view of the participants, the replies were assessed on a likert scale in a multiple-choice question format. For Section-I percentage format was used starting form 0% to 100% for familiarization with MASS. Responses in Section-II were scaled as 'Strongly disagree,' 'Disagree,' 'Neutral,' 'Agree,' and 'Strongly agree'. Google form was used for electronic data gathering for participants ease. After gathering the data from different maritime departments and experts, the data was analyzed through SPSS (data analysis software). The survey questionnaire was also forwarded to different LEA's. The consent form obtained from participants is at Appendix B. Results of the survey are at Appendix E.

3.4.3 **Scenario Validation**

At present, time is categorized by improbability, revolution, and disorder change. This stresses scenario upon planning techniques for their acknowledged efficacy, uncertainty and compound situations. Scenario planning provokes reasoning, arguments, planning and overwhelms the thinking process by creating multiple futures. In order to overcome and to prepare of any upcoming eventuality by the organizations and companies, scenarios are reflected as the best tool (Amer et al., 2013). It is also used for the development of future strategies and problem solving. Further, it critically observes, identify and examines what is likely to happen in future with several conclusions (Kim, Y. & Cha, 2012). The study utilized the scenarios related to threats to MASS by examining/authenticating selected cyber security and piracy (physical) attacks/incidents. Small description of the two formulated scenarios are explained in ensuring paragraphs. Two hypothetical scenarios are at Appendix C.

3.4.3.1 **Scenario-I (Cyber Attack)**

In this scenario, it is envisaged that MASS/SCC came under cyber-attack by cyber pirates/hackers. The cyber pirates take control of the MASS at sea and able to direct MASS in any direction they desire. There are few situations highlighted in the scenarios which may happen if MASS went under control of the cyber pirates. The questions asked are what happens if that situations occurs and what will be the role of LEA's.

3.4.3.2 **Scenario-II (Physical Attack)**

In this situation, it is envisaged that SCC which is on land came under physical attack and a NSA group take control of the SCC and made the workers hostage. This group made it possible and utilize the same workers to maneuver the MASS in the direction where they desire. There are few situations highlighted in the scenario which may happen after SCC went under physical control of the NSA group and what will be the role of LEA's.

3.5 Ethical Issues

This study demanded the presence of a human element. Keeping in mind the concerns of 'ethical issues' throughout the researcher data collecting process. The survey questionnaire had to be approved after a detailed valuation to certify that it fulfil the utmost ethical standards. Before any act concerning human action/involvement was undertaken, the WMU Ethics Committee assessed all the sections of the survey questionnaire. In addition, the participant's rights and privacy will be preserved. Moreover, factors like confidentiality, secrecy, data security, and the flexibility to withdraw from participation by the participants were closely followed. Furthermore, participation is on voluntary basis, there will be no fee to be charged. There will be no addition or deletion of data once it will be submitted by the participants. The entire data will be kept under secured password and after final submission of the research the entire data will be deleted. WMU Research Ethnic Committee protocol is at Appendix D.

3.6 Brief Summary of the Chapter

To achieve the research objectives of the research, this chapter delivers a synopsis of the research methodology being used. To study the research questions researcher involved and used a quantitative approach. The process includes the making of security scenarios related to cyber and piracy threat based on literature review, which was followed by authentication of scenarios through survey questionnaire to learn the threats and challenges to MASS and role of LEA's.

Chapter 4 – Analysis

4.1 Introduction

In this chapter, statistical findings are presented of data gathered using survey and the analyses of the research questions.

4.2 Survey Questionnaire

The survey commenced on 26th of July and was completed on 10th of Aug 22. A total of 61 respondents participated in the survey out of which 56 were male (91.8%) and 5 were female (8.2%) (Figure 13) from 16 different countries of the world (figure 14). The respondents belong to different parts of the maritime sector (8 from maritime administration, 7 were maritime experts, 3 belonged to maritime academia, 6 were seafarers and 3 form other professions) including the representatives of LEA's (34 from Navy/Coast Guard/MSA) as shown in figure 15.

Figure 13

Gender of Participants

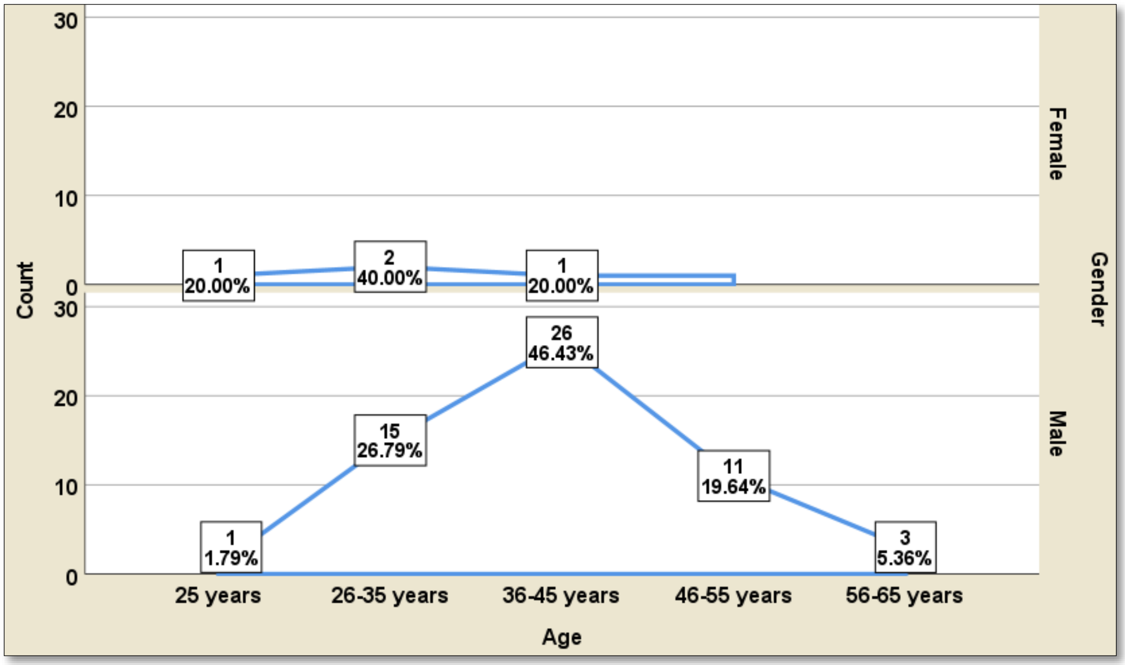


Figure 14

Participants Nationality

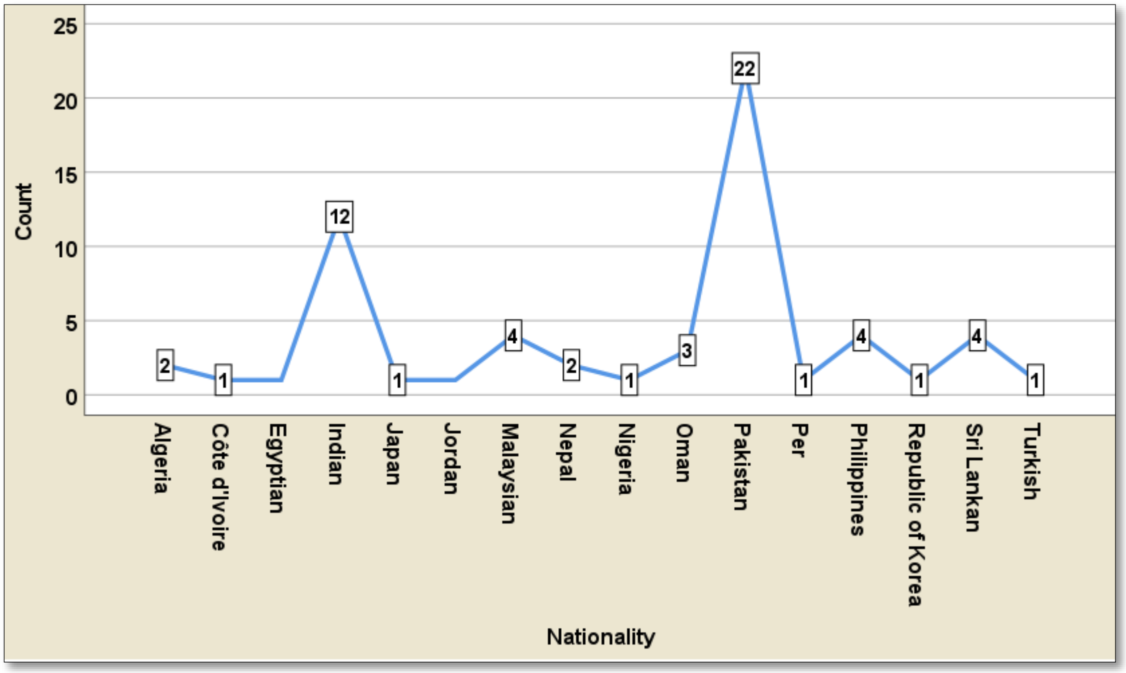
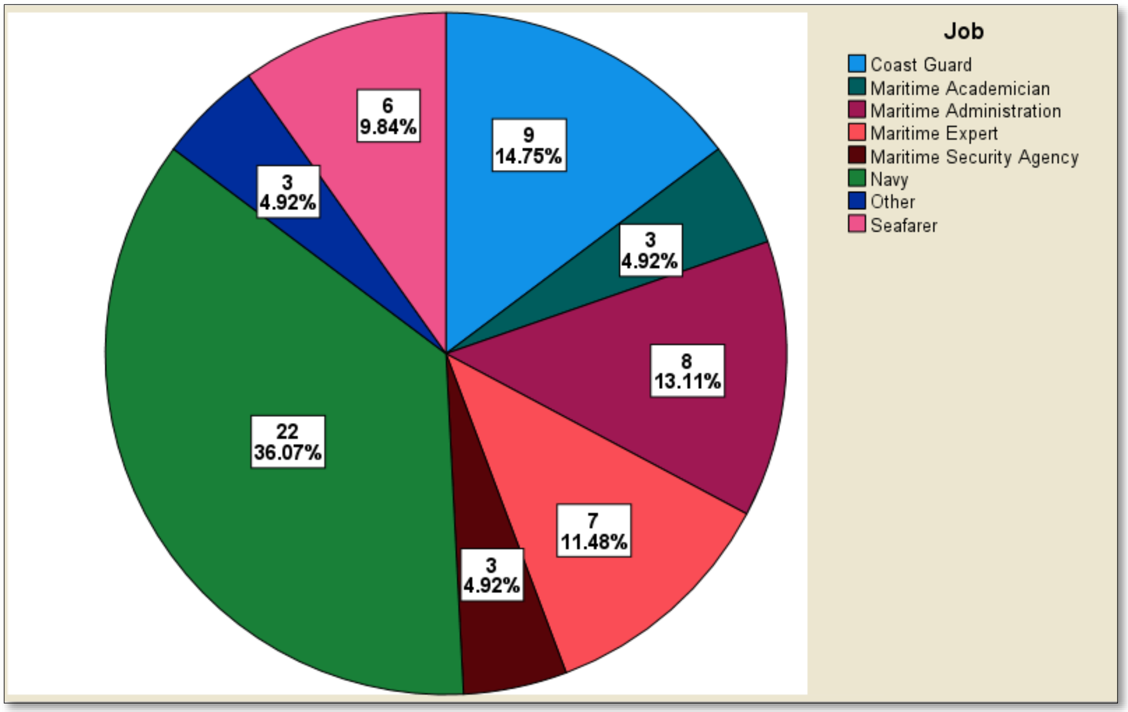


Figure 15

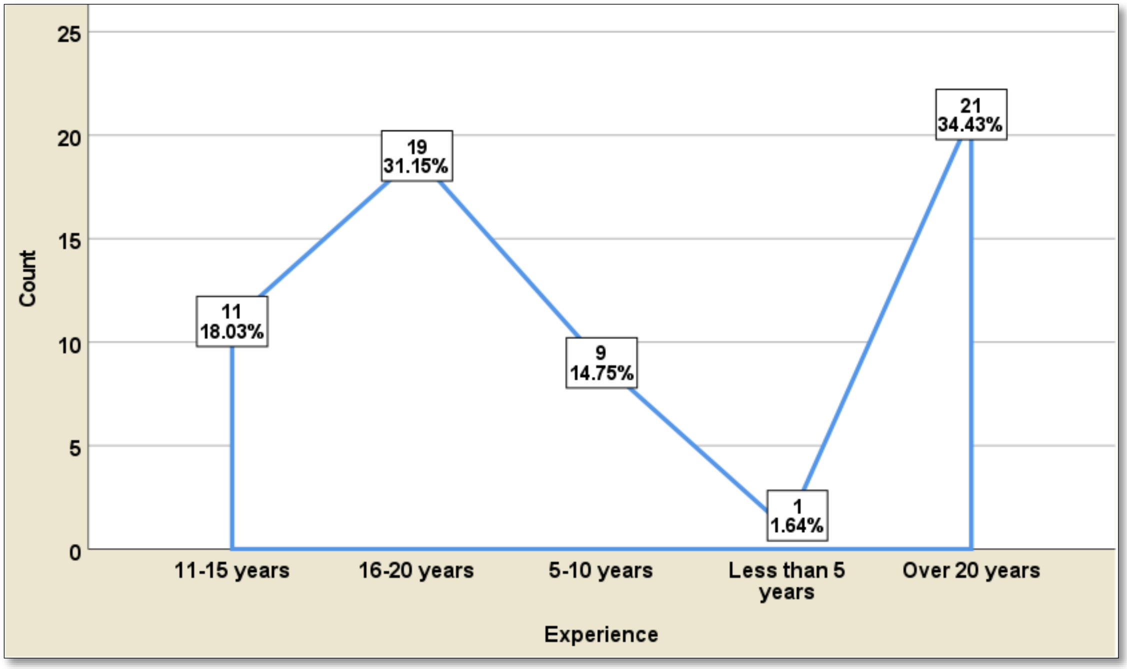
Participant's Profession



It is important to mention that all the responders had a vast experience in their respective fields and were able to share their experience and comment on threats and challenges to MASS and the role of LEA's. The figure 16 shows that 34.43% of the respondents have over 20 years of experience and 31.15% respondents have an experience of 16-20 years. Whereas 18.03% have 11-15 years, 14.75% have 5-10 and 1.64% have less than five year experience. This concludes that the responders have a vast maritime experience.

Figure 16

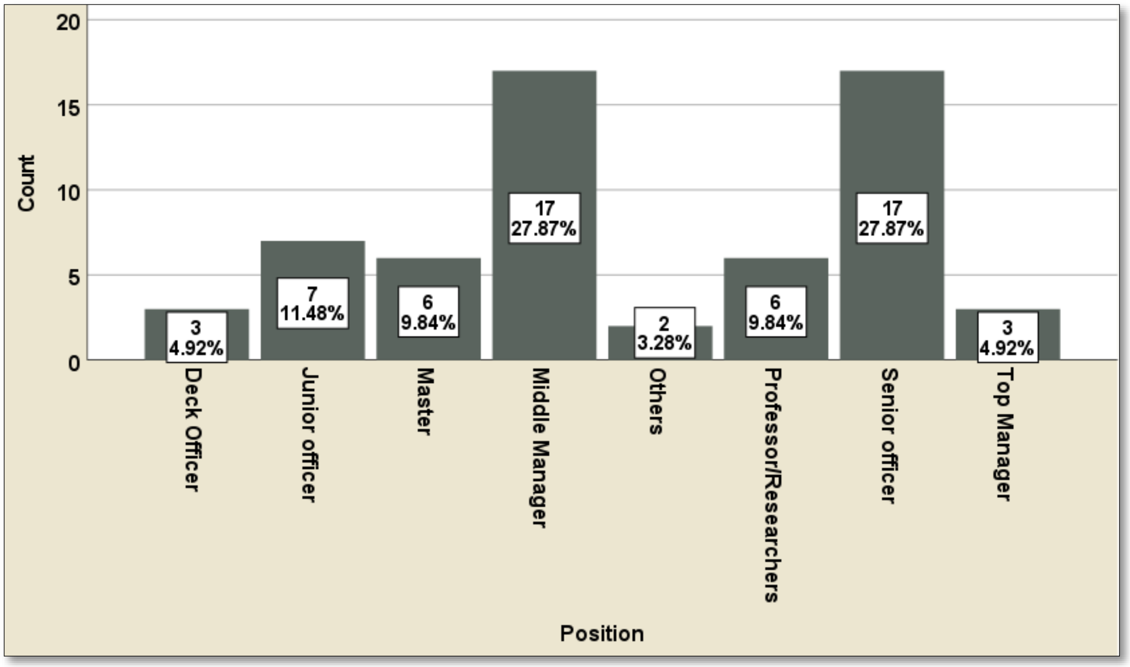
Responder's Experience



Mostly the respondents are at the level of senior officer (27.87%), middle managers (24.87%), junior officers (11.48%), professors/researchers (9.84%), masters (9.84%), deck officers (4.92%) and top managers (4.92%) as shown in figure 17. This shows that the data gathered is from vast variety of people operating at different levels in maritime fields.

Figure 17

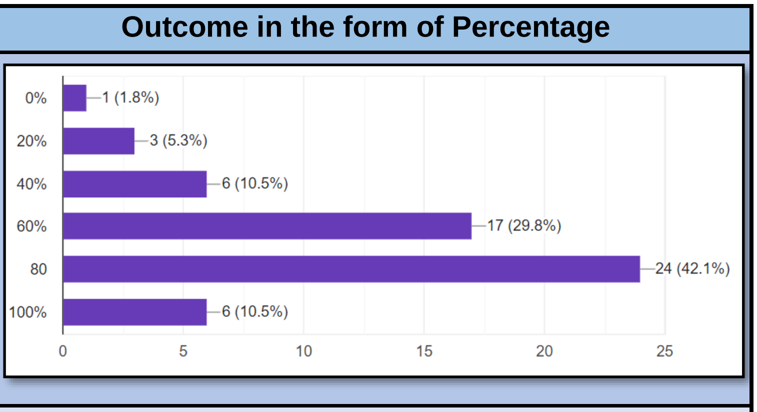
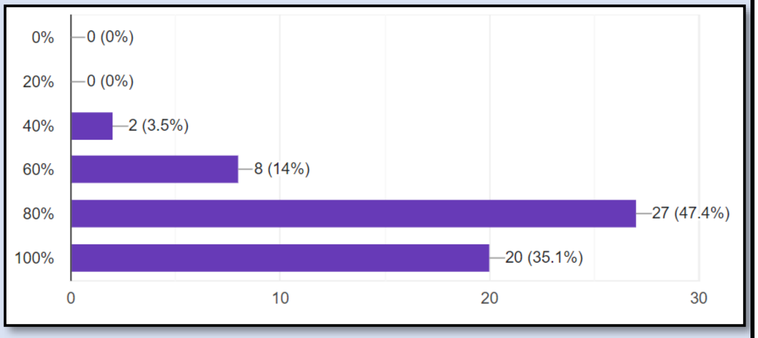
Participants Positions of Working

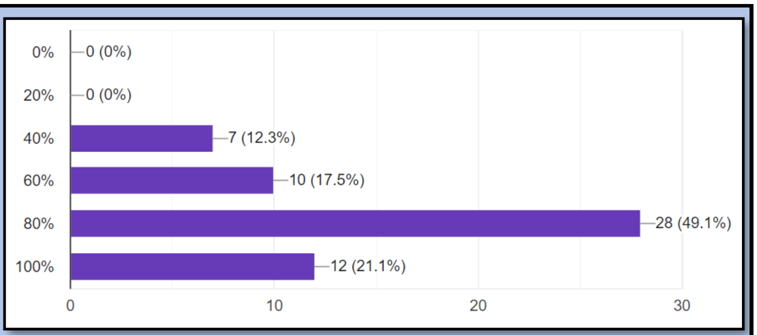
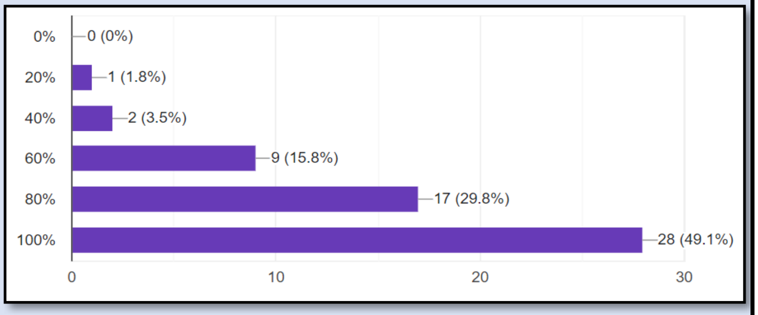


Furthermore, it was also important to know the knowledge of the participant's on the four areas which the author has mentioned in the survey. These are the concept of MASS, concept of maritime security and its importance, threats and challenges to MASS and the concept of law enforcement at sea for analysis so that correct and accurate findings could be extracted. Majority of the participants were familiar with the concept of MASS, concept of maritime security, threats and challenges to MASS and the concept of law enforcement at sea except one out of 61 as shown in figure 8. Finally, total of 60 participant were considered for evaluation and only one was excluded. A detailed outcome/ result of the survey form in graphical display is placed at Appendix D.

Table 8

Participants – Percentage (%) of Familiarization with the Topic

Questions	Outcome in the form of Percentage
Are you familiar with the concept of MASS	
Are you familiar with Maritime Security and its importance in maritime sector	

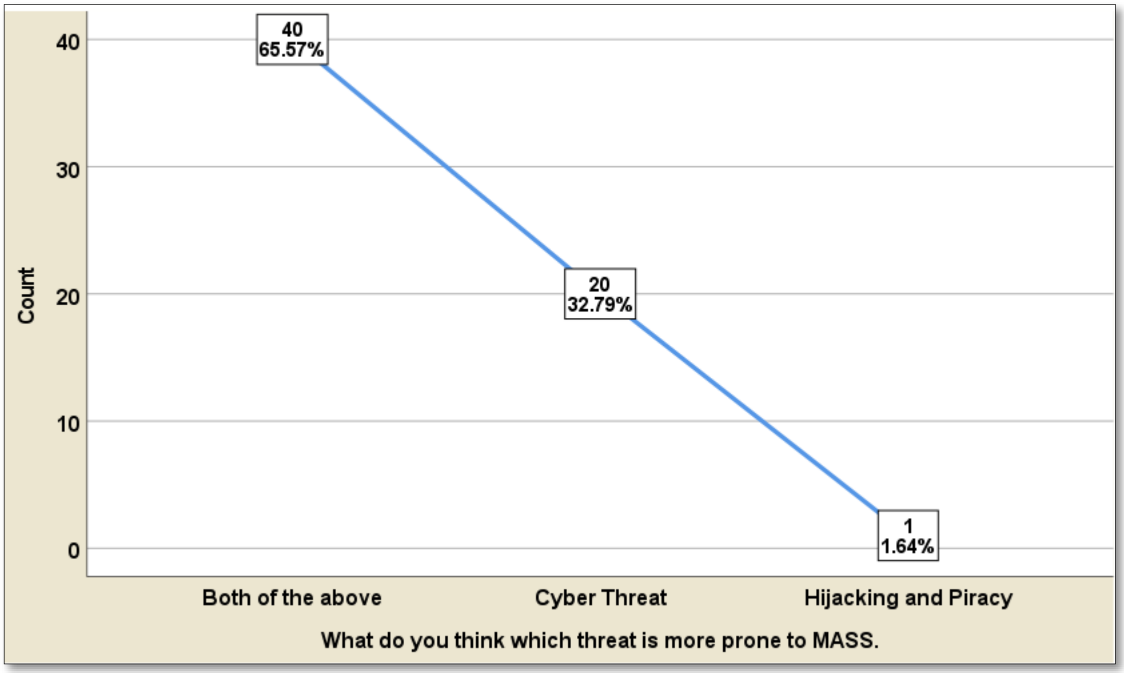
Are you familiar with the threats and challenges MASS may face in future like: a. Cyber Threat. b. Hijacking or seizure of the ship. c. Piracy activity. d. Use of ship to conduct security incident. e. Use of ship itself as a weapon or means to cause damage or destruction. f. Smuggling weapons or equipment, including weapons of mass destructions.	
Are you familiar with the concept of law enforcement at sea by Coast Guard, Navy, Police, Maritime Security Agency's	

4.3 Threats and Challenges to MASS and Role of LEA's Using Scenarios

Before analyzing the threats and challenges to MASS, it is pertinent to mention that after getting the responses and once compared with the literature review, majority of the respondents as shown in the figure 18 were of the same view that the most prominent threat prone to MASS in future will be the cyber threat and piracy threat. Therefore it is obvious that cyber and piracy/hijacking threats (65.57%) are the two top must threats which will effect MASS. Moreover, it must be kept into consideration by the manufactures and the law enforcement agencies. They need close coordination to make and establish a robust and strong communication network along with system in order to deal with these type of threats.

Figure 18

Threat Most Prone to MASS



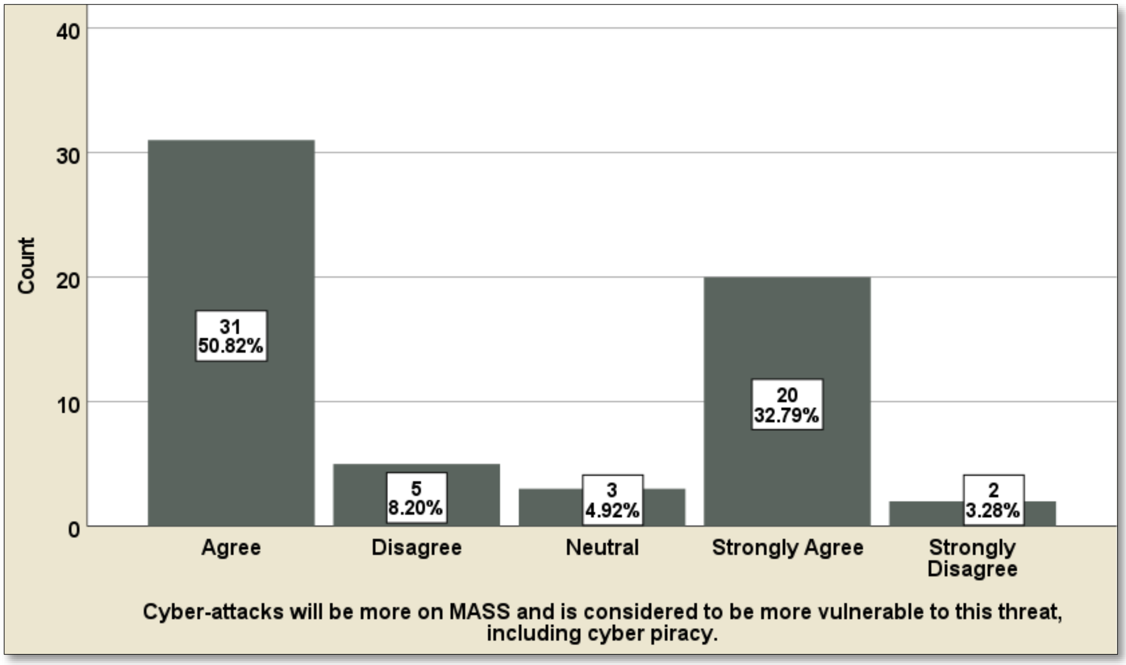
To discuss in detail the cyber and physical threat to MASS/SCC and the role of LEA's, two scenarios have been made and the criteria is discussed in para 2.7 and 3.4.2, and further mentioned in table 10. These two scenarios are purely based on researcher's assumption for discussion which were then analyzed explicitly using the headings of vulnerability of technology and mitigation measures.

4.3.1 **Scenario – I (Analysis)**

The scenario relates to cyber-attack by hacker on SCC/MASS and is at Appendix C. Cyber-attacks will increase in future and will be the top most threat to MASS as compared to other threats. In response to SQ7 as shown in figure 19, majority of the respondents (83.61%) agreed/strongly agreed that cyber-attack will be more on MASS including cyber piracy in future.

Figure 19

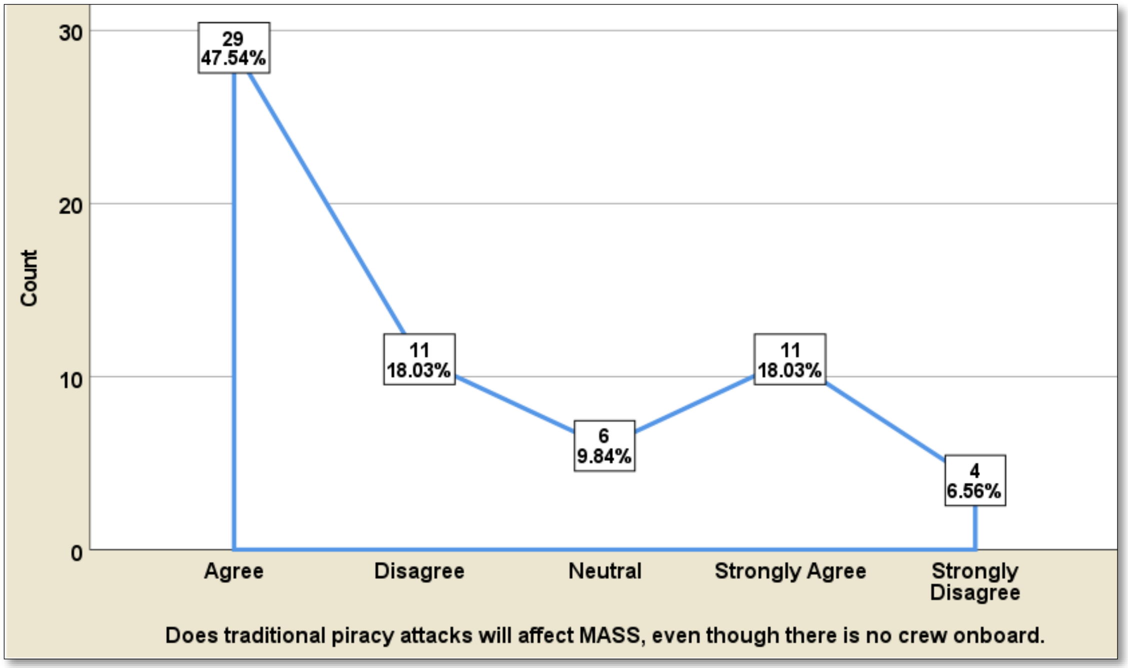
Cyber-Attacks More on MASS Including Cyber Piracy



In response to SQ6 as shown in figure 20, majority of the respondents (65.57%) agreed/strongly agreed that traditional piracy attacks will affect MASS even when there will be no crew onboard.

Figure 20

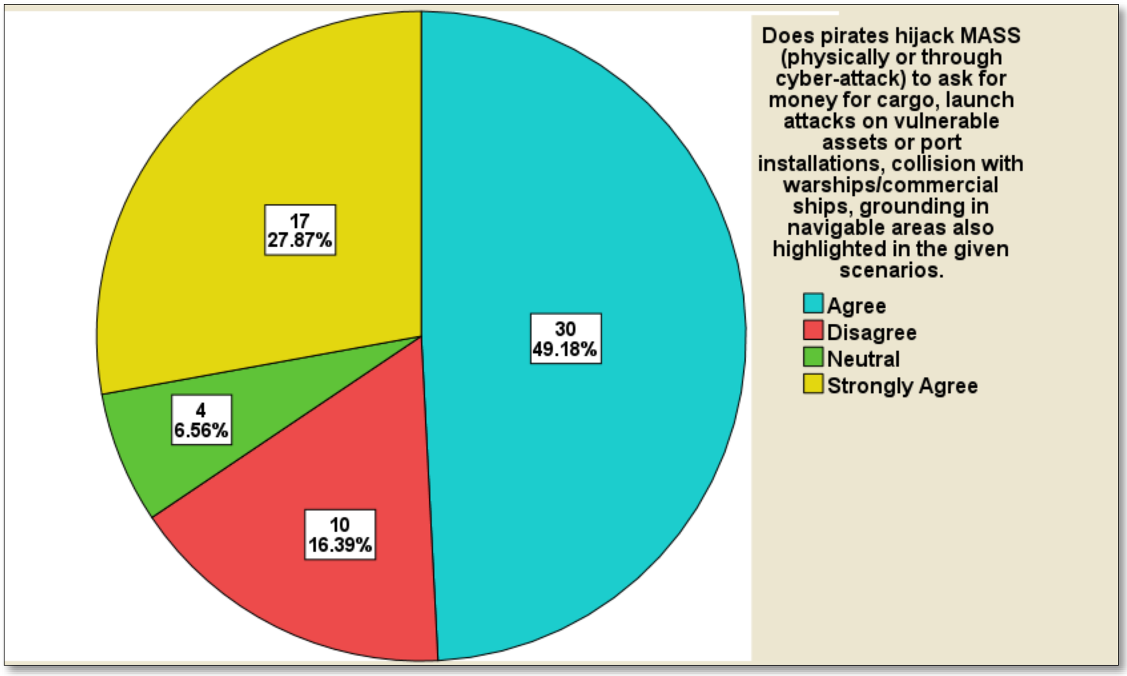
Traditional Piracy Attacks Affect MASS



In response to SQ8 as shown in figure 21, majority of the respondents (77.05%) agreed/strongly agreed upon that hijacking will be done because of the ransom, cargo and stealing a ship.

Figure 21

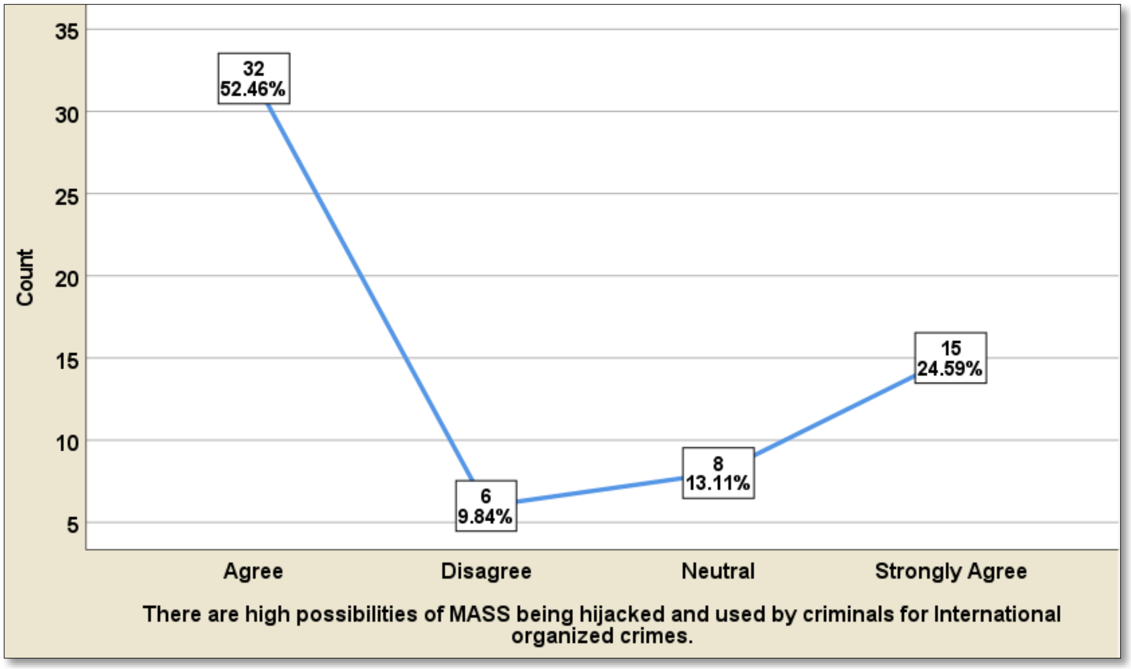
Pirates/ Hackers Ask for Money



In response to SQ13 as shown in figure 22, majority of the respondents (77.05%) agreed/strongly agreed that there are high possibilities of MASS being hijacked and used by criminals/hijackers for different types of international crime.

Figure 22

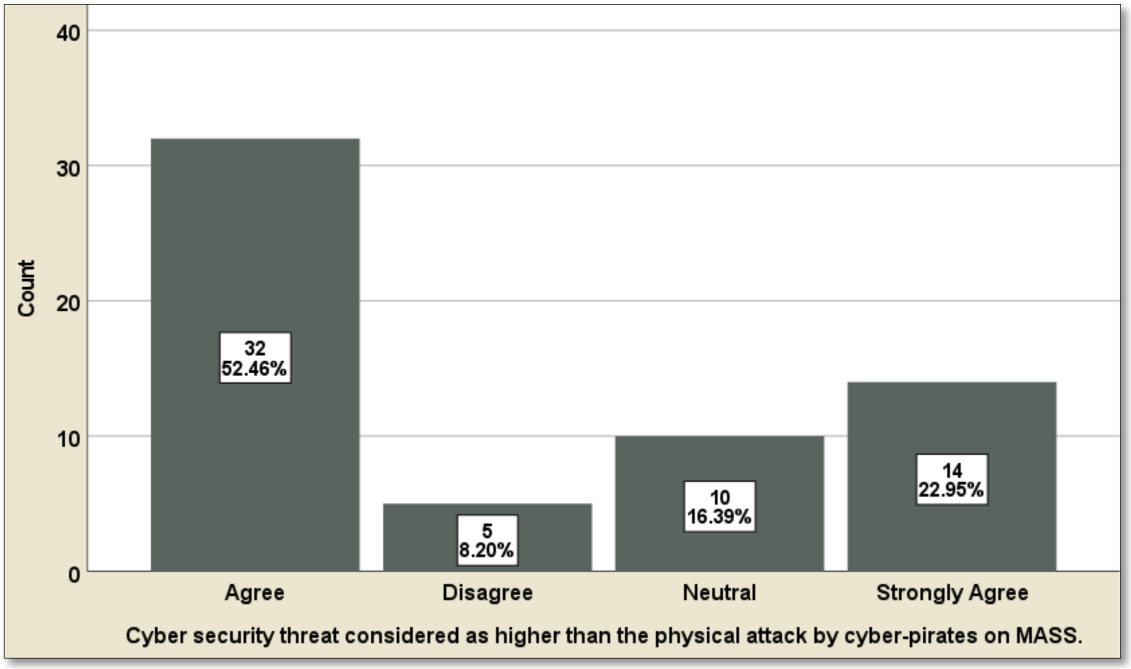
High Possibilities of MASS Hijacking - Used for International Organized Crimes



Therefore, Cyber threat is considered more as compared to physical attack on MASS. In response to SQ11 as shown in figure 23 majority of the responders (75.41%) agreed/strongly agreed upon what is stated above.

Figure 23

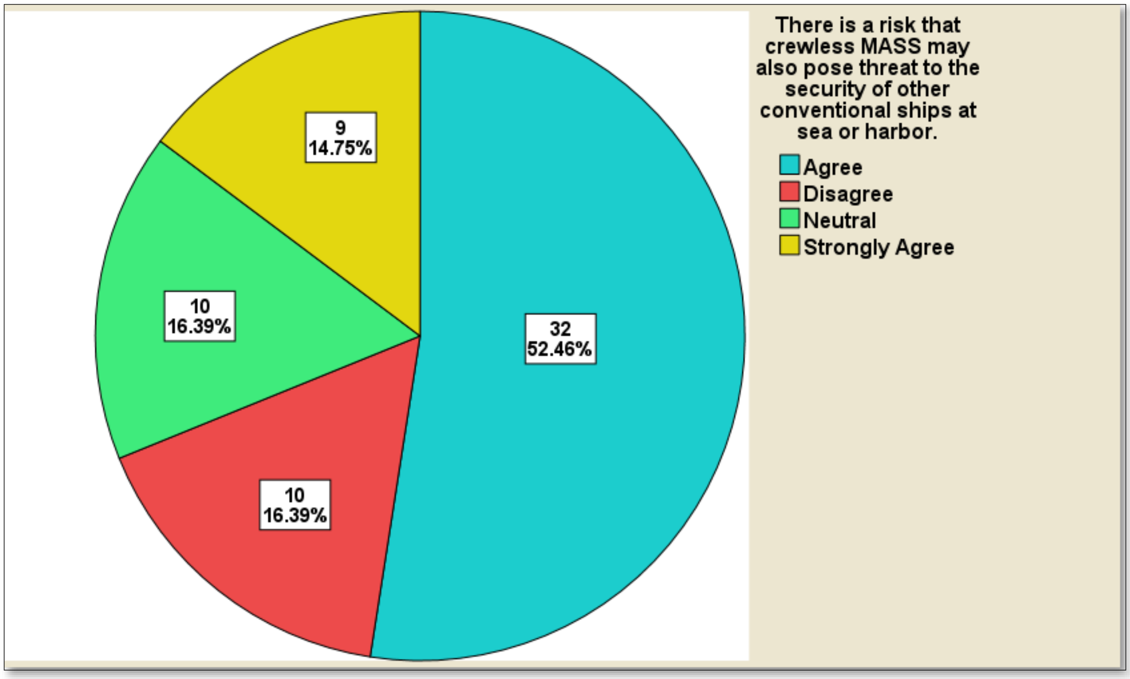
Cyber Security Threat Considered Higher than Physical Attack



Furthermore, crewless MASS may also be directed to drive into commercial shipping at sea and in harbors. In response to SQ11 as shown in figure 24, majority of the respondents (67.21%) agreed/strongly agreed that the possibility of collusion with other commercial ships at sea and harbor is more and cyber-attack is considered as a major threat by the majority of the respondents (82.4%) to MASS as shown in figure 1.

Figure 24

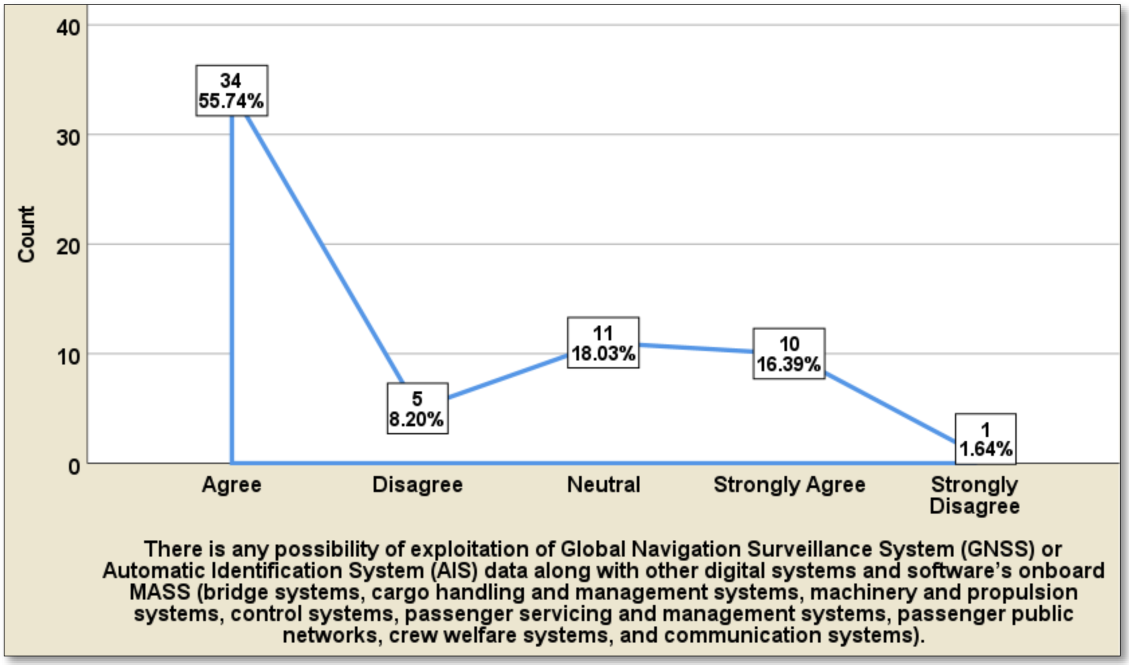
Crewless MASS Pose Threat to the Security of Other Conventional Ships



In response to SQ9 as shown in figure 25, majority of the responders (72.13%) agreed/strongly agreed that there is a possibility of exploitation of GNSS and AIS data of MASS.

Figure 25

Possibility of Exploitation of GNSS, AIS Data Along with Digital Systems of MASS

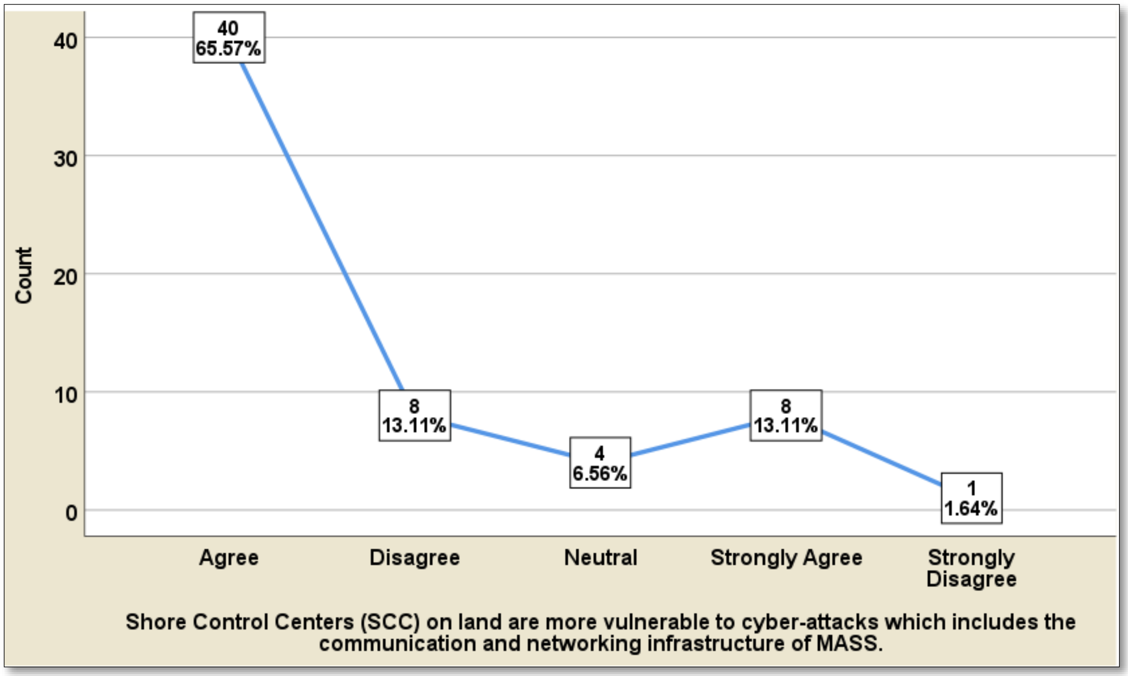


4.3.2 **Scenario – II (Analysis)**

This scenario relates to intrusion/physical-attack by a NSA's group on SCC which is operating/monitoring a number of MASS simultaneously is present at Appendix C. In response to SQ15 (figure 26), majority of respondents (78.68%) agreed/strongly agreed that the communication and network infrastructure of SCC/MASS is more vulnerable to cyber-risks.

Figure 26

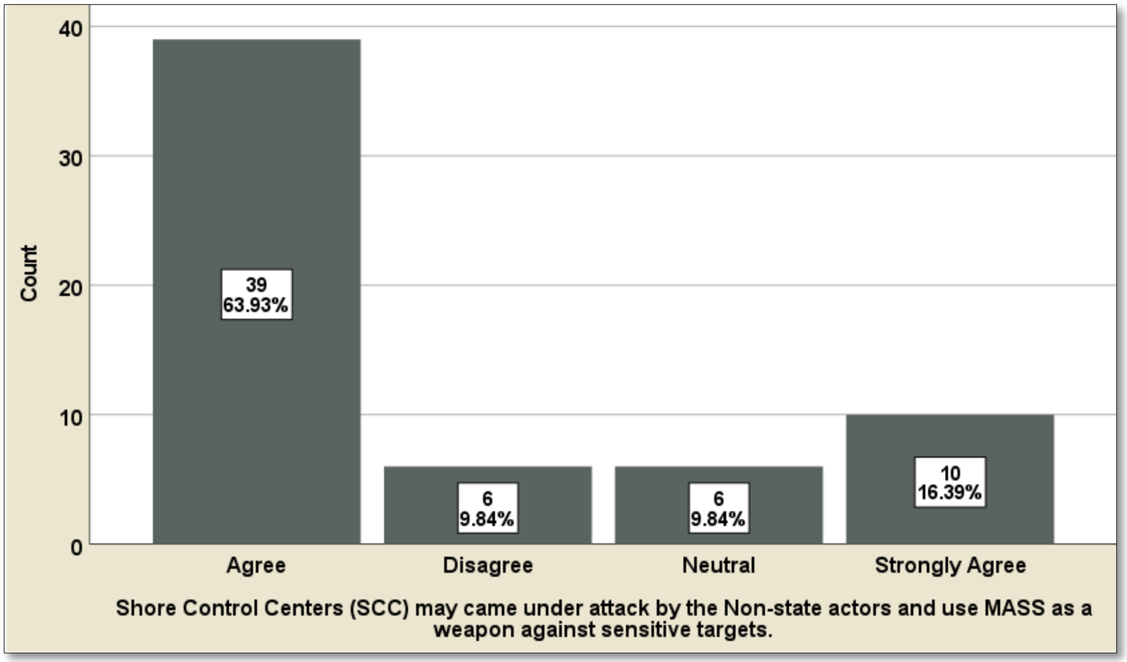
SCC More Vulnerable to Cyber-Attacks - Communication & Networking Infrastructure of MASS



In response to SQ16 as shown in figure 27, majority of the respondents (80.32%) agreed/strongly agreed that SCC came under attack by NSA's and used MASS as a weapon against any sensitive targets (sensitive installation along the coast, warships and commercial ships carrying vital cargo, oil racks in the oceans).

Figure 27

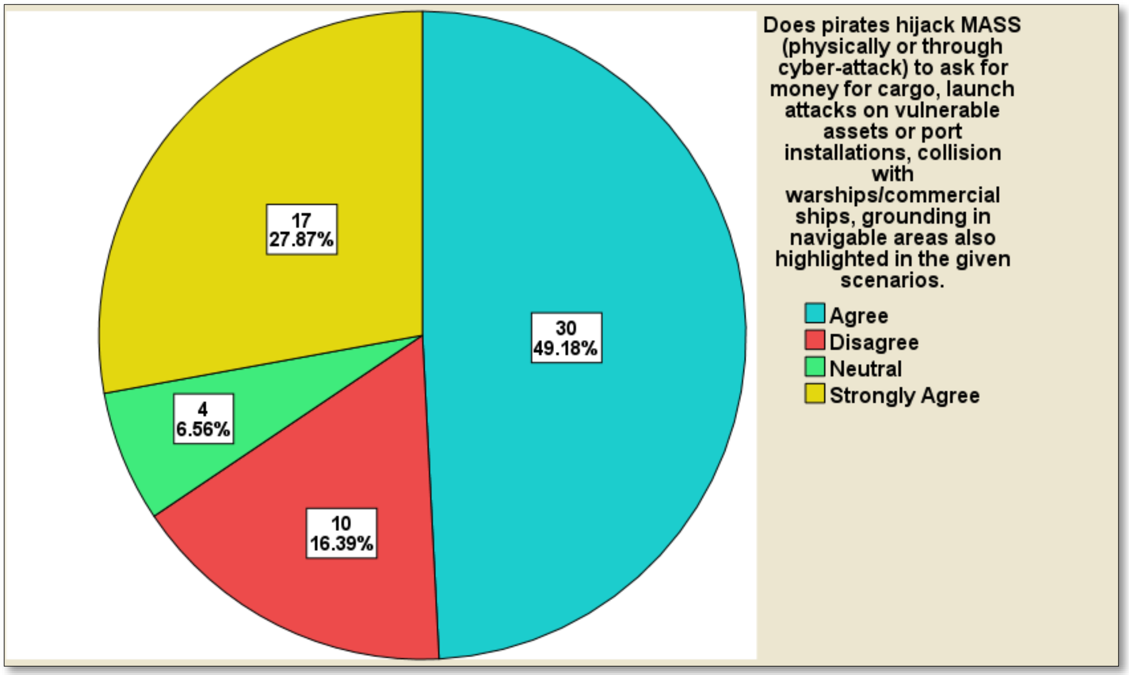
SCC Came Under Attack by the NSA's - MASS Used as a Weapon, against Sensitive Targets



In response to SQ8 as shown in figure 28, majority of the respondents (77.05%) agreed/strongly agreed upon the same results as shown above regarding the hackers and NSA’s.

Figure 28

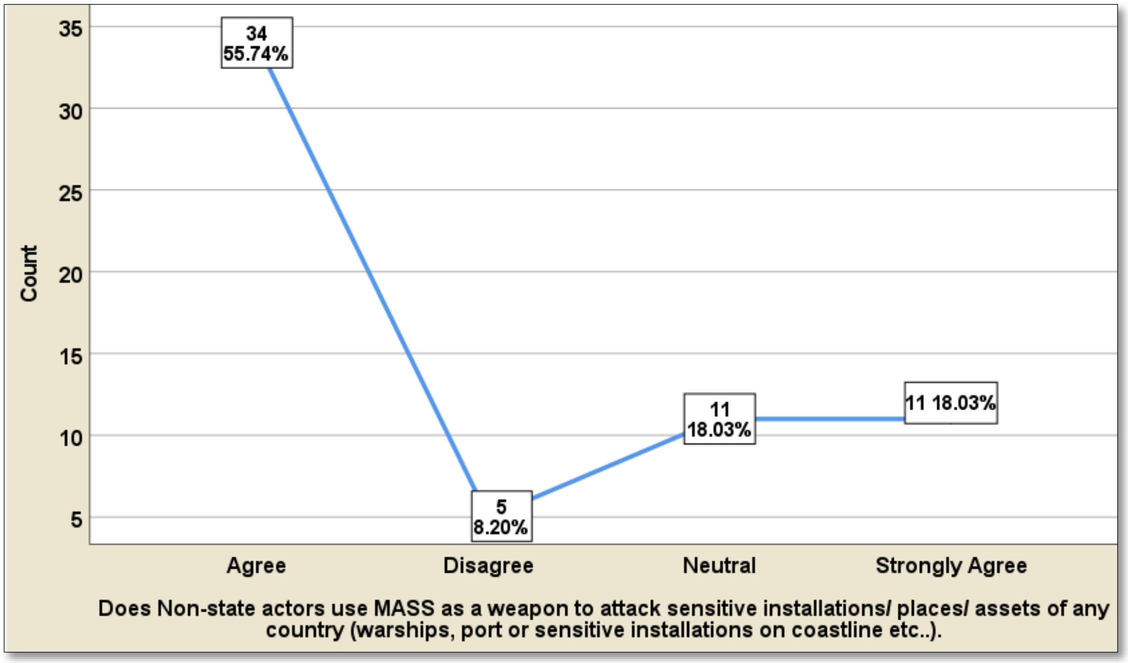
Pirates/ Hackers Ask for Money, Attacks on Vulnerable Assets or Port Installations, Collision, Grounding



In response to SQ10 as shown in figure 29, majority of the respondents (73.77%) agreed/strongly agreed upon and are of the same view which is highlighted and discussed above.

Figure 29

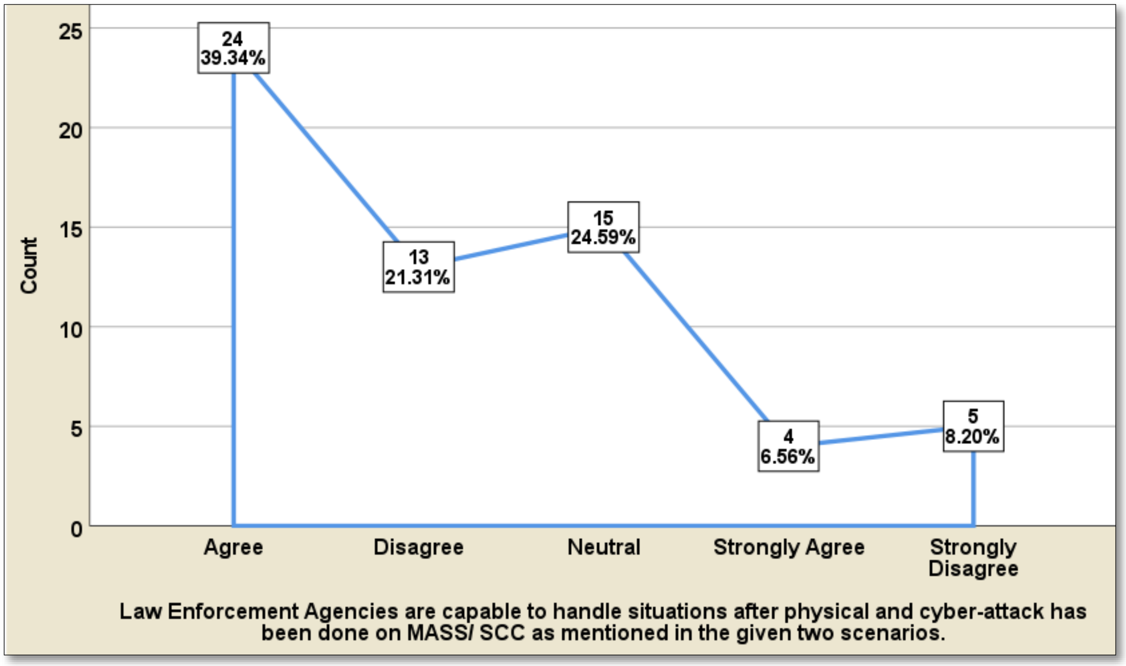
NSA's Use MASS as a Weapon to Attack Sensitive Installations of any Country



In response to SQ17 as shown in figure 30, around 27.51% are disagreeing and 24.59% are neutral whereas half of them (45.90%) are agreeing to what is discussed above. Therefore, it is revealed that LEA's has the capability to deal only physical attacks not the cyber-attacks.

Figure 30

Capability of LEA's - Once Physical & Cyber-Attack Done on MASS/SCC

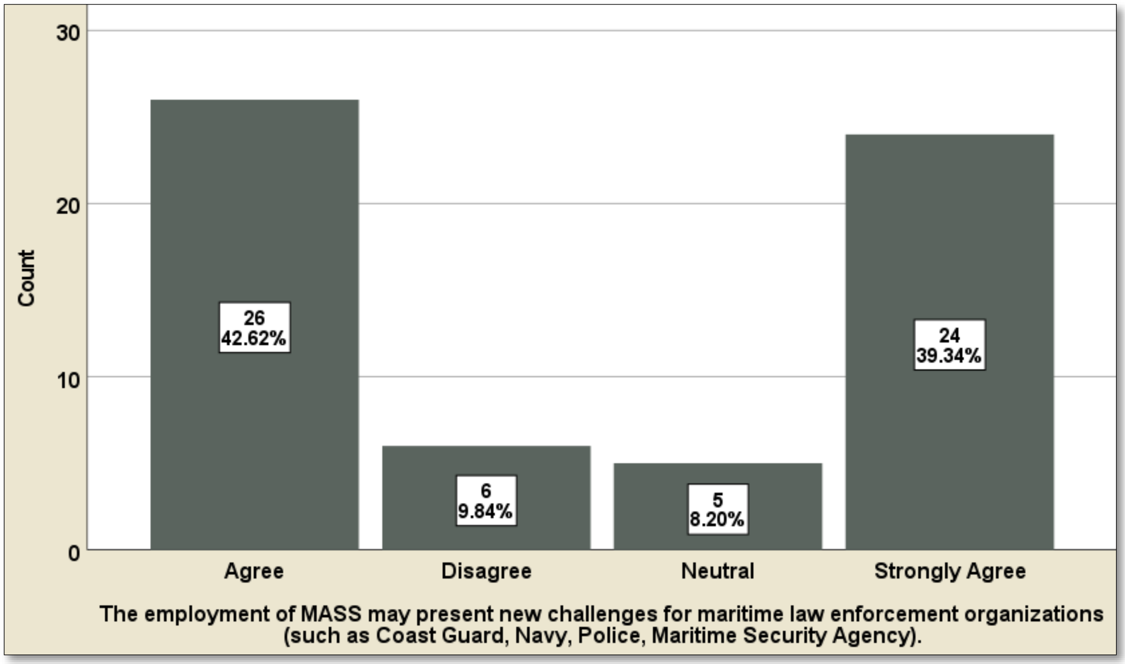


4.3.3 **Role of Law Enforcement Agencies (Analysis)**

In response to SQ18 as shown in figure 31, majority of the respondents (81.96%) agreed/strongly agreed that the employment of MASS will present new challenges for LEA's. Therefore, it is highlighted that MASS is also a new challenge for LEA's as well and to deal with this they have to prepare themselves better.

Figure 31

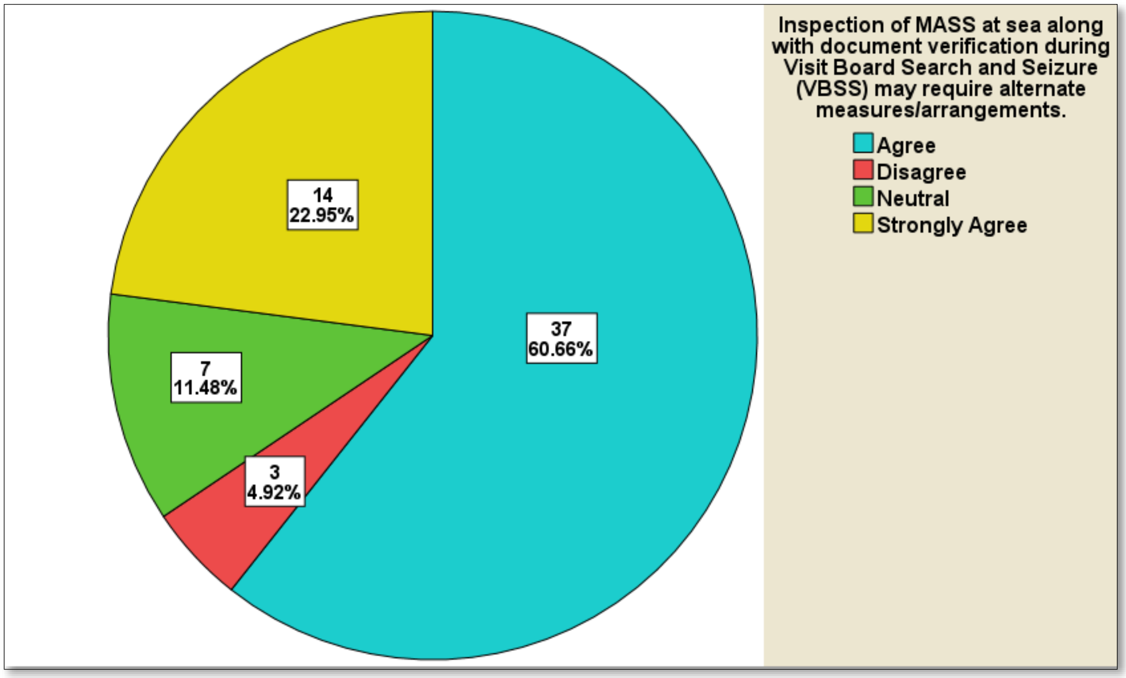
Employment of MASS, Present New Challenges for LEA's



In response to SQ20 as shown in figure 32, majority of the respondents (82.1%) agreed that there must be some alternate means and arrangements for LEA's to verify MASS documents and conduct inspection.

Figure 32

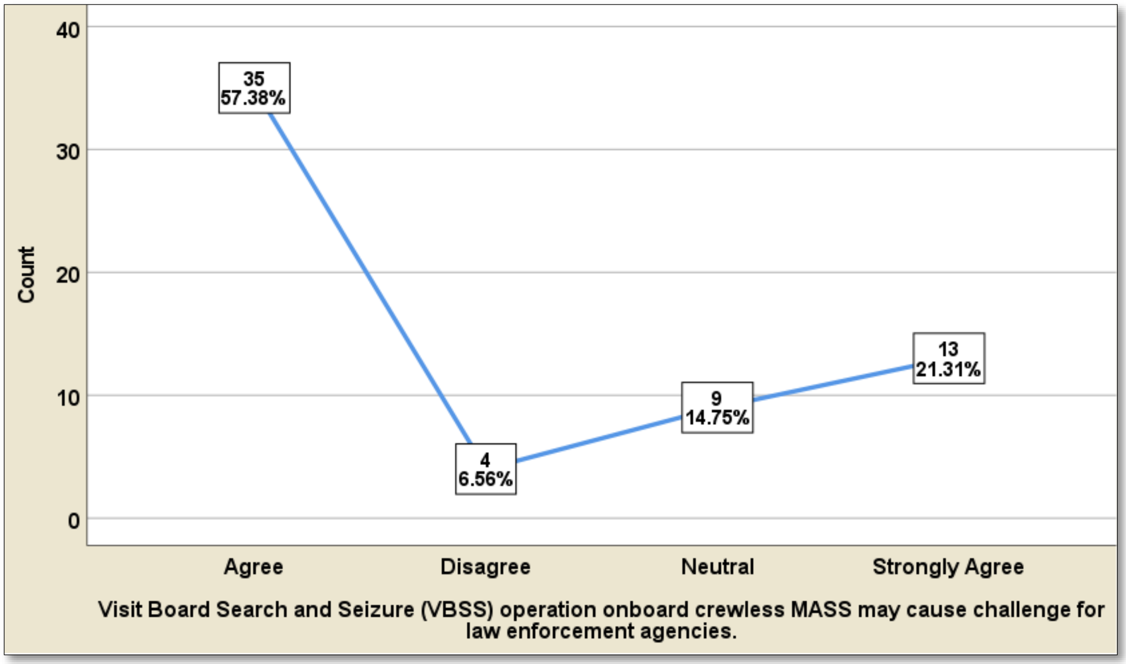
Inspection of MASS, Document Verification Requires Alternate Measures



It is very obvious that after MASS came in operation, the design feature is such that it is very difficult for anyone to get access of MASS once at seas especially the pirates. It also becomes a great challenge for LEA's . In response to SQ21 as shown in figure 33, majority of the respondents (78.69%) agreed that VBSS operations may cause a challenge for LEA's.

Figure 33

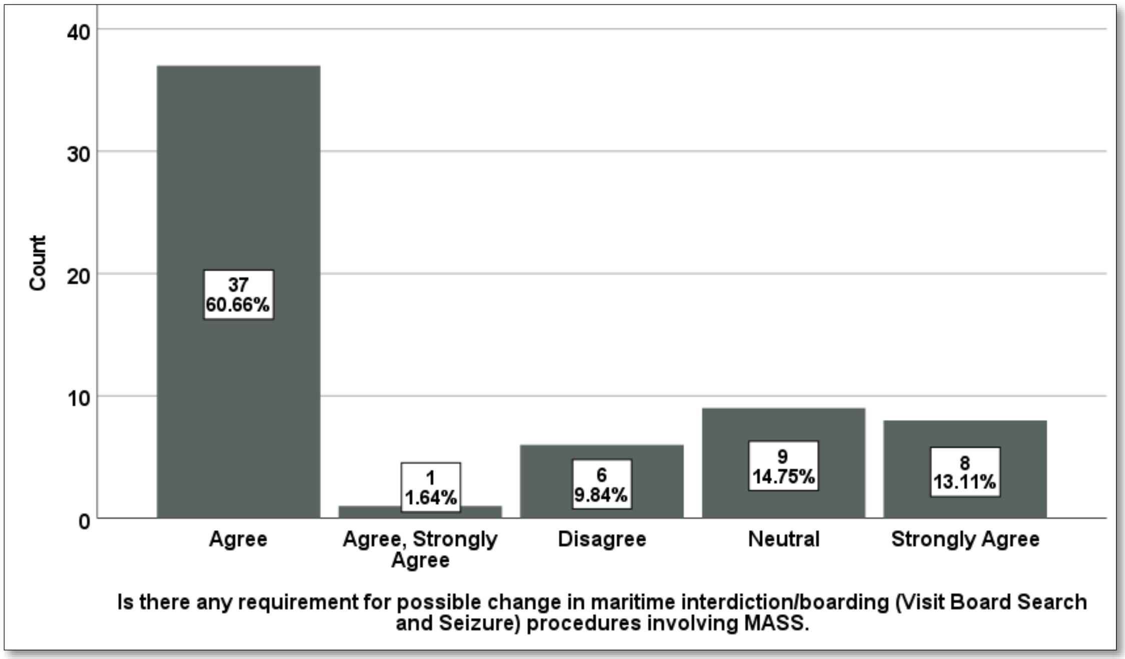
VBSS Operation Onboard Crewless MASS Cause Challenge for LEA's



Keeping in view the challenges of MASS being faced by the LEA's, there must be a requirement for possible change of maritime interdiction/boarding procedures in which MASS is involved. In response to SQ22 as shown in figure 34, majority of the respondents (73.77%) agreed that there is a requirement to change in maritime interdiction operations.

Figure 34

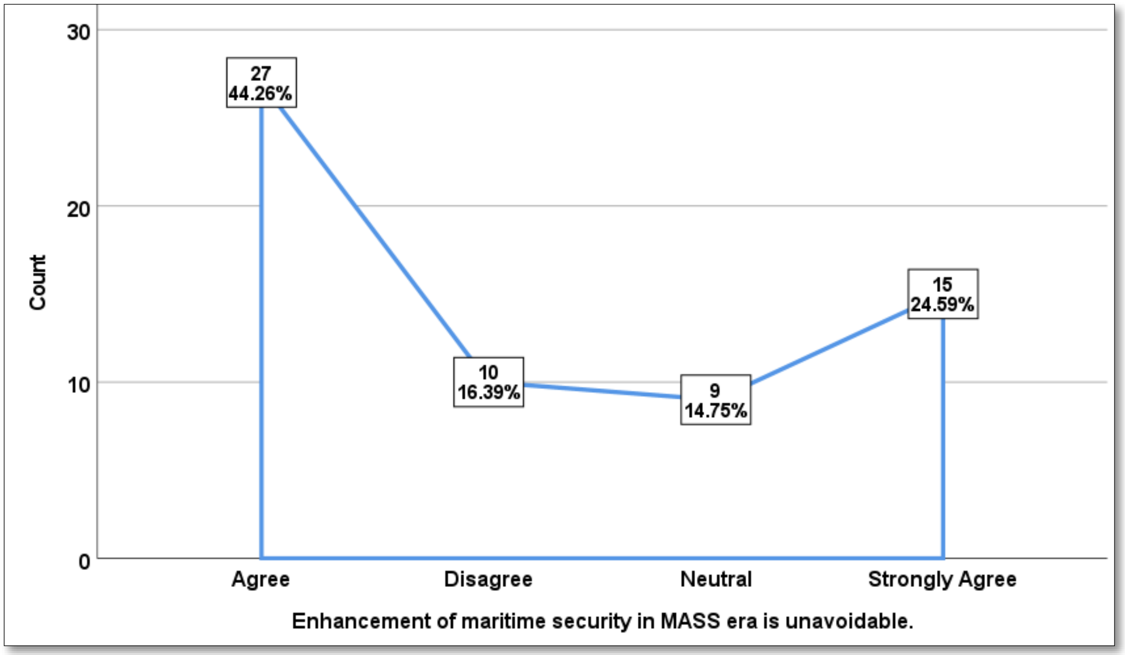
Requirement to Change Boarding (VBSS) Procedures Involving MASS



In response to SQ23 as shown in figure 35, majority of the respondents (68.81%) agreed that enhancement of maritime security in MASS era is unavoidable.

Figure 35

Enhancement of Maritime Security



Chapter 5 – Discussion Recommendations and Limitations

5.1 Introduction

In this chapter, researcher will discuss in detail the threats and challenges to MASS and role of LEA's based on the analysis presented in the previous chapter. Thereafter, some recommendations will be put forward for dealing with cyber and physical threats. In the end some parameters of the study will be presented.

5.2 Discussion (Scenario – I)

If we talk about the cyber piracy, one of the threat includes hijacking of a ship at sea (piracy attack) and MASS itself can also become a maritime security threat as mentioned in figure 20. This threat to MASS may cause devastating consequences in the minds of the peoples' perception (Fan et al., 2020). This hijacking will remain like a traditional piracy attack for some financial advantages or some political agenda but as discussed it will be a multi-mode attack of initially cyber followed by a physical attack.

According to some experts, piracy includes two types of offences, first is hijacking (for ransom, cargo onboard, stealing of a ship) and second is kidnapping which includes threatening of crew until some ransom has been paid to the pirates as shown in figure 21 (Tumbarska, 2018).

In level of autonomy 1 and 2, the kidnapping as well as hijacking may be done whereas in level of autonomy 3 and 4 only act of hijacking may be possible. However, it is possible only when the cyber-attack is done initially. MASS will be technologically very advance and will entirely dependent on communication network, AI and satellite link which will definitely bring some new risks for MASS. AI may become security weakness for MASS during its operations (Heikkilä, 2018). The gaining of access to control system of MASS by hackers is a vulnerability due to which it is considered as a main disadvantage of MASS (Li & Fung, 2019). As per the maritime decision-makers, there must be some reason for pirates to board ship like cargo onboard, ship itself and may use as a weapon for a mass destruction. In case of Southeast Asian pirates, their main cause of hijacking a ship is for cargo in that the crew suffer injuries (Jiang & Lu, 2020).

As highlighted above in case of level of autonomy 3 and 4, there will be no crew onboard and it may be considered as a soft target for the hijackers to steal cargo or take control of the MASS. Hence, there is a threat that MASS will be in the hands of the pirates who may conduct terrorist activity. There is also a possibility that MASS may be used to conduct international organized crimes or collide with an oil rig as shown in figure 22 (Eriksson & Gevriye, 2018).

The possibility of physical attack on MASS is lower as compared with the cyber-attack because MASS is entirely dependent on IT, satellite and ICT systems on land (SCC) and at sea (MASS) as shown in figure 23. Taken into account the three security aspects people, processes and technology, technology is considered as a weak link along all elements of security. As technology is advancing day by day, there are many loopholes for interference especially in ICT of MASS. Moreover, the design feature (hull structure) of MASS will be in such a way that it will be very difficult to get access on MASS by the pirates, it's like a free board (Chae et al., 2020). Further, it also restricts the entry of unauthorized personnel on MASS.

There are many incidents reported worldwide as shown in the table 9. There are still possibilities that modern pirates may also alter their techniques with the change and advancement of the technology. If in any situation, pirates are able to physically get into the MASS, there will be no accommodation except control room and engine room. To get access of the control room great degree of knowledge will be required. An IT expert with an ultimate hacking capability is considered very less possibility that all these capabilities are present in ordinary pirate. Moreover, in autonomy level 1 and 2 it is possible but it is not possible in autonomy level 3 and 4.

Table 9

Incidents Reported in Year 2020

S. No	Incidents in year 2020	Quantity	Remarks
1.	Piracy and armed robbery Incidents	195	Higher than the year 2019
2.	Hijacking of the ships/vessels	03	-

3.	Attempted attacks by the pirates	20	-
4.	Boarding done by the pirates	161	-

Note. Prepared from "Shipping and new technologies," by International Chamber of Shipping. 2021, (https://www.ics-shipping.org/shipping-fact/shipping-and-new-technologies/).

There are examples of physical as well as cyber-attacks on commercial ships as shown in table 10. Terrorist/hackers might use MASS as a weapon against countries that have a strategic and economic importance (Suez & Panama Canals) or where they consider that the risk of environmental disaster is high. There is an example on 23 March 2021 when container vessel "Ever Given" stuck in the Suez Canal. As a result, one of the busiest shipping trade route of the world was blocked for 6 days and resulted in economic loss as more than 100 ships were waiting on both ends on the canal (NY Times, 2022).

Table 10

Incidents of Physical and Cyber-Attack in Year 2021

S. No	Incident	Year	Explanation
1.	Hijacking of Panama flagged vessel Asphalt Princess.	August 2021	Reported in Gulf of Oman (GoO) by the United Kingdom Maritime Trade Operations (UKMTO). The vessel was boarded by heavily armed men, but the crews prompt action in disabling the engine prevented the incident.
2.	Cyber-attack on 5-6 Oil tankers	August 2021	On the same day of the above reported incident, in the same region reported problems with their navigation equipment of the oil tankers which led to the speculation of a possible cyber-attack on vessels in area.

Note. Prepared from "SBS Boarding Team Detains Stowaways After Confrontation Aboard Tanker," by Maritime Executive. 2020, (https://www.maritime-executive.com/article/sbs-boarding-team-detains-stowaways-after-confrontation-aboard-tanker).

Aforesaid discussion in view, it may be said that cyber-security or threats of cyber-piracy as compared to physical attack is more likely and practical as shown in figure 24. Cyber-attacks take advantage of communication network weaknesses, which may endanger the reliability or accessibility of data and MASS regulatory systems (Bolbot et al., 2019). MASS is exposed to cyber-attacks, and the threat is not related to MASS itself or its cargo, but it may be a threat to the sensitive installation/infrastructure along the coast and offshore if MASS is hacked. Consider MASS is approaching these sensitive installations with high speed and lead to collision which result in a serious damage and disaster. This will be true even if it is a small tonnage of MASS as it will also damage those installations. A cyber-attack is compared with a terrorist activity/attack conducted on USS Cole (Guided Missile Destroyer) of the US Navy. A small fiber glass boat hit with the warship full of explosive along with two suicide bombers (Vinnem & Utne, 2018).

For cyber security, appropriate technology is present nowadays, the only point is system should be properly designed and consequently accurate crypto solutions are to be used by the manufacturers. There is another side related to MASS communication which is of jamming and spoofing and can possibly be used by NSA's/criminals against MASS (Akpan et al, 2022). Jamming is consider as a significant concern other than cyber-security, which is manageable through appropriate AI software's which can pinpoint signal irregularities. However, spoofing may confuse AI to commence unwanted evasive maneuverers. It is also pertinent to mention that, when one AIS transmission has been hacked, 50% of the job is done related to controls of the MASS, which is not easy to fix quickly and requires time as well as money (Eriksson & Gevriye, 2018). Further, GNSS system will also be jammed or spoofed as shown in figure 25.

5.2.1 **Mitigation Measures (Scenario - I)**

Against pirates, MASS is considered as an effective solution, Hull structure (design feature) of MASS is the major proponent (Chae et al., 2020). It is always easy to recapture an unmanned MASS. In case of any emergency, SCC can play its role and take appropriate measures and especially get necessary assistance from LEA's. However, it would be difficult to stop a MASS which is hijacked because its operations and controls are in the hands of the hackers.

Hull structure/design feature is the key factor of preventing MASS from elements like pirates (Chae et al., 2020). If these elements try to hijack MASS, design may be like free board that they should not succeed in getting inside MASS or if it happened there must be some heat sensors motion detectors and cameras (internal and external) installed by the shipping companies at the access points along with the places like main control system and engine control system. This will ensure that SCC may come to know that some unauthorized entry has happened or about to happen on MASS so that necessary actions are taken by SCC and if required also coordinate with LEA's.

Better coordination with local authorities, cooperation with different states and keeping LEA's in loop may bring MASS safer against these type of threats. Coastal states have responsibility to make themselves technologically strong and attain such capability to control MASS for safe operations (BIMCO et al, 2018).

MASS should also avoid passing through HRA's and as per Best Maintenance Practices (BMP's), it should adopt security protection measures and physical barriers like Razor wire (barbed tape) and use of non-leather weapons (BIMCO et al, 2018).

Cyber security must be maintained during cyber-attack responses and prevention plans centered on vulnerability identification. The implementation of high standards is necessary for both MASS and SCC in order to deter any type of threat.

To avoid hacker's attack, IT staff along with security experts must plan and conduct regular incident checks and drills in order to identify weaknesses and bring improvement in the security program of the ship (Li & Fung, 2019).

There should also be a continuous risk assessment as mitigation measure depending upon an identified risk. Follow/implement cyber security guideline promulgated by IMO (MSC-FAL.1/Circ.3/Rev.1 – Guidelines on maritime cyber security assessment (IMO, 2017d), MSC.1/Circ.1639 – Guidelines on cyber security onboard ships, ISO/ IEC 27001 – Standard on Information Technology) and recommendations (IACS recommendations on cyber resilience (Rec.166)) on cyber security.

5.3 **Discussion (Scenario – II)**

In case of vulnerability to the technology in the degree of autonomy 3 and 4, MASS control is shifted to SCC where the operator is capable of handling and operating several MASS simultaneously. Through ICT, MASS establish link with SCC through satellite which may also open an opportunity for hackers to access the main system practically and exploit it. There are possibilities of cyber as well as physical attack on SCC. All the participants of the survey showed a great concern about the security of SCC. The first concern is the cyber threat to SCC. In the field of communication sector, 5G is a new jump and illegally it's very difficult to get access, same is the case with the SCC. However, still cyber-attack being well known and prone threat could possibly make SCC its target as shown in figure 26.

The second concern is that NSA's group can attack on SCC and get control of the MASS through communication network. There is definitely a possibility that SCC may also come under physical attack/intrusion due to which its security is paramount as shown in figure 27.

In addition to this, the issue raised by SMEs in one of the qualitative study by Roberts and colleagues stated that hackers hijack the network system of SCC and direct MASS at a place where attackers can board MASS very easily (2019). Hence, stealing of MASS through physical attack may appear less helpful in the scenarios (Carey, 2017). The security threats for SCC tend to vary based on the state of security of the country. In case of a developed country, the security state will be good due to which the threat to SCC will be low and vice versa. However, in both cases if SCC is vulnerable to physical attacks, maritime security is considered incomplete. Hence, if the control of SCC went into the hands of NSA's group, they might lead MASS to a safe place in the ocean for different purposes. These include embarking terrorist to enter the port or conducting terrorist activity, to bang into a warship/commercial ship inside port or at sea, conduct grounding near port entrances/inside Channels, blocking international shipping routes, carryout environmental pollution and demand for ransom as shown in figure 28.

Furthermore, if we talk about the sensitive installations of any particular country which includes sensitive installation along the coast of strategic in nature, warships and commercial ships carrying vital cargo, oil racks in the oceans. The NSA's may also be used and derived by some other country to achieve their political agendas and use MASS against sensitive installations as shown in figure 29.

Once SCC comes under cyber and physical attack, is there any possibility to deal with this situation by LEA'S? In case of physical attack, yes there is a role of LEA's and has the capability to counter physical attack done by the NSA's group and further bring SCC in its normal working state through those operators who are already working in SCC. However, LEAS's don't have the capability to counter the cyber-attack and resume SCC in its normal working condition as shown in figure 30.

5.3.1 **Mitigation measures (Scenario - II)**

Communication link system between MASS and SCC is considered crucial for MASS's safe and proficient operation. Therefore, this system needs to be bidirectional, vigorous, correct, and capable of reinforcing with different systems, without making any redundancy and reducing the interference of third party (Chae et al., 2020). Present era is the era of technology, where cyber-security is considered as an important proponent/tool to deal with different types of cyber-attacks. In order to deter and neutralize the cyber threats, it is very important to implement high standards of measures for MASS/SCC. Hackers try to attack the main system in case of SCC/MASS. Communication link is the loophole where hacker try to interfere. Therefore it is important to give stress on this aspect in order to prevent these type of attacks (Akpan et al, 2022).

Furthermore, it is important to conduct training of personnel who are working inside SCC as operators and technicians, carry out practical drills, conduct the audits and do valuation of all the vulnerabilities to come up with good solutions (Akpan et al, 2022). There is an example of 9/11 attacks, in that US government implemented strong security measures for the protection of ports and maritime transport in form of ISPS and Container Security Initiatives (CSI) after the terrorist activity was done through commercial aircraft.

Therefore it is necessary for those states having high security environment to develop proactive security measures for SCC.

There must be some contingencies for SCC and they need to be well defined. There can be an overriding option available in other SCC to shift control immediately in their hands. This option is not only in case of cyber-attack it can also be helpful to deal some other emergencies. Therefore, they must have strong and well protected passwords, communication and links in encrypted form and security cleared personal inside SCC.

Manufacturers also have a very important role in the security of SCC as they are the SMEs of that system which is installed in SCC and its security is paramount. Therefore, they must make and build such strong Information Communication Systems (ICS) and networks which cannot become victim of any cyber-attack. Furthermore, strict measures should be enforced and strong powerful programs should be installed which are able to deal with cyber threats. In case of physical security of SCC, barriers are to be placed, deployment of security guards, security cameras and protected walls/ fences/ barriers around SCC.

Based on above discussion, it is concluded that SCC is an important and high risk place/asset which requires physical and cyber security. For maritime sector, IMO is the only platform which can play an important role especially for the security of SCC. All SCC's must comply with the IMO present security standards and in future it is suggested that IMO must regulate more robust standards for SCC to establish uniform policies which are to be implemented by every coastal states. Furthermore, in RSE outcome SCC is taken as the top priority issue as far as revision of the IMO instruments are concern (IMO, 2021). Though, SOLAS chapter XI-2 was not came under consideration as likely theme.

We can say that, SCCs will affect the maritime security arena in days to come, and all the SCC's should be secured against cyber threat and physical attacks. A single center (SCC) which is hijacked can aid hackers to control many MASS simultaneously and probably be used as per the wish of the hackers. IMO have an important role in safeguarding high standards for these centers.

5.4 **Role of Law Enforcement Agencies**

The employment of MASS is considered a major challenge for coastal states and law enforcement agencies. Threats to MASS which are discussed above somehow have to be neutralized and in that the role of LEA's is very important as shown in figure 31. It is considered that if the coastal state's law enforcement is less in number or scarce, occurrences like piracy, hijacking and physical attacks will continue to occur. However, if the number of patrolling timings increases; increase of accessibility at longer distances and provisioning of advance technology to LEA's; the chances of these incidents/situations might be relatively low.

Van Hooydonk (2014) and Wrobel (2017) have explained the problems of technology in relation to situational awareness and consistent working of technical components. Nevertheless port security along with other procedures, the security of MASS/SCC is totally controlled and managed through technological means. Therefore, MASS/SCC vulnerability and security situation in that particular area decides the figures and severity of incidents happened on MASS/SCC.

MASS is expected to uphold the maximum ISPS code requirements. There are limitations of both technology and automation. Moreover, most of the ISPS complied ports are aided with surveillance arrangements to detect any type of unwanted presence or unauthorized personal in the port areas. Furthermore, physical security should also be used and integrated with these electronic surveillance systems. Resultantly, there must not be any situation occurred to attack physically on SCC by any NSA's group.

In case of inspection of MASS during VBSS at sea, it will be difficult for LEA's to check the documents and verify them. In level of autonomy 1 and 2, it is possible as there will be crew onboard however in level of autonomy 3 and 4, it is not possible. Therefore there is a dire need to take up this issue at an appropriate level and come up with solutions as shown in figure 32.

5.5 Recommendations

Based on above analysis and discussion, following recommendations are suggested:

- Global strategy is required to be developed in order to facilitate MASS operations. In this regard, all regulatory bodies, member states along with element of LEA's and MASS manufacturers should sit together to find potential gaps in making MASS operations more secure and strong enough to deal with man-made threats.
- Manufacturers before constructing MASS must consult and keep in mind the viewpoint of LEA's to prevent any type of security incident. In situation where risk is kept as low as possible, stringent access control measures, active surveillance techniques, cyber security solutions of high grade are to be used and are to be frequently upgraded.
- Port security measures need to be enhanced and those ports which are in a planning phase of operating MASS should undertake risk assessment first.
- Impose and implement regulations related to new emerging security risks to MASS by IMO to gain trust of maritime transport industry.
- Stringent security measures must be taken against both cyber and physical threats to SCC as it emerges as the hub of MASS operations.

5.6 Limitations

There were many limitations which were faced during the research. Firstly, it is important to inform that the concept of MASS is in the evolving phase and most of the people were unaware of this concept. Secondly, there is no historical data available online related to the incidents of MASS or case studies. Therefore, to overcome the first issue, researcher had to develop two scenarios for the ease of the respondents. The response of participants was totally based upon their own perception, professional attitude and one-side knowledge of their field. However, the two scenarios definitely helped them in understanding MASS and filling the survey form with good knowledge. Thirdly, due to nature of the topic and less knowledge about MASS, participation level was affected. Lastly, many of the experts haven’t replied to the emails and obtaining physical access was very difficult. Nevertheless, this research will add great value in the areas as mentioned above. Further, the limitations should be overcome through additional research in the future.

Chapter 6 – Conclusion

6.1 Conclusion

During the research, researcher has done quantitative analysis based on the survey form to answer the two research questions. The conclusion of research questions (RQs) after carrying out detailed analysis and data processing is as under:

RQ-1*: What are the different security threats and challenges to MASS in different maritime zones and its impact on maritime security?*

The outcome of the research shows that there will be two major threats to MASS which are Cyber-attacks and physical attacks (hijacking, piracy and control of SCC). They will pose a distinct impact on maritime security in future. The conventional piracy activity may face downfall because of the new design feature of MASS along with the limited expertise of traditional pirates in the field of technology with less bargaining ability to protect monetary gains. However, this shouldn't be entirely anticipated. The risk of cyber and piracy cannot be ruled out or be entirely diminished. There may be more efforts by pirates to physically board unmanned MASS (Level 3 and 4) or NSA's group physically attacking SCC. Above all, cyber-attacks attempts by hackers occur on both MASS and SCC in a much larger quantity which become a major risk for the maritime security. To avoid severe consequences of above said threats in future, MASS/SCC are to be effectively managed and maritime authorities should focus on finding some solid solutions.

NSA's group on land may explore different options by hiring terrorists and employing technical persons (hackers) to attack SCC/MASS physically. Through cyber-attack, international trade will be disrupted as it will be a multi-mode attack (cyber followed by physical attack). Criminals may also practice jamming techniques to interrupt GNSS and AIS signals which may require a detailed consideration. Furthermore to confuse MASS, cyber-attackers may also use spoofing technique. Therefore, AI systems must be technologically advanced so that they can identify/detect such anomalies immediately and take remedial actions and generate responses. SCCs are considered as the main hub for MASS operations and is a soft as well as vulnerable target for both NSA's groups and hackers. Hence, it requires special attention to protect against physical and cyber-attacks. In case of any infiltration in SCC, infiltrator will have the entire control of MASS. The communication system (Satellite) between MASS/SCC can also be targeted through hackers. In addition, human element may be transformed/shifted from ship to shore which still impact the security aspects of maritime sector.

Notwithstanding with all the concerns, there are a lot of possibilities and chances of improvement in the field of maritime security as MASS is considered as complex and costly system. Therefore, investment should be done by only serious owners and operators who are more concerned about the security aspect.

Mitigation strategy along with the impact of MASS on maritime security should be addressed. This will be done through coordination of highest level and cooperation among those stakeholders which are involved in this field especially the flag states, coastal states, SCCs, the ship owners, manufacturers, operators, the port facilities and LEAs. In order to evaluate the security aspect, there is a dire need to understand what kind of remote control crafts are being operated at sea and a uniform coordinated methodology is to be adopted.

Overall, the wide range of onsite security measures include motion detectors, heat sensors, camera and alarms. The difficulty in accessibility of MASS would definitely turn as mitigation measures to notice pirates and prevent from any infiltration physically. To prevent from cyber-attacks, different measures include strong password protected systems, safe and secure communication, capability of dealing any cyber-attack, train operators, conduct of cyber drills and regularly upgrade the network systems. In the above said measures, the role of manufactures along with the SCC staff especially operator is very important. Moreover, the responsibility shifts from seafarers to authorities on shore. Therefore, an effective, efficient and prompt maritime security and law enforcement by port authorities, coastal states and LEA's is required to avert incidents onboard MASS.

***RQ-2**: What is the role of law enforcement authorities in order to address the security threats and challenges related to MASS?*

The analysis revealed that the role of LEA's must be enhanced to ensure security of MASS especially in coastal waters as well as open seas and to deal with operations of MASS's implications on maritime security. It is expected that MASS will lead some new challenges for the coastal states, port authorities, and LEA's in order to manage maritime security inside their operational regions. In future, there are chances in shifting of responsibilities where the role of SCC's operators would also become limited due to bad situational awareness. Therefore, substantial necessity may exist in upgrading the technological capability onboard law enforcement platforms (ships), to cooperate and handle or in some situations control MASS. VBSS operations in future may also be affected, and become difficult to undertake on MASS. This will be due to access restraints and no crew onboard. However, in some circumstances and situations, desired requirements need to be fulfilled. This will occur when MASS is being used against sensitive installations, collusion with warships/commercial ships, blocking of port entrances and conduct of terrorist activity by exploding MASS inside port, and an illicit activity for which there is a need of making procedures and protocols. Bilateral agreements must be done with those coastal states which are also employing MASS. Therefore, for smooth conduct of operations and handling of bad situations, there is a dire need for agencies to uphold great level of cooperation and coordination with numerous stakeholders like manufacturers, coastal state, flag state, port authorities and operators.

For future and days to come, research struggles may be focused towards a specific scenario (cyber or physical). Security risk assessment of SCC and MASS may be done using requisite tools as both of these have a meaningfully effect on security of maritime domain. The other important point is responsibilities plan and procedures related to deal such incidents (manufacturer, flag state, coastal state, LEA's).

References

Akpan, F.; Bendiab, G.; Shiaeles, S.; Karamperidis, S.; Michaloliakos, M. (2022). Cybersecurity Challenges in the Maritime Sector. *Network,*2, 123–138. https://doi.org/10.3390/network2010009

Allianz. (2021). Safety and Shipping. Review 2021. Retrieved from https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/AGCS-Safety-Shipping-Review-2021.pdf

Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures*, 46, pp. 23-40.

Andritsos, F. (2013). EU port security & growth. Paper presented at the Proceedings of the 8th Future Security Research Conference, pp. 267-274.

Attard, F. (2014). IMO's contribution to international law regulating maritime security. *Journal of Maritime Law and Commerce*, 45, p. 479.

BIMCO, ICS, IGP & I Clubs, INTERTANKO and OCIMF, (2018). Best Management Practices to Deter Piracy and Enhance Maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea. Retrieved from https://www.ukmto.org/-/media/ukmto/images/indian-ocean/bmp5-small.pdf?la=en-gb&rev=bc56aec5752140b0a8864f81cf9558cf&hash=13CCC986C8FE9F99D8D63B86618DFDF9

Bolbot, V., Theotokatos, G., Boulougouris, E., & Vassalos, D. (2019). Safety related cyber-attacks identification and assessment for autonomous inland ships. Paper presented at the International Seminar on Safety and Security of Autonomous Vessels (ISSAV).

Callum, O. B. (2018). Key advantages and disadvantages of ship autonomy. Retrieved from https://safety4sea.com/key-advantages-and-disadvantages-of-ship-autonomy/

Carey, L. (2017). All hands off deck? The legal barriers to autonomous ships. NUS Law Working Paper No. 2017/011.

Chae, C.-J., Kim, M., & Kim, H.-J. (2020). A Study on Identification of Development Status of MASS Technologies and Directions of Improvement. *Applied Sciences*, 10(13), 4564. https://doi.org/10.3390/app10134564

China Classification Society. (2015). Rules for Intelligent Ships. Retrieved from https://www.ccs.org.cn/ccswzen/file/download?fileid=201950000000000607

Cook, P. (2020). Comment: The emerging spectrum of maritime security. International *Journal of Maritime Crime & Security (IJMCS)*, 1(1), 30-55.

Creswell, J. W. (2021). *A concise introduction to mixed methods research*. SAGE publications.

Cyberstar. (2022). How Bad Was Maritime Cyber Security in 2021? Consider These 8 Incidents. https://www.zkcyberstar.com/2022/03/15/how-bad-was-maritime-cyber-security-in-2021-consider-these-8-incidents/#:~:text=On%20the%20cyber%20security%20front,and%20port%20systems%20in%202020

de Klerk, Y., Manuel, M. E., & Kitada, M. (2021). Scenario planning for an autonomous future: A comparative analysis of national preparedness of selected countries, *Marine Policy*, 127, 104428.

Emad, G. R., Khabir, M., & Shahbakhsh, M. (2020). Shipping 4.0 and training seafarers for the future autonomous and unmanned ships. Paper presented at the Proceedings of the 21th Marine Industries Conference (MIC2019), Qeshm Island, Iran, 1-2.

EMERJ. (2022). Autonomous Ships Timeline – Comparing Rolls-Royce, Kongsberg, Yara and More. Retrieved from https://emerj.com/ai-adoption-timelines/autonomous-ships-timeline/

Eriksson, A., & Gevriye, S. (2018). The biggest challenges with autonomous costal ferries and the benefits with sailing autonomous. Retrieved from https://publications.lib.chalmers.se/records/fulltext/255986/255986.pdf

Fan, C., Wróbel, K., Montewka, J., Gil, M., Wan, C., & Zhang, D. (2020). A framework to identify factors influencing navigational risk for Maritime Autonomous Surface Ships. *Ocean Engineering*, 202, 107188.

Felski, A., & Zwolak, K. (2020). The ocean-going autonomous ship—Challenges and threats. *Journal of Marine Science and Engineering*, 8(1), 41.

Fraunhofer. (2015). Practice Solutions at MUNIN Final Event Introduced. Retrieved from https://www.cml.fraunhofer.de/content/dam/cml/en/documents/PressReleases/Press%20Release%20MUNIN%20Final%20Event_EN.pdf

Galani, S., & Evans, M. D. (2020). *The interplay between maritime security and the 1982 United Nations Convention on the Law of the Sea: help or hindrance? Maritime Security and the Law of the Sea*, Edward Elgar Publishing.

Galdorisi, G. (2022). Employing unmanned surface vehicles to guard ports and harbours. Retrieved from https://cimsec.org/employing-unmanned-surface-vehicles-to-guard-ports-and-harbors/

Guilfoyle, D. (2017). Maritime Law Enforcement Operations and Intelligence in an Age of Maritime Security. Retrieved from https://digital-commons.usnwc.edu/ils/vol93/iss1/11/

Heikkilä, E. (2018). AI for Autonomous Ships: Challenges in Design and Validation. Paper presented at the International Seminar on Safety and Security of Autonomous Vessels, ISSAV 2018,

Herbert-Burns, R., Bateman, S., & Lehr, P. (2019). *Lloyd's MIU handbook of maritime security*. Auerbach Publications.

Honekamp, W. (2018). Electronic navigation challenges for autonomous ships. *Mobility in a Globalised World*, 19, 211.

IMO. (2017a). Maritime cyber risk. https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

IMO. (2017b). Facilitation Committee and Maritime Safety Committee. Guidelines on maritime cyber risk management (MSC-FAL.1/Circ.3, 5.7.2017).

IMO. (2018a). Working group report in 100th session of IMO Maritime Safety Committee for the regulatory scoping exercise for the use of maritime autonomous surface ships (MASS). Maritime Safety Committee 100th session MSC 100/ WP.8..

IMO. (2018b). Regulatory Scoping Exercise for the Use of Maritime Autonomous Surface Ships (MASS); Maritime Safety Committee 99/WP.9; IMO: London, UK.

IMO. (2021a). The International Ship and Port Facility (ISPS) Code. https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

IMO. (2021b). Outcome of the regulatory scoping exercise for the use of maritime autonomous surface ships (MASS) Maritime Safety Committee.1/Circ.1638.

IMO. (2022). Autonomous Shipping https://www.imo.org/en/MediaCentre/HotTopics/Pages/Autonomous-shipping.aspx

Innovation News network. (2020). The benefits of autonomous shipping technologies. https://www.innovationnewsnetwork.com/the-benefits-of-autonomous-shipping-technologies/6531/

International Chamber of Shipping. (2021). Shipping and new technologies https://www.ics-shipping.org/shipping-fact/shipping-and-new-technologies/

International Maritime Organization (IMO), (2017d). Resolution MSC-FAL.1/Circ.3. Guidelines on Maritime Cyber Risk Management; *International Maritime Organization: London*, UK, 2017.

International Maritime Organization (IMO), Maritime Safety Committee, (2017c). Maritime Cyber Risk Management in Safety Management Systems (Resolution MSC. 428 (98)).

International Maritime Organization (IMO), Maritime Safety Committee, 2017b. Maritime Cyber Risk Management in Safety Management Systems (Resolution MSC. 428 (98)).

Jiang, M., & Lu, J. (2020). The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. Transportation Research Part E: *Logistics and Transportation Review*, 139, 101965.

Kavallieratos, G., Diamantopoulou, V., & Katsikas, S. K. (2020). Shipping 4.0: Security requirements for the cyber-enabled ship. *IEEE Transactions on Industrial Informatics*, 16(10), 6617-6625.

Kim, T., & Mallam, S. (2020). A Delphi-AHP study on STCW leadership competence in the age of autonomous maritime operations. *WMU Journal of Maritime Affairs*, 19, 163-181.

Kim, Y., & Cha, S. (2012). Threat scenario-based security risk analysis using use case modeling in information systems. *Security and Communication Networks*, 5(3), 293-300.

Klein, N. (2011). *Maritime Security and the Law of the Sea*. Oxford University Press.

Klein, N. (2019). Maritime Autonomous Vehicles within the International Law Framework to Enhance Maritime Security. *International Law Studies*, 95(1), 8.

Komianos, A. (2018). The autonomous shipping era. operational, regulatory, and quality challenges. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 12(2).

Kretschmann, L., Burmeister, H., & Jahn, C. (2017). Analyzing the economic benefit of unmanned autonomous ships: An exploratory cost-comparison between an autonomous and a conventional bulk carrier. *Research in Transportation Business & Management*, 25, 76-86.

Kumar, R. (2018). *Research methodology: A step-by-step guide for beginners*. Sage.

Kunz, M., & Ó hÉigeartaigh, S. (2020). *Artificial Intelligence and Robotization*. Robin Geiß and Nils Melzer (Eds.), Oxford Handbook on the International Law of Global Security (Oxford University Press, Forthcoming).

Kutsuna, K., Ando, H., Nakashima, T., Kuwahara, S., & Nakamura, S. (2019). NYK's approach for autonomous navigation–structure of action planning system and demonstration experiments. Paper presented at the *Journal of Physics: Conference Series*,1357(1) 012013.

Laurinen, M. (2016). *Remote and Autonomous Ships: The Next Steps; AAWA: Advanced Autonomous Waterborne Applications*: London, UK.

Li, S., & Fung, K. S. (2019). Maritime autonomous surface ships (MASS): implementation and legal issues. Maritime Business Review, 4(4).

https://www.emerald.com/insight/content/doi/10.1108/MABR-01-2019-0006/full/html

Lloyd’s Register Group Services Limited. (2016). Cyber-enabled ships ShipRight Procedure. LR defines 'autonomy levels' for ship design and operation. Retrieved from https://www.lr.org/en/latest-news/lr-defines-autonomy-levels-for-ship-design-and-operation/

Maritime Executive. (2020). SBS Boarding Team Detains Stowaways After Confrontation Aboard Tanker. Retrieved from https://www.maritime-executive.com/article/sbs-boarding-team-detains-stowaways-after-confrontation-aboard-tanker

Metaparti, P. (2010). Rhetoric, rationality and reality in post-9/11 maritime security. *Maritime Policy & Management*, 37(7), 723-736.

Munim, Z. H. (2019). Autonomous ships: a review, innovative applications and future maritime business models. Paper presented at the *Supply Chain Forum: An International Journal*, 20(4) 266-279.

MUNIN. (2016). Research in maritime autonomous systems project results and technology potentials (final brochure). & nbsp; Retrieved from http://www.unmannedship.org/munin/wp-content/uploads/2016/02/MUNIN-final-brochure.pdf.

NY Times. (2022). Suez Canal Blocked After Giant Container Ship Gets Stuck. Retrieved from https://www.nytimes.com/2021/03/24/world/middleeast/suez-canal-blocked-ship.html

Osinuga, D. (2020). Unmanned ships: Coping in the murky waters of traditional maritime law. *Poredbeno Pomorsko Pravo*, 59(174), pp. 75-105.

Porathe, T., Hoem, Å, Rødseth, Ø, Fjørtoft, K., & Johnsen, S. O. (2018). At least as safe as manned shipping? Autonomous shipping, safety and “human error”. *Safety and Reliability–Safe Societies in a Changing World*, (pp. 417-425). CRC Press.

Progoulakis, I.; Nikitakos, N.; Dalaklis, D. & Yaacob, R. (2022). Cyber-physical security for ports infrastructure. Conference: *The International Maritime and Logistics Conference “Marlog 11”At: Alexandria-Egypt*, Volume: ISBN: 987-977-85808-5-3

Progoulakis, I. & Nikitakos, N. (2019). Risk Assessment Framework for the Security of Offshore Oil and Gas Assets. Conference: IAME 2019 conference.

Roberts, F. S., Egan, D., Nelson, C., & Whytlaw, R. (2019). Combined cyber and physical attacks on the maritime transportation system. NMIOTC Maritime Interdiction Operations Journal, Retrieved from https://par.nsf.gov/servlets/purl/10166239.

Rødseth, J.O. & Nordahl, H. (2017). Definitions for Autonomous Merchant Ships. Retrieved from https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/autonom-defs.pdf

Rødseth, Ø J. (2018). *Assessing business cases for autonomous and unmanned ships. Technology and Science for the Ships of the Future* (pp. 1033-1041). IOS Press.

Rødseth, Ø J., & Burmeister, H. C. (2012). Developments toward the unmanned ship. Paper presented at the *Proceedings of International Symposium Information on Ships–ISIS*, 201 30-31.

Rødseth, Ø J., Wennersberg, L. A. L., & Nordahl, H. (2021). Towards approval of autonomous ship systems by their operational envelope. *Journal of Marine Science and Technology*,1-10.

Rødseth, Ø. (2017). *Towards Shipping 4.0. Proceedings of Smart Ship Technology;* Royal Institution of Naval Architects: London, UK.

Rothblum, A. M. (2006). Human error and marine safety. Volume 4 in U.S. Coast Guard Risk-Based Decision-Making Guidelines. U.S. Coast Guard Research and Development Center.

Rylander, R., & Man, Y. (2016). Autonomous safety on vessels. Lighthouse Swedish Maritime Competence Centre. Retrieved from https://lighthouse-prod.hawco1.se/wp-content/uploads/2021/06/autonomous_safety_on_vessels_-_webb.pdf

Safety4sea. (2018). Maersk Line: Surviving from a cyber-attack. Retrieved from https://safety4sea.com/cm-maersk-line-surviving-from-a-cyber-attack/

Sakhi, F. E., Allal, A. A., Mansouri, K., & Qbadou, M. (2019). Determination of merchant ships that most likely to be autonomously operated. Paper presented at the 2019 1st International Conference on Smart Systems and Data Science (ICSSD), 1-5.

Seif, H.G.; Hu, X. (2016). Autonomous Driving in the City—HD Maps as a Key Challenge of the Automotive Industry. *Engineering*, 2, 159–162.

Şenol, Y., Gökçek, V., & Seyhan, A. (2017). SWOT-AHP Analysis of Autonomous Shipping. Paper presented at the 4th International Multidisciplinary Congress of Eurasia Proceedings, 2; 58-69.

ShipInsight, (2019). What are the benefits of adopting autonomy technology for the maritime industry. Retrieved from https://shipinsight.com/articles/what-are-the-benefits-of-adopting-autonomy-technology-for-the-maritime-industry

Star, J., Rowland, E. L., Black, M. E., Enquist, C. A., Garfin, G., Hoffman, C. H., Hartmann, H., Jacobs, K. L., Moss, R. H., & Waple, A. M. (2016). Supporting adaptation decisions through scenario planning: Enabling the effective use of multiple methods. *Climate Risk Management*, 13, 88-94.

Szelangiewicz, T., & Żelazny, K. (2020). Unmanned ships–maritime transport of the 21st century. Scientific journals of the Maritime University of Szczecin, 64(136), pp. 14-21.

Tam, K., & Jones, K. (2018). Cyber-risk assessment for autonomous ships. Paper presented at the 2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security), 1-8.

Tumbarska, A. (2018). Maritime Piracy and Armed Robbery Evolution in 2008-2017. *Security & Future*, 2(1), 18-21.

UNCTAD. (2018). Review of maritime transport. Geneva: UNCTAD Secretariat. Geneva-New York. Retrieved from https://unctad.org/system/files/official-document/rmt2018_en.pdf

UNCTAD. (2020). Review of maritime transport. (Geneva: UNCTAD secretariat. Geneva-New York.). Retrieved from https://unctad.org/system/files/official-document/rmt2020_en.pd

Utne, I.B., Sørensen, A.J., Schjølberg, I. (2017). Risk Management of Autonomous Marine Systems and Operations. In Proceedings of the 36th *International Conference on Ocean, O_shore and Arctic Engineering, American Society of Mechanical Engineers Digital Collection*, Trondheim, Norway, 25–30 June 2017.

Van Hooydonk, E. (2014). The law of unmanned merchant shipping–an exploration. *The Journal of International Maritime Law*, 20(3), 403-423.

Verschuren, P., Doorewaard, H., & Mellion, M. (2010). *Designing a research project*. Eleven International Publishing The Hague.

Vinnem, J. E., & Utne, I. B. (2018). Risk from cyberattacks on autonomous ships. *Safety and Reliability-Safe Societies in a Changing World*, CRC Press.

Wariishi, K. (2019). Maritime Autonomous Surface Ships: Development Trends and Prospects-how Digitalization Drives Changes in Maritime Industry. Mitsui & Co.Global Strategic Studies Institute.

World Maritime University. (2019). Transport 2040: Autonomous ships: A new paradigm for Norwegian shipping - Technology and transformation. World Maritime University, Malmö.

Wróbel, K., Gil, M., & Montewka, J. (2020). Identifying research directions of a remotely-controlled merchant ship by revisiting her system-theoretic safety control structure. *Safety Science*, 129, 104797.

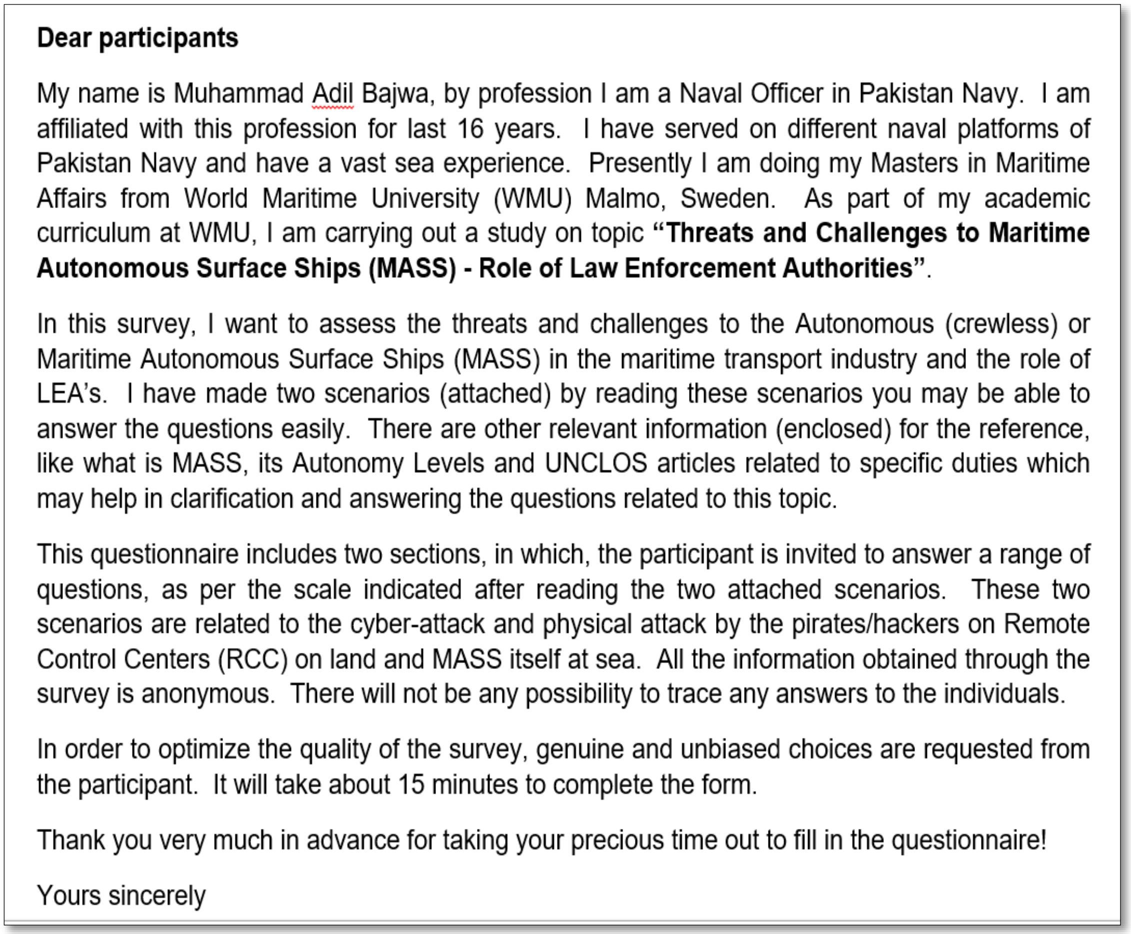
Wróbel, K.; Montewka, J.; Kujala, P. (2017). Towards the assessment of potential impact of unmanned vessels on maritime transportation safety. Reliability engineering & system safety,165, 155–169.

Zhou, X., Liu, Z., Wang, F., & Wu, Z. (2021). A system-theoretic approach to safety and security co-analysis of autonomous ships. *Ocean Engineering*, 222, 108569.

Zhou, X., WU, Z., WANG, F., & LIU, Z. (2019). Definition of autonomous ship and its autonomy level. *Jiaotong Yunshu Gongcheng Xuebao/Journal of Traffic and Transportation Engineering,* 19, 149-162.

Appendix A

Survey Questionnaire



Dear participants

My name is Muhammad Adil Bajwa, by profession I am a Naval Officer in Pakistan Navy. I am affiliated with this profession for last 16 years. I have served on different naval platforms of Pakistan Navy and have a vast sea experience. Presently I am doing my Masters in Maritime Affairs from World Maritime University (WMU) Malmo, Sweden. As part of my academic curriculum at WMU, I am carrying out a study on topic **"Threats and Challenges to Maritime Autonomous Surface Ships (MASS) - Role of Law Enforcement Authorities"**.

In this survey, I want to assess the threats and challenges to the Autonomous (crewless) or Maritime Autonomous Surface Ships (MASS) in the maritime transport industry and the role of LEA's. I have made two scenarios (attached) by reading these scenarios you may be able to answer the questions easily. There are other relevant information (enclosed) for the reference, like what is MASS, its Autonomy Levels and UNCLOS articles related to specific duties which may help in clarification and answering the questions related to this topic.

This questionnaire includes two sections, in which, the participant is invited to answer a range of questions, as per the scale indicated after reading the two attached scenarios. These two scenarios are related to the cyber-attack and physical attack by the pirates/hackers on Remote Control Centers (RCC) on land and MASS itself at sea. All the information obtained through the survey is anonymous. There will not be any possibility to trace any answers to the individuals.

In order to optimize the quality of the survey, genuine and unbiased choices are requested from the participant. It will take about 15 minutes to complete the form.

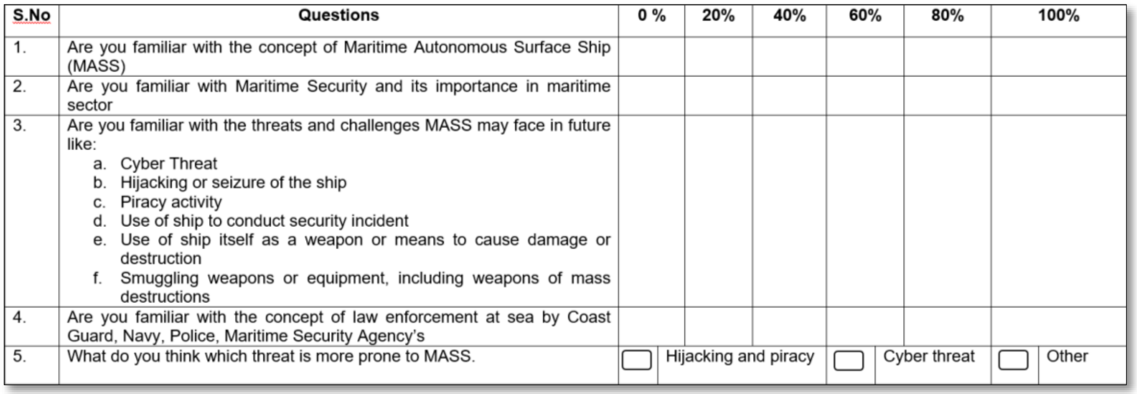
Thank you very much in advance for taking your precious time out to fill in the questionnaire!

Yours sincerely

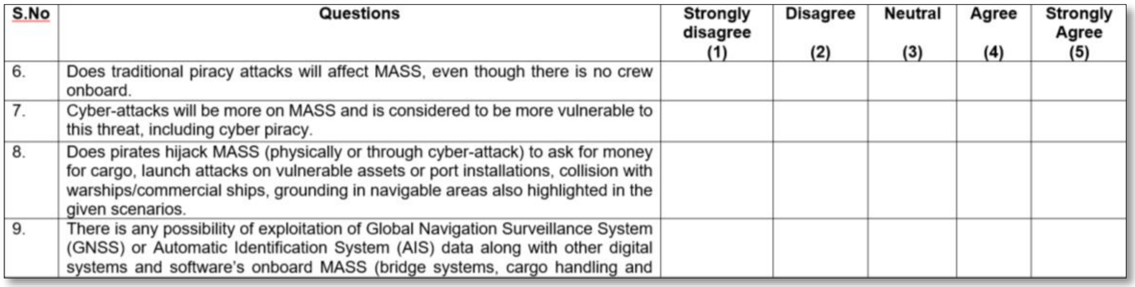
Section – I

Name (Optional)	□															
Nationality	□															
Gender	□	Male	□	Female	□	Preferred not to say										
Age	□	25 years	□	26-35 years	□	36-45 years	□	46-55 years	□	56-65 years	□	Over 66 years				
Job	□	Maritime Administration	□	Maritime Expert	□	Maritime Academician	□	Navy/Police/ Coast Guard/MSA	□	Seafarer	□	Other				
Position	□	Top Manager	□	Middle Manager	□	Master	□	Professor/ Researchers	□	Senior officer	□	Junior officer	□	Deck Officer	□	Others
Experience	□	Less than 5 years	□	5-10 years	□	11-15 years	□	16-20 years	□	Over 20 years						

Section – II



S.No	Questions	0 %	20%	40%	60%	80%	100%
1.	Are you familiar with the concept of Maritime Autonomous Surface Ship (MASS)						
2.	Are you familiar with Maritime Security and its importance in maritime sector						
3.	Are you familiar with the threats and challenges MASS may face in future like: a. Cyber Threat b. Hijacking or seizure of the ship c. Piracy activity d. Use of ship to conduct security incident e. Use of ship itself as a weapon or means to cause damage or destruction f. Smuggling weapons or equipment, including weapons of mass destructions						
4.	Are you familiar with the concept of law enforcement at sea by Coast Guard, Navy, Police, Maritime Security Agency's						
5.	What do you think which threat is more prone to MASS.	□	Hijacking and piracy	□	Cyber threat	□	Other

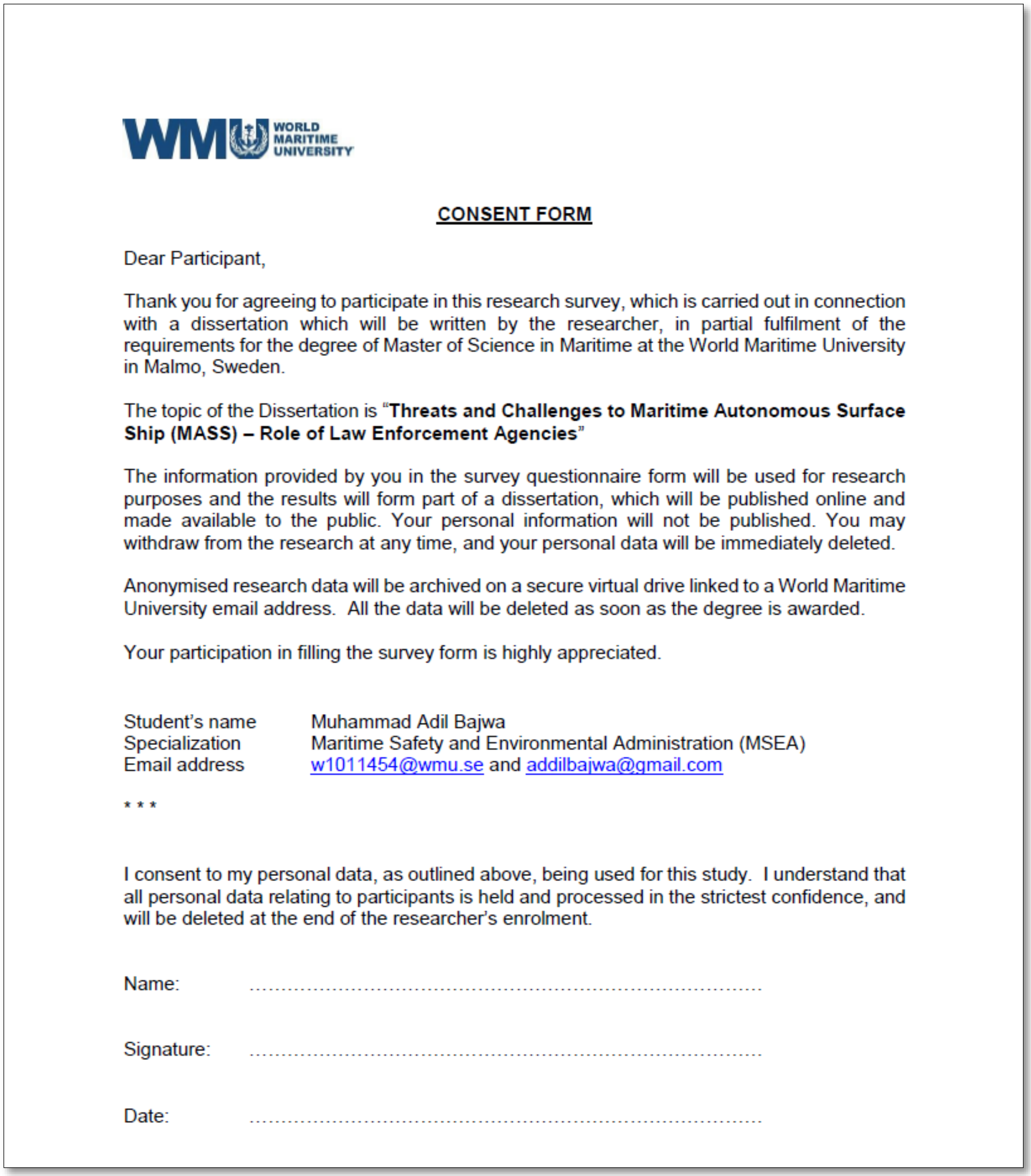


S.No	Questions	Strongly disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)
6.	Does traditional piracy attacks will affect MASS, even though there is no crew onboard.					
7.	Cyber-attacks will be more on MASS and is considered to be more vulnerable to this threat, including cyber piracy.					
8.	Does pirates hijack MASS (physically or through cyber-attack) to ask for money for cargo, launch attacks on vulnerable assets or port installations, collision with warships/commercial ships, grounding in navigable areas also highlighted in the given scenarios.					
9.	There is any possibility of exploitation of Global Navigation Surveillance System (GNSS) or Automatic Identification System (AIS) data along with other digital systems and software's onboard MASS (bridge systems, cargo handling and					

6.	Does traditional piracy attacks will affect MASS, even though there is no crew onboard.					
7.	Cyber-attacks will be more on MASS and is considered to be more vulnerable to this threat, including cyber piracy.					
8.	Does pirates hijack MASS (physically or through cyber-attack) to ask for money for cargo, launch attacks on vulnerable assets or port installations, collision with warships/commercial ships, grounding in navigable areas also highlighted in the given scenarios.					
9.	There is any possibility of exploitation of Global Navigation Surveillance System (GNSS) or Automatic Identification System (AIS) data along with other digital systems and software's onboard MASS (bridge systems, cargo handling and management systems, machinery and propulsion systems, control systems, passenger servicing and management systems, passenger public networks, crew welfare systems, and communication systems)					
10.	Does non-state actors use MASS as a weapon to attack sensitive installations/ places/ assets of any country (warships, port or coastline installations etc. see both the scenarios outcome)					
11.	Cyber security threat considered as higher than the physical attack by pirates on MASS					
12.	There is a risk that crewless MASS may also pose threat to the security of other conventional ships at sea or harbor.					
13.	There are high possibilities of MASS being hijacked and used by criminals for international organized crimes.					
14.	The ship's security may be weakened on crewless MASS under the ISPS code.					
15.	Shore Control Centers (SCC) on land are more vulnerable to cyber-attacks which includes the Communication and networking infrastructure of MASS (See Scenario II).					
16.	Shore Control Centers (SCC) may came under attack by the Non-state actors and use MASS as a weapon against sensitive targets (See Scenario II).					
17	Law Enforcement Authorities are capable to handle situations after physical and cyber-attack has been done on MASS/ SCC as mentioned in the given two scenarios					
18.	The employment of MASS may present new challenges for maritime law enforcement organizations (such as Coast Guard, Navy, Police, Maritime Security Agency)					
19.	The acceptance of MASS in shipping industry will considerably influence law enforcement authorities use of Visit Board Search and Seizure (VBSS)					
20.	Inspection of MASS at sea along with document verification during VBSS may require alternate measures/arrangements					
21.	VBSS operation onboard crewless MASS may cause challenge for law enforcement authorities.					
22.	Is there any requirement for possible change in maritime interdiction/ boarding (VBSS) procedures involving MASS					
23.	Enhancement of maritime security in MASS era is unavoidable					

Appendix B

Consent Form



WMU WORLD MARITIME UNIVERSITY

CONSENT FORM

Dear Participant,

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

The topic of the Dissertation is "**Threats and Challenges to Maritime Autonomous Surface Ship (MASS) – Role of Law Enforcement Agencies**"

The information provided by you in the survey questionnaire form will be used for research purposes and the results will form part of a dissertation, which will be published online and made available to the public. Your personal information will not be published. You may withdraw from the research at any time, and your personal data will be immediately deleted.

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

Your participation in filling the survey form is highly appreciated.

Student's name	Muhammad Adil Bajwa
Specialization	Maritime Safety and Environmental Administration (MSEA)
Email address	w1011454@wmu.se and addilbajwa@gmail.com

* * *

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

Name: ....

Signature: ....

Date: ....

Appendix C

Scenario – 1 (Cyber Attack)

Situation. Shore Control Center (SCC) which is established on land is operating/monitoring several Autonomous Ships which are operating at sea. This SCC is considered as the heart of (command center) the ship's operations. SCC is capable of communicating, controlling and maneuvering ship movement, building the situational awareness and planning the routes of the MASS. Everything is being controlled through Information Communication Technology (ICT). This SCC is under cyber-attack by an unknown hacker and the entire control is now in the hands of that hacker.

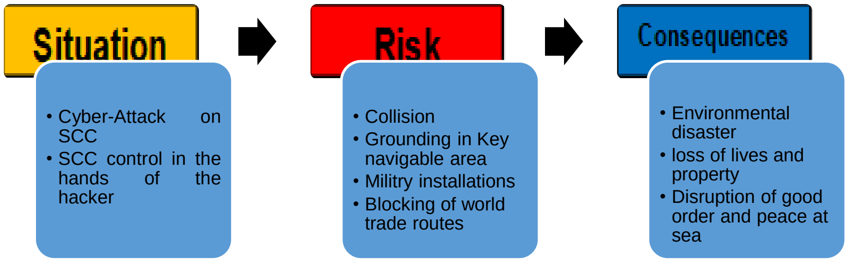
Development in the Situation. Once the hacker gets the control of the SCC without physical interference only through cyber-attack due to which he is in a position to maneuver and control the MASS operations. It's now his choice where to divert that MASS. We must also consider that, the hacker is a professional hacker and he may have some demands like money/ransom or some other political agenda from the government or from the flag state.

Outcome. Following may be envisaged:

a. The hacker directs MASS toward vital military installation/ships in the port.
b. The hacker directs MASS towards vital cargo vessel for collision.
c. The hacker directs MASS towards grounding and blocking the channels.
d. The hacker directs MASS towards oil carrier for environmental pollution.
e. The hacker directs MASS towards the critical points/areas like (Malacca Strait, Strait of Hormuz, Suez canal etc.) of the world trade routes and block that points/ areas by grounding and collision.
f. The hacker directs MASS towards the other country port and explode that vessel.
g. The hacker uses MASS as a bargaining chip and ask for ransom.
h. The hacker uses MASS itself as a weapon of mass destruction.

Role. Here comes the role of under mentioned organs:

a. Flag State
b. Manufacturer
c. Law Enforcement Agencies


Situation
• Cyber-Attack on SCC
• SCC control in the hands of the hacker
Risk
• Collision
• Grounding in Key navigable area
• Militry installations
• Blocking of world trade routes
Consequences
• Environmental disaster
• loss of lives and property
• Disruption of good order and peace at sea

Scenario – 2 (Physical Attack)

Situation. According to IMO's degree/levels of automation (IMO, 2018) in which at level 3 and 4 there will be no men onboard MASS. It will be controlled from Shore Control Center (SCC) which is established on land. SCC is responsible to control and monitor several Autonomous Ships which are being operating at sea. This SCC is considered as the heart of the ship's operations. SCC is capable of communicating, controlling and maneuvering ship movement along with observing situation of the sea and planning the routes of the ship. SCC being the central hub, its security is paramount. Therefore, a banned non-state actor group plans and undertakes invasion of the SCC to attack any military installations in the area, government installation on shore, blocking the port entrances and carryout collision incident with other commercial ships at sea. This SCC came under attack physically.

Development in the Situation. Upon taking physical control of the SCC and making the personnel hostage. The entire ship control is in the hands of those non state actor's/group. This group use the same personnel to maneuver MASS in the direction where they want. As these personal are hostages and they are force to obey the instructions of that group.

Outcome. Following may be envisaged:

a. The group directs MASS toward vital military installation/ships in the port.

b. The group directs MASS towards vital cargo vessel for collision.

c. The group directs MASS towards grounding and blocking the channel.

d. The group directs MASS towards oil carrier for environmental pollution.

e. The group directs MASS towards the critical points/areas like (Malacca Strait, Strait of Hormuz, Suez Canal etc.) of the world trade and block that points/ areas by grounding and collision.

f. The group directs MASS towards the other country's port and explodes that vessel.

g. The group uses that MASS as a bargaining chip to free their men or for ransom.

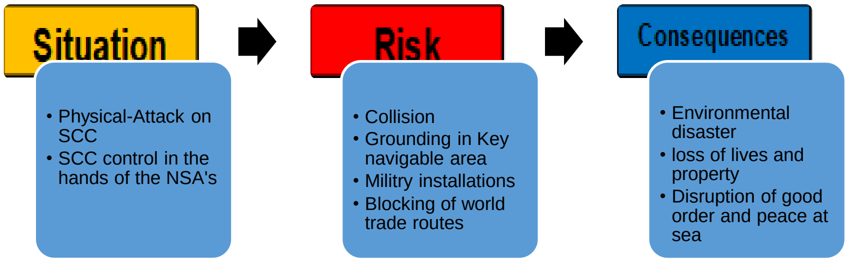
h. The group uses MASS itself as a weapon of mass destruction.

Role. Here comes the role of under mentioned organs:

a. Flag State

b. Manufacturer

c. Law Enforcement Agencies



Situation

- Physical-Attack on SCC
- SCC control in the hands of the NSA's

Risk

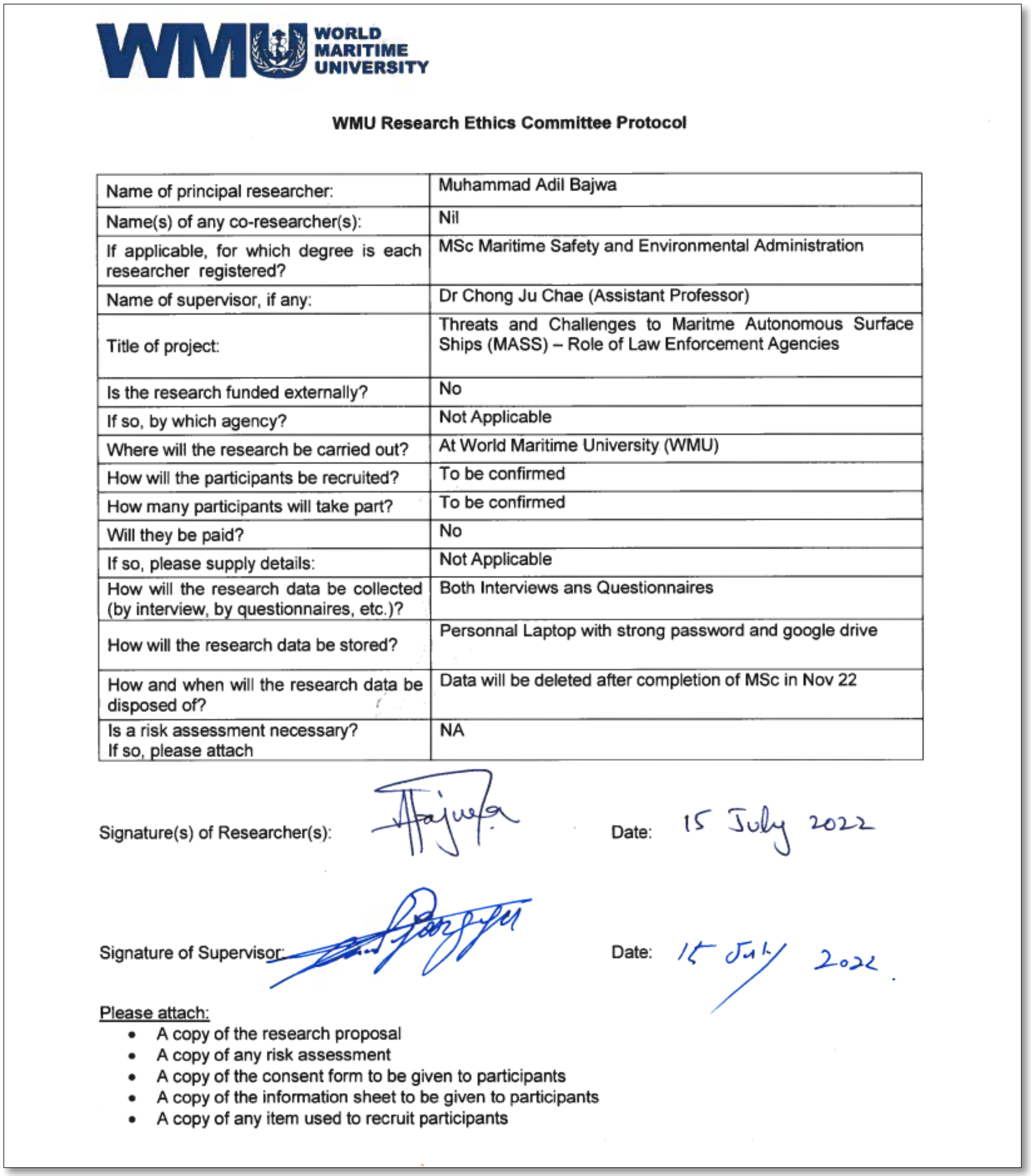
- Collision
- Grounding in Key navigable area
- Militry installations
- Blocking of world trade routes

Consequences

- Environmental disaster
- loss of lives and property
- Disruption of good order and peace at sea

Appendix D

WMU Research Ethics Committee Protocol



WMU WORLD MARITIME UNIVERSITY

WMU Research Ethics Committee Protocol

Name of principal researcher:	Muhammad Adil Bajwa
Name(s) of any co-researcher(s):	Nil
If applicable, for which degree is each researcher registered?	MSc Maritime Safety and Environmental Administration
Name of supervisor, if any:	Dr Chong Ju Chae (Assistant Professor)
Title of project:	Threats and Challenges to Maritme Autonomous Surface Ships (MASS) – Role of Law Enforcement Agencies
Is the research funded externally?	No
If so, by which agency?	Not Applicable
Where will the research be carried out?	At World Maritime University (WMU)
How will the participants be recruited?	To be confirmed
How many participants will take part?	To be confirmed
Will they be paid?	No
If so, please supply details:	Not Applicable
How will the research data be collected (by interview, by questionnaires, etc.)?	Both Interviews ans Questionnaires
How will the research data be stored?	Personnal Laptop with strong password and google drive
How and when will the research data be disposed of?	Data will be deleted after completion of MSc in Nov 22
Is a risk assessment necessary? If so, please attach	NA

Signature(s) of Researcher(s): Date: 15 July 2022

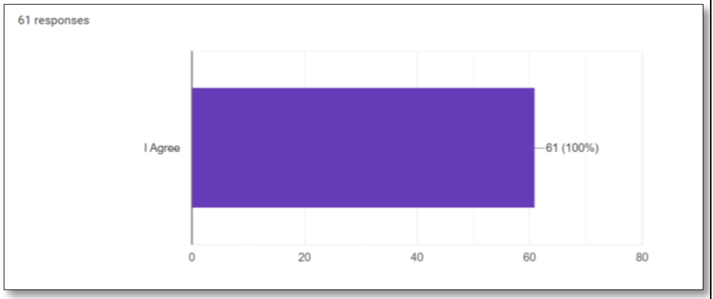
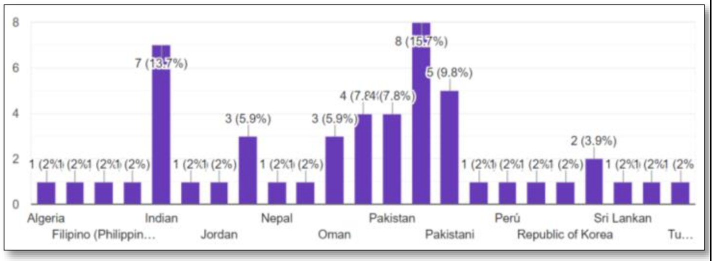
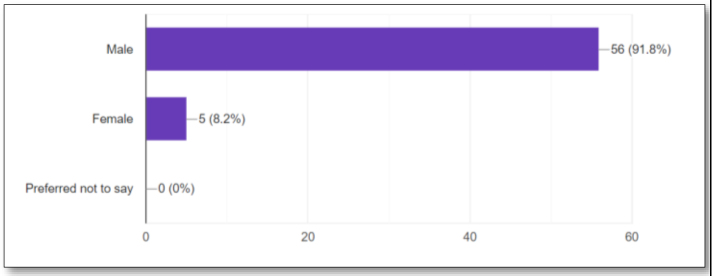
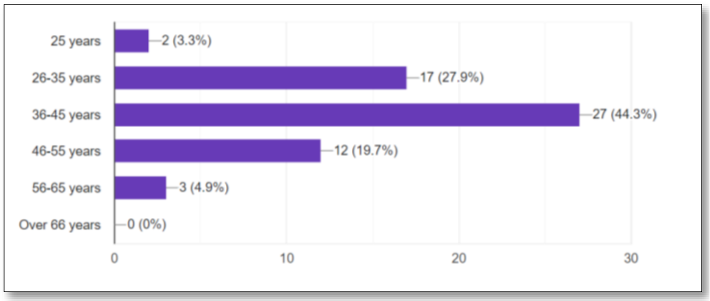
Signature of Supervisor: Date: 15 July 2022.

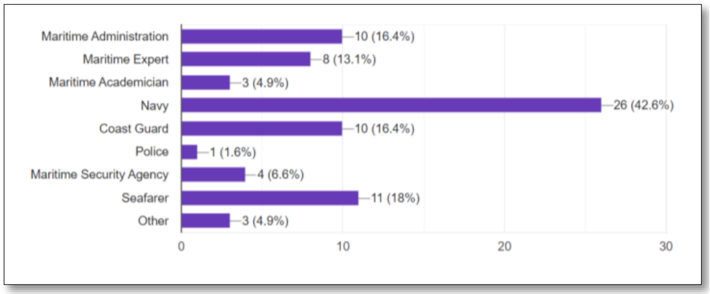
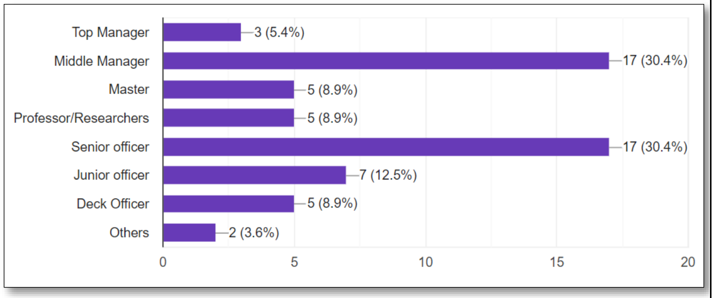
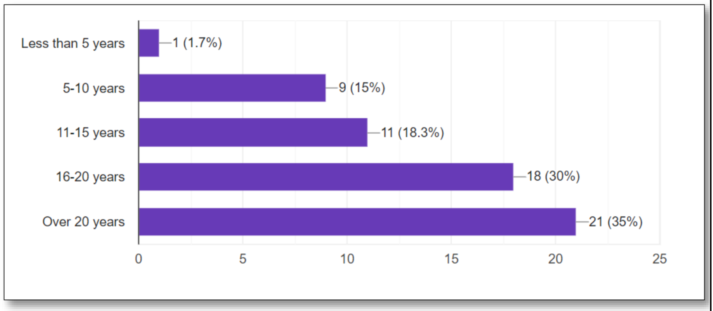
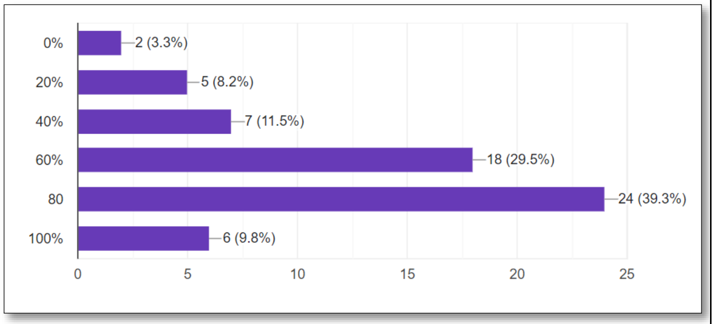
Please attach:

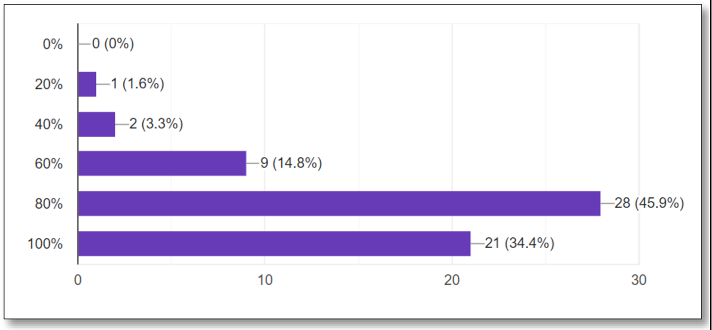
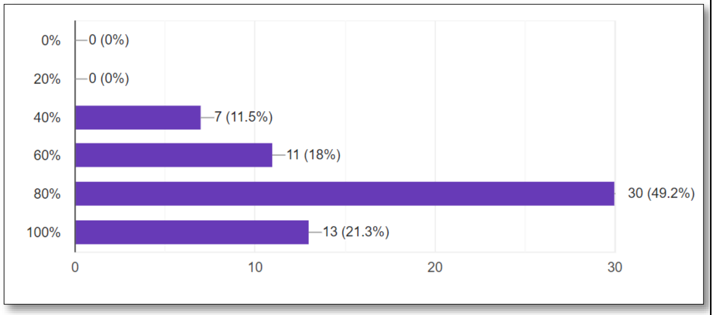
- A copy of the research proposal
- A copy of any risk assessment
- A copy of the consent form to be given to participants
- A copy of the information sheet to be given to participants
- A copy of any item used to recruit participants

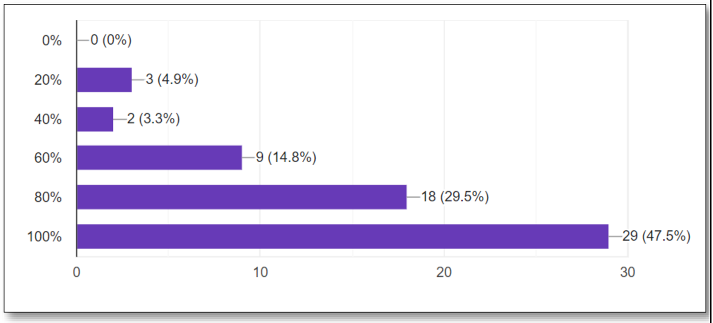
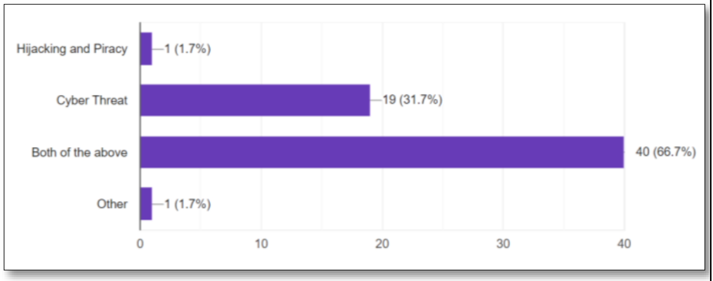
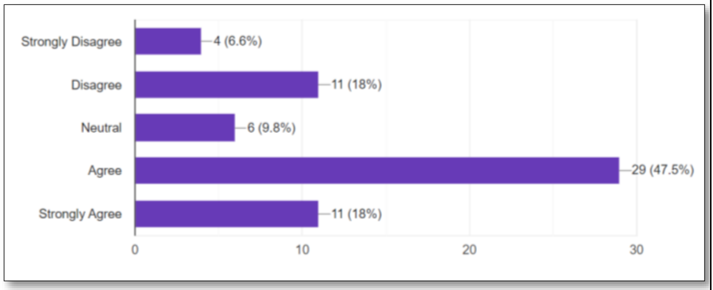
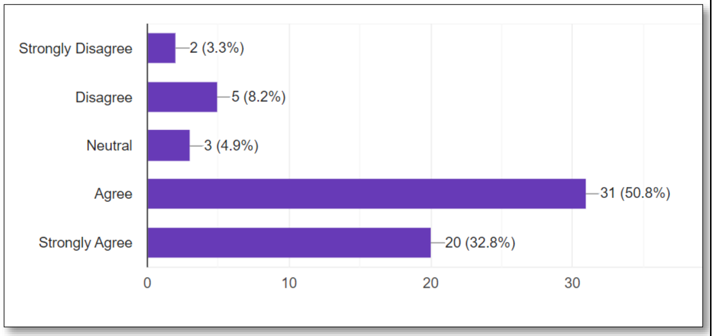
Appendix E

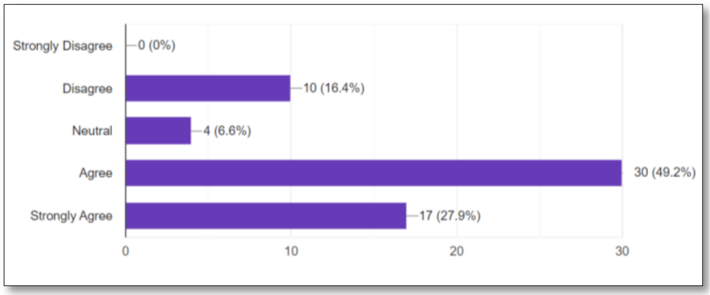
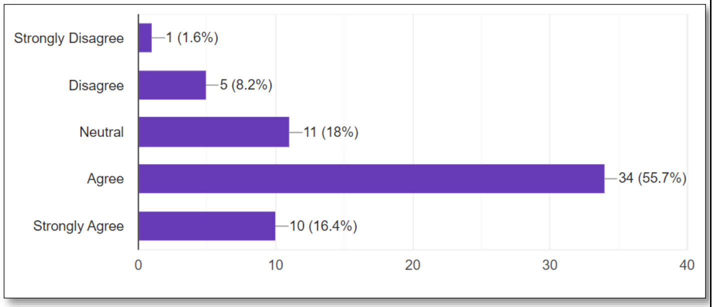
Section I and II Survey Questionnaire Results

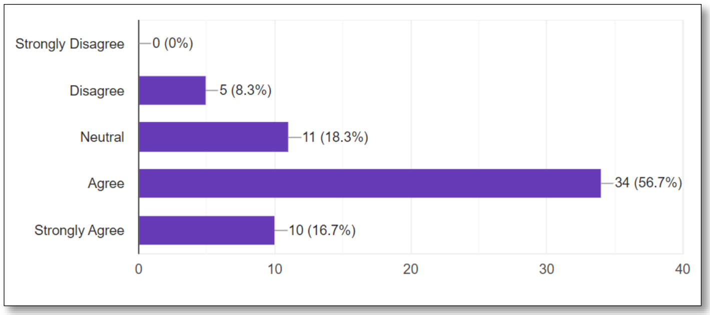
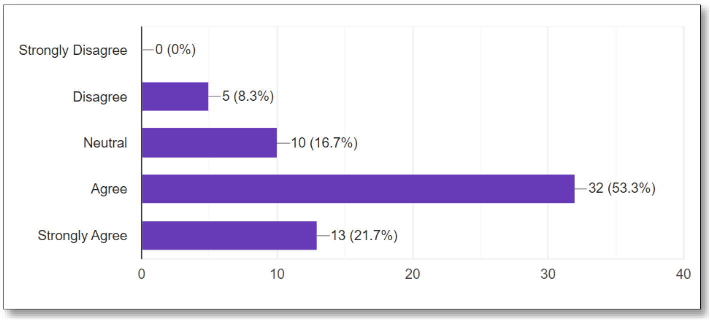
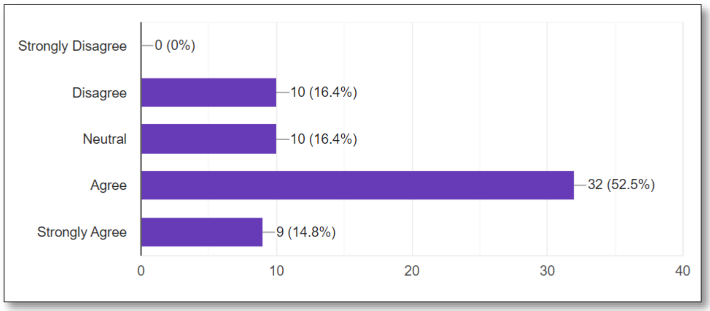
Question Number	Questions	Results
General Information (Section – I)		
1.	No of personnel participated	
2.	Nationality	
3.	Gender	
4.	Age	

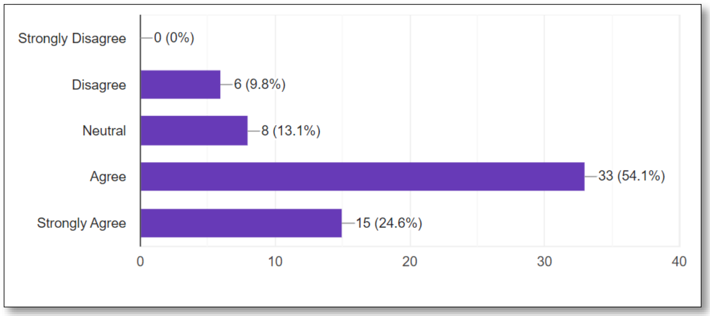
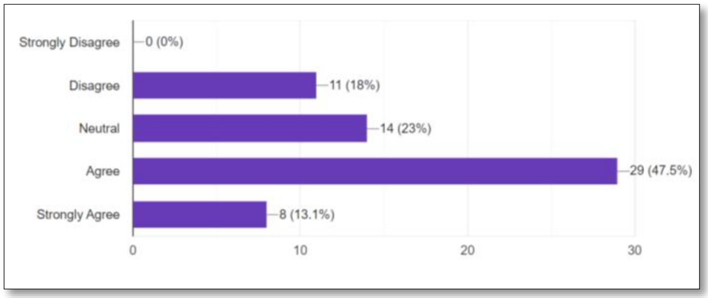
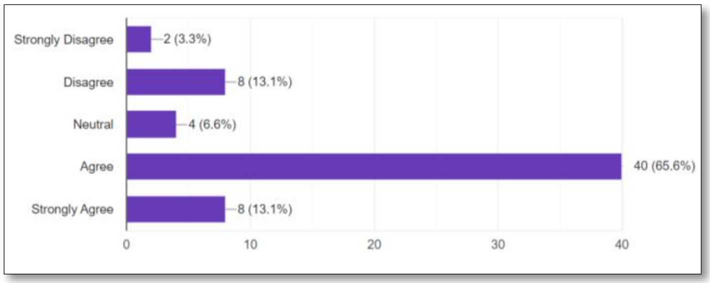
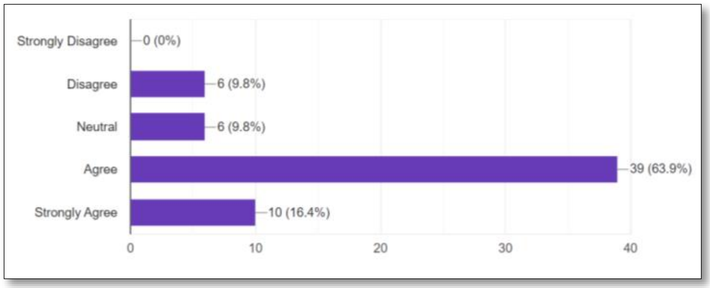
<table>
<tr><td>5.</td><td>Job</td><td>
</td></tr>
<tr><td>6.</td><td>Position</td><td>
</td></tr>
<tr><td>7.</td><td>Experience</td><td>
</td></tr>
<tr><td colspan="3">Section - II</td></tr>
<tr><td>SQ1.</td><td>Are you familiar with the concept of Maritime Autonomous Surface Ship (MASS)</td><td>
</td></tr>
</table>

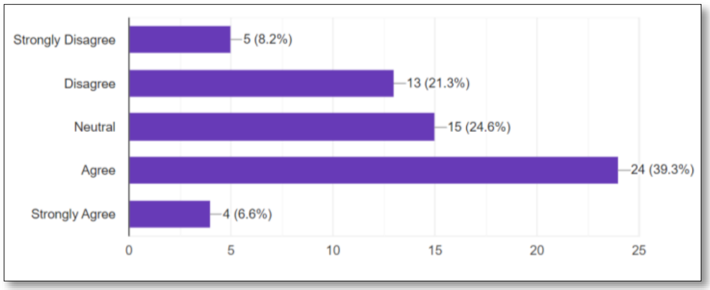
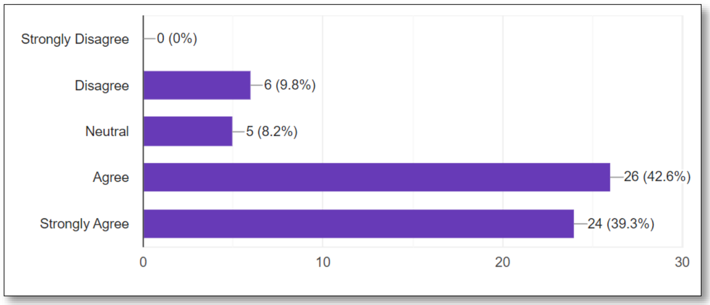
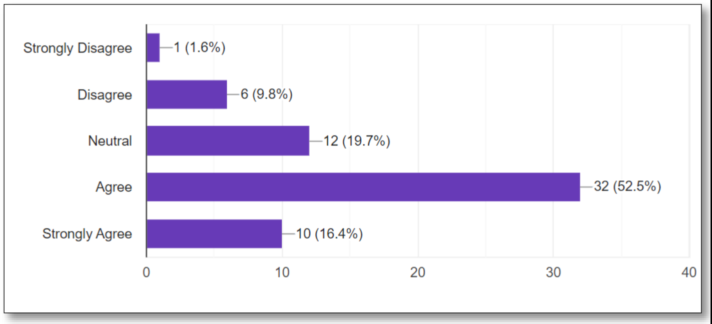
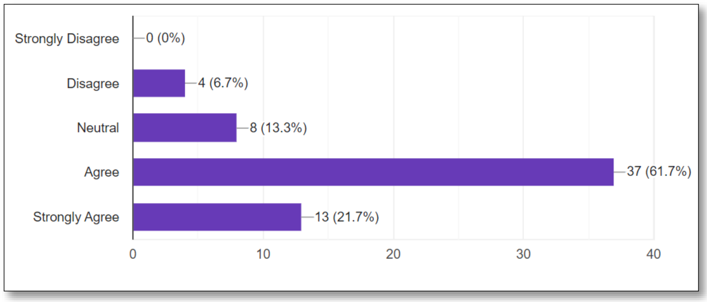
SQ2.	Are you familiar with Maritime Security and its importance in maritime sector	
SQ3.	Are you familiar with the threats and challenges MASS may face in future like: a. Cyber Threat. b. Hijacking or seizure of the ship. c. Piracy activity. d. Use of ship to conduct security incident. e. Use of ship itself as a weapon or means to cause damage or destruction. f. Smuggling weapons or equipment, including weapons of mass	

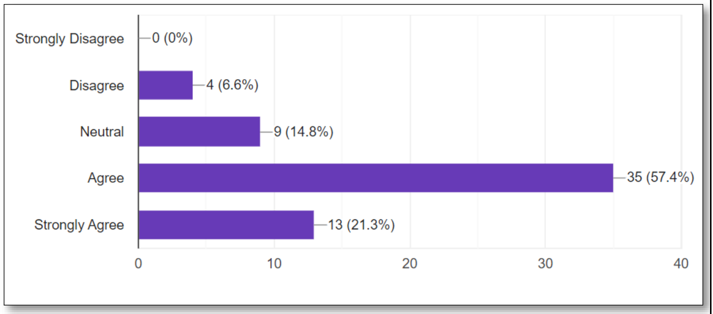
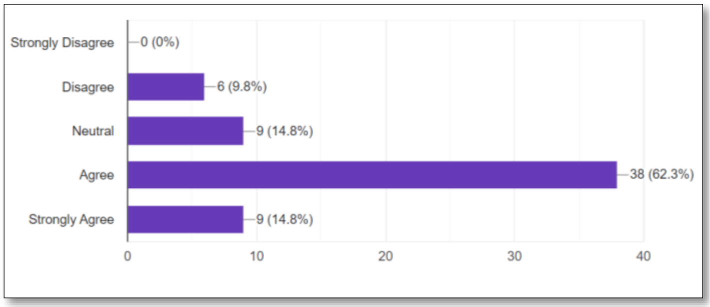
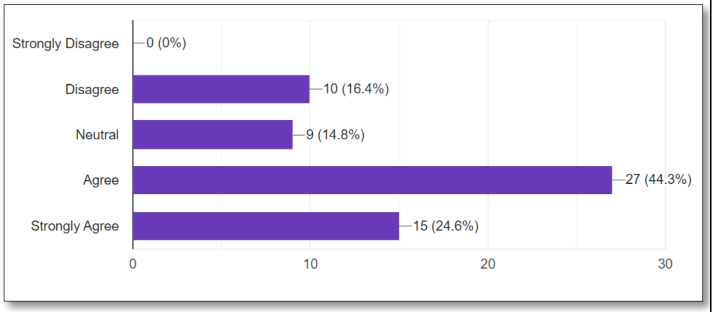
	destruction s.	
SQ4.	Are you familiar with the concept of law enforcement at sea by Coast Guard, Navy, Police, Maritime Security Agency's	
SQ5.	What do you think which threat is more prone to MASS.	
SQ6.	Does traditional piracy attacks will affect MASS, even though there is no crew onboard.	
SQ7.	Cyber-attacks will be more on MASS and is considered to be more vulnerable to this threat, including cyber piracy.	

SQ8.	Does pirates hijack MASS (physically or through cyber-attack) to ask for money for cargo, launch attacks on vulnerable assets or port installations, collision with warships/commercial ships, grounding in navigable areas also highlighted in the given scenarios.	
SQ9.	There is any possibility of exploitation of Global Navigation Surveillance System (GNSS) or Automatic Identification System (AIS) data along with other digital systems and software’s onboard MASS (bridge systems, cargo handling and management systems, machinery and propulsion systems, control systems, passenger servicing and management	

	systems, passenger public networks, crew welfare systems, and communication systems)	
SQ10.	Does non-state actors use MASS as a weapon to attack sensitive installations/ places/ assets of any country (warships, port or coastline installations etc. see both the scenarios outcome)	
SQ11.	Cyber security threat considered as higher than the physical attack by pirates on MASS	
SQ12.	There is a risk that crewless MASS may also pose threat to the security of other conventional ships at sea or harbor.	

SQ13.	There are high possibilities of MASS being hijacked and used by criminals for international organized crimes.	
SQ14.	The ship's security may be weakened on crewless MASS under the ISPS code.	
SQ15.	Shore Control Centers (SCC) on land are more vulnerable to cyber-attacks which includes the Communication and networking infrastructure of MASS (See Scenario II).	
SQ16.	Shore Control Centers (SCC) may came under attack by the Non-state actors and use MASS as a weapon against sensitive targets (See Scenario II).	

SQ17.	Law Enforcement Agencies are capable to handle situations after physical and cyber-attack has been done on MASS/ SCC as mentioned in the given two scenarios	
SQ18.	The employment of MASS may present new challenges for maritime law enforcement organizations (such as Coast Guard, Navy, Police, Maritime Security Agency)	
SQ19.	The acceptance of MASS in shipping industry will considerably influence law enforcement agencies use of Visit Board Search and Seizure (VBSS)	
SQ20.	Inspection of MASS at sea along with document verification during VBSS may require alternate measures/arrangements	

SQ21.	VBSS operation onboard crewless MASS may cause challenge for Law Enforcement Agencies.	
SQ22.	Is there any requirement for possible change in maritime interdiction/ boarding (VBSS) procedures involving MASS	
SQ23.	Enhancement of maritime security in MASS era is unavoidable	 Strongly Disagree 0 (0%) Disagree 10 (16.4%) Neutral 9 (14.8%) Agree 27 (44.3%) Strongly Agree 15 (24.6%) 0 10 20 30