

World Maritime University

The Maritime Commons: Digital Repository of the World Maritime University

World Maritime University Dissertations

Dissertations

10-31-2021

Study on the implications of automomous ships on maritime security and law enforcement by reviewing maritime security incidents

Aditya Pratap Singh

Follow this and additional works at: https://commons.wmu.se/all_dissertations



Part of the [Robotics Commons](#)

This Dissertation is brought to you courtesy of Maritime Commons. Open Access items may be downloaded for non-commercial, fair use academic purposes. No items may be hosted on another server or web site without express written permission from the World Maritime University. For more information, please contact library@wmu.se.

WORLD MARITIME UNIVERSITY

Malmö, Sweden

**Study on the implications of autonomous ships on maritime security
and law enforcement by reviewing selected maritime security
incidents**

By

Aditya Pratap Singh

India

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 ENVIRONMENT ADMINISTRATION)

2021

© Copyright Singh, Aditya Pratap, 2021

Declaration

I certify that all the material in this dissertation that is not my 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 or other organisation.



(Signature): _____

(Date): _____ 21 Sep 21 _____

Supervised by : Dr. Jens-Uwe Schröder-Hinrichs

Supervisor's affiliation : Vice-President (Academic Affairs) and Professor
World Maritime University, Malmö, Sweden

Assessor:

Institution/ Organisation:

Co-assessor:

Institution/ Organisation:

Acknowledgements

It is a genuine pleasure to express my deep sense of thanks and gratitude to my supervisor, Dr. Jens-Uwe Schröder-Hinrichs, whose expertise was invaluable in guiding me in my dissertation work and providing me with valuable advice and suggestions leading me to accomplish the dissertation. Your insightful feedback pushed me to sharpen my thinking and brought my work to a higher level.

I want to thank the World Maritime University, professors, and staff for continuous support and imparting the highest standard of education.

My sincere thanks and gratitude also goes to my esteemed organisation Indian Coast Guard for providing me with the opportunity to attend the programme. Special thanks to Sasakawa (Nippon Foundation) for extending generous full fellowship which has provided me with this opportunity of expanding my knowledge of maritime affairs at the World Maritime University (WMU).

I also take this opportunity to thank my co-supervisor, Dr Tiago Fonseca, who has shared valuable materials and insights. Thanks to my seniors, whose continuous support and motivation contributed immensely to enhance my knowledge.

I would like to express my profound gratitude to Ørnulf Jan Rødseth, *Senior Research Scientist, Sintef*, whose valuable inputs inspired and became the basis of this research, and Professor Dr. Dimitrios Dalaklis for material and insights, and Professor Dr Anish Hebbar for his valuable inputs and support. A sincere thanks to Miss Yvette De Klerk, WMU alumni, who shared her inputs and assisted in making valuable connections. I thank all maritime experts and participants who contributed to this study and made it possible. Special thanks to my friends of MSEA and World Maritime University especially Jose Ronnie Jr Ong, Nadhir Kahlouche for their help and support, irrespective of their own timeline.

Last but not the least, I would like to thank my family, who believed in what I did with trust in me. The journey would not be possible without my wife Namitha's unstinted support and boundless confidence in me and, finally, my lovely daughters, for their infinite love.

Abstract

Title of Dissertation : “Study on the implications of autonomous ships on maritime security and law enforcement by reviewing selected maritime security incidents”

Degree : Master of Science

MASS is the future of shipping. Technological advancement has taken humans to the moon and space, which was earlier explored only by machines. However, the same technology has proved that machines can replace human presence at sea, which is an advancement of the human race. The world is widely accepting MASS, and it has proved to be the key to the future of sustainable shipping. This giant leap in the shipping industry calls for bigger challenges for maritime security as well.

In the context of a maritime security threat, including maritime terrorism, piracy, armed robbery against ships, the IMO has formulated several regulations. Ships as a means of transport can easily impact maritime security, good order, and peace at sea. There is a reasonable fear that a ship might be transformed easily from a simple mode of transport to a weapon. The arrival in the maritime world of autonomous vessels will also affect the spectrum of maritime security. In addition, this ultra-technological change will have certain ramifications in the enforcement scheme too. The idea of independent, unmanned ships disrupts the whole maritime regulatory scene and affects the fundamental concepts of law.

This dissertation discusses the implications of MASS on maritime security and law enforcement as the transition will witness bigger security challenges, the ship being totally unmanned. In line with this, possible mitigation measures are also investigated. On autonomous crewless ships, the threat factors are more cyber than on conventional ships, where physical attacks are more likely. The focus on the mitigation measures that the law enforcement agencies and shipping industry have to consider is the need of the hour. The implementation of the preventive measures requires equal overhauling in infrastructure, coordination between agencies, and law enforcement procedures. Thereupon, the dissertation discusses the need for applicable solutions for preventing security threats.

Keywords: Maritime Autonomous Surface Ships (MASS) Autonomous ships, Unmanned Ships, Shore Control Centres (SCC), Maritime Security, ISPS, Piracy, Cyber-piracy, Armed robbery, Stowaway, Transnational organised crimes, Drug Trafficking, Maritime law enforcement, VBSS

Table of Contents

Declaration	i
Acknowledgement	ii
Abstract	iii
List of Tables	vii
List of Figures	viii
List of Abbreviations	ix
Chapter 1 – Introduction	1
1.1 <i>Background – MASS in the Maritime World</i>	1
1.1.1 Defining MASS	2
1.1.2 Level of Autonomy	3
1.1.3 Development timeline - MASS.....	4
1.2 <i>IMO MASS Initiatives</i>	5
1.3 <i>Problem statement</i>	6
1.4 <i>Objectives of the study</i>	7
1.5 <i>Research questions</i>	7
1.6 <i>Research methodology and methods</i>	7
1.7 <i>Expected outcomes</i>	8
1.8 <i>Scope and limitations</i>	9
1.9 <i>Structure</i>	9
Chapter 2 - Literature Review	10
2.1 <i>Introduction</i>	10
2.2 <i>MASS - Perceived Opportunities and Uncertainties</i>	10
2.2.1 Opportunities.....	10
2.2.2 Uncertainties	11
2.3 <i>Shipping and Maritime Security – A background</i>	11
2.3.1 What is Maritime Security?	12

2.3.2	<i>Maritime Security Instruments – International Shipping</i>	13
2.3.2.1	SUA Convention 1988 and 2005 SUA Protocol	14
2.3.2.2	ISPS Code	15
2.3.2.3	Maritime Security in non-IMO treaties	17
2.4	<i>Security Incident (Scenario) – MASS</i>	17
2.4.1	<i>Cyber-security threats</i>	18
2.4.2	<i>Hijacking and piracy</i>	19
2.4.3	Stowaway.....	20
2.4.4	Transnational Organised Crime/ Drug Trafficking.....	21
2.5	<i>Law Enforcement at Sea</i>	23
2.6	<i>Literature Review Summary</i>	24
	Chapter 3 – Methodology	25
3.1	<i>Introduction</i>	25
3.1.1	Adopted Research Methodology.....	25
3.1.2	Rationale for Research Methodology	25
3.1.3	Research Approach	25
3.2	<i>Research Process</i>	26
3.2.1	Literature Review.....	26
3.2.2	Scenario Validation.....	27
3.3	<i>Ethical Issues</i>	27
3.4	<i>Data Collection</i>	27
3.4.1	Personal Interviews.....	27
3.4.2	Questionnaire survey	28
3.5	<i>Limitations</i>	28
3.6	<i>Brief Summary of the chapter</i>	29

Chapter 4 - Data Description and Analysis	29
4.1 <i>Introduction</i>	30
4.2 <i>Survey questionnaire and interviews</i>	30
4.3 <i>Study of Impacts on Maritime Security and challenges for law enforcement using Security incidents (scenarios)</i>	31
4.4 <i>Scenario – 1</i>	32
4.5 <i>Scenario – 2</i>	37
4.6 <i>Scenario - 3</i>	46
4.7 <i>Scenario - 4</i>	51
4.8 <i>Scenario – 5</i>	55
Chapter 5 – Conclusions and Recommendations.....	61
5.1 <i>Introduction</i>	61
5.2 <i>Conclusion</i>	61
5.3 <i>Recommendations</i>	63
5.4 <i>Limitations and future research</i>	64
Reference	65

List of Tables

Table 1. Potential risks with MASS.....	2
Table 2. List of security incidents.....	16
Table 3. Overview of interview participants.....	31
Table 4. Selected security incidents (scenarios).....	32
Table 5. Influencing factors of Piracy.....	41

List of Figures

Figure 1. Envisaged ship control methods	3
Figure 2. MASS – Taxonomy of autonomy level.....	4
Figure 3. European initiatives in development of autonomous ships	5
Figure 4. Autonomous ship future development timeline	5
Figure 5. Process of Research Methodology	8
Figure 6. Schematic breakdown of the maritime security threats in context of AS	13
Figure 7. IMO and global measures for maritime security.....	14
Figure 8. ISPS Code Process Phase	16
Figure 9. Categorization of three blue crimes	21
Figure 10. Data on seized narco vessels between 1993-2013.....	23
Figure 11. Flowchart of the methodology.....	26
Figure 12. Scenario-1 “Intrusion/attack on SCC”.....	32
Figure 13. Participants response to SQ23	33
Figure 14. Participants response to SQ 24	34
Figure 15. Scenario – 2 “Hijacking of AS by pirates/non-state actors”	37
Figure 16. Participants response to SQ 10.....	39
Figure 17. Participants response to SQ 11	43
Figure 18. A systematic diagram of Hijack attack on AS.....	44
Figure 19. Scenario -3 “Armed robbery”.....	47
Figure 20. Participants response for SQ15	48
Figure 21. Scenario-4 “Stowaway onboard MASS”.....	51
Figure 22. Participants response to SQ 16.....	53
Figure 23. Participants response SQ 22	55
Figure 24. Scenario-5 “AS involved in transnational organized crime”	55
Figure 25. Participants response SQ 14	57

List of Abbreviations

AAWA	Advanced Autonomous Waterborne Applications Initiative
AI	Artificial Intelligence
AIS	Automatic Identification System
AS	Autonomous Ship/ Shipping
ATC	Air Traffic Control
BMP	Best Maintenance Practices
CS	Coastal State
CSO	Company Security Officer
CSI	Container Security Initiatives
CPS	Cyber-Physical Systems
EU	European Union
GISIS	Global Integrated Shipping Information System
GNSS	Global Navigation Satellite System
HRA	High Risk Area
IACS	International Association of Classification Societies
ICT	Information and Communication Technologies
IMO	International Maritime Organisation
IMB	International Maritime Bureau
IMarEST	Institute of marine engineering, science and technology
ISPS	International Ship and Port Facility Security Code
ISSC	International Ship Security Certificate
IT	Information Technology

IoT	Internet of Things
IQ	Interview Question
LEA	Law Enforcement Agency
LOSC	Law of the Sea Convention
LRIT	Long Range Identification and Tracking
MASS	Maritime Autonomous Surface Ships
MOWCA	Maritime Organisation for West and Central Africa
MSC	Maritime Safety Committee
MUNIN	Maritime Unmanned Navigation through Intelligence in Networks
SSA	Ship Security Assessment
SBO	Shore Based Operator
SSO	Ship Security Officer
MV	Merchant Vessel
MT	Motor Tanker
OOW	Officer of the Watch
OT	Operations Technologies
PCASP	Privately Contracted Armed Security Personnel
PFSA	Port Facility Security Assessment
PFSP	Port Facility Security Plan
PSC	Port State Authorities
RECAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RSE	Regulatory Scoping Exercise
RQ	Research Question

SCC	Shore Control Centre
SIG	Special Interest Group
SME	Subject Matter Expert
SSA	Ship Security Assessments
SSO	Ship Security Officer
SSP	Ship Security Plan
SLOC	Sea Lanes of Communication
SOLAS	Safety of Life at Sea Convention
STCW	Standards for Training, Certification, and Watchkeeping Convention
SQ	Survey Question
SUA	Suppression of Unlawful Acts against the Safety of Maritime Navigation
TW	Territorial waters
UKMTO	United Kingdom Maritime Trade Operations
UMV	Unmanned Maritime Vehicle
UN	United Nations
UNCTAD	United Nations Conference on Trade and Development
UNCLOS	United Nations Convention on the Law of the Sea, 1982
USS	United States Ship
VTS	Vessel Traffic Service
VBSS	Visit, board, search and seizure
WMU	World Maritime University
WMD	Weapon of MASS Destruction

Chapter 1 – Introduction

1.1 Background – MASS in the Maritime World

The maritime industry, including modern ships, are involved in the revolution denoted by the term Industry 4.0, resulting in defining the new term 4.0 ship, describes the trend in maritime technology towards increasing automation. It includes the internet of things (IoT), artificial intelligence (AI), autonomous and unmanned technology (Im et al., 2018; Trump, 2020). Shipping 4.0 revolution has introduced autonomous ships (AS) or maritime autonomous surface ships (MASS¹), which can be operated from a Shore Control Centre (SCC²) by an automated decision-making system (Emad et al., 2020; Sakhi et al., 2019).

There are multiple rationale³ for the shipping industry to embrace AS (Chang et al., 2021). However, there are concerns about whether the new technology will be accepted by the governments and the conservative maritime industry as many legitimate issues exist about the safety and security of its operation and reliability (UNCTAD, 2018). Although the maritime sector is advancing technologically, 4.0 ships still lack robustness and resilience against many dangers, including cyber or physical attacks (Trump, 2020).

Hazards, both traditional safety hazards, such as the possibility of collision or grounding and security threats, including piracy, are ever-present at sea. Shipping and ship represent great monetary and symbolic value and thus can be the target of the security threats such as robbery, piracy or terrorist attack (Liwång, 2016). Maritime security has been a perpetual concern to all involved in the maritime transport industry. Over the years, international organizations, governments, shipowners, and operators have reinforced legal and administrative instruments and procedures to maintain the highest security for ships, people, and cargo (Herbert-Burns et al., 2019). Today, the challenge for AS is to establish a technological system that is sufficiently

¹ Defined by the IMO as “ships which, to a varying degree, can operate independently of human interaction.”

² A Shore Control Center (SCC) is a “Place from where an operator can monitor and remotely control unmanned vessels” (Porathe, 2014).

³ Elimination of human errors, reducing operational cost, enhanced efficiency by allocating more space for cargo, saving fuel and reducing emission.

capable of dealing with terrorist attacks and pirates (Sakhi et al., 2019). Also, MASS may change the pattern of pirates, terrorists, criminal activities and introduce potential security risks (Table 1) (Kim, M., Joung, Jeong, & Park, 2020a).

Table 1. Potential risks with MASS (Kim et al., 2020)

Potential Risks	Examples
Rise of cybersecurity threats	<ul style="list-style-type: none"> • Hackers attacks to abduct ship and hijack cargo • Leakage of sensitive information on cargo and customer • Failure of a ship due to failure of critical operating systems, including the propulsion system • Failure of information and communication system required for autonomous operation • Distortion of information communication with SCC, including information on ship operation • Failure or delay of an onshore operator to recognise the occurrence of an accident • The weaponization of autonomous ship
Failure of equipment or device	
Error or distortion of information	
Difficulty of recognising accident	
Challenge of cargo management	
Threat against port Security	

1.1.1 Defining MASS

The concept of e-navigation as a harmonised electronic automation system that integrates, exchanges, and analyses marine information has provided a firm basis for unmanned and autonomous maritime systems. Further, the development of satellite communication ensured seamless interaction between shore and ships at sea, which enabled autonomous technology to be implemented (Emad et al., 2020). AS means the ability of a ship to independently govern its operations while transporting cargo from one location to another (Rødseth, Ø J. & Nordahl, 2017). In comparison, MUNIN⁴ defined autonomous ship as a vessel with “Next-generation modular control systems and communications technology that will enable wireless monitoring and control functions both on and off the board. These will include advanced decision support systems to provide a capability to operate ships remotely under semi or fully autonomous control” (figure 1) (Munim, 2019, p.3). In 2017, the IMO adopted MASS to refer to future unmanned or fully autonomous ships (Emad et al., 2020). According to various levels of autonomy, many alternative

⁴ Maritime Unmanned Ships through Intelligence in Networks

names for autonomous ships, including crewless ships and MASS, were used (Rødseth & Nordahl, 2017).

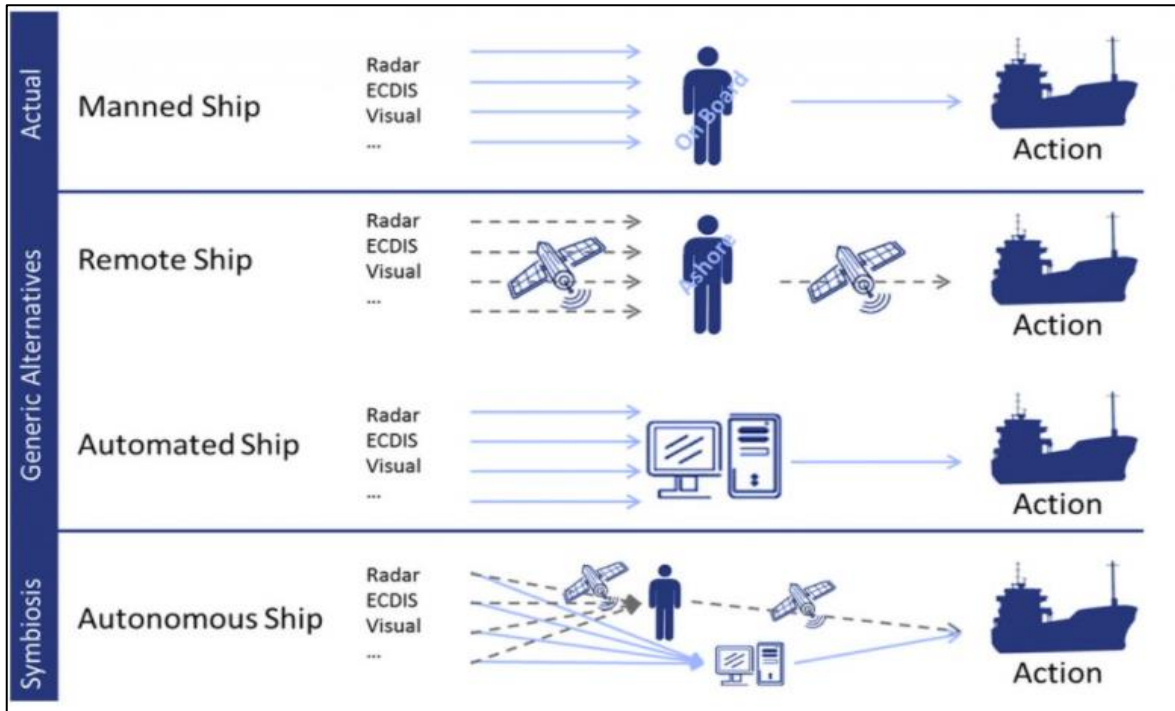


Figure 1. Envisaged ship control methods (Şenol et al., 2017; MUNIN)

1.1.2 Level of Autonomy

The level of autonomy for autonomous ships is widely discussed and deliberated by various agencies. Over six global authorities⁵ defined their category for the level of autonomy (Zhou et al., 2019). Lloyd’s register classification includes seven levels of autonomy⁶ (onboard decision support to a fully autonomous). IMO adopted the autonomy levels (figure 2) suggested by the Danish Maritime Authority (Zhou et al., 2021). For Regulatory Scoping Exercise (RSE), IMO has established four degrees of autonomy (IMO, 2018). Degree 3-4/ level RU-A would not have seafarers onboard, and vessels would be controlled remotely or fully autonomously with limited or no direct human interactions (Klein, 2019; Şenol et al., 2017). The degree of autonomy is not

⁵ Lloyd’s Register, Norwegian Forum for Autonomous Ships, Danish Maritime Authority, Maritime Autonomous Systems Regulatory Working Group, Bureau Veritas and IMO

⁶ AL0 ~ AL 6

essentially linear or hierarchical. MASS can work at one or more autonomous levels during a single passage (Kim, T. & Mallam, 2020).

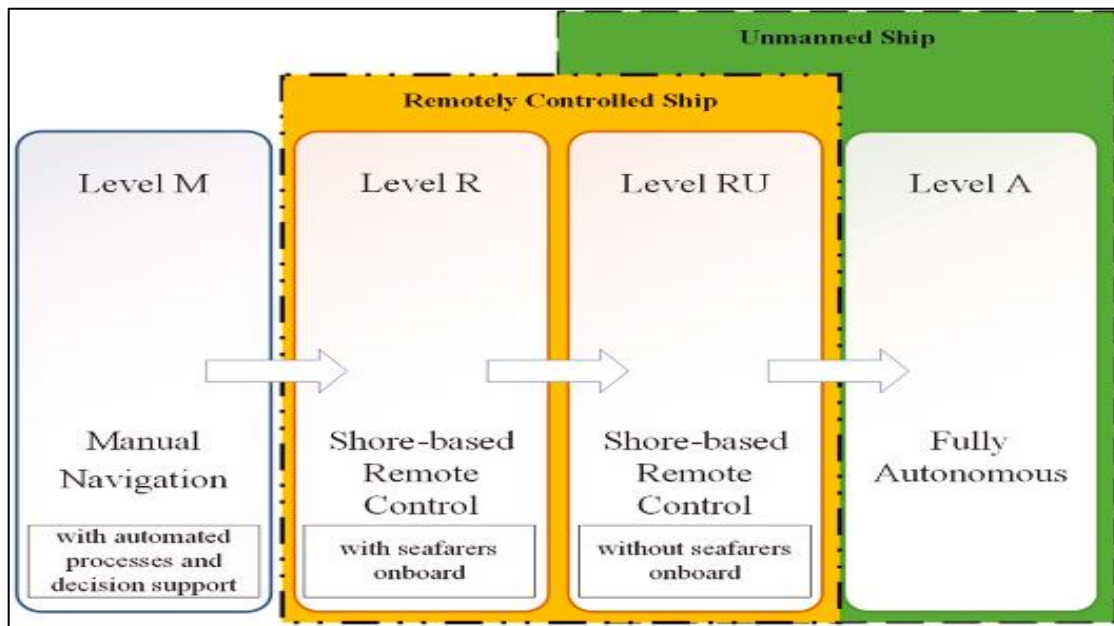


Figure 2. MASS – Taxonomy of autonomy level (Zhou et al., 2021)

1.1.3 Development timeline - MASS

The notion of autonomy is not new⁷, as the idea of autonomous “self-steered” robots has been around since the advent of computers. With improvements in automation, smart ships have grabbed attention (Kim, M., Joung, Jeong, & Park, 2020b; Zhou et al., 2021). The first significant study on a crewless and autonomous merchant ship was carried out under EU flagship-project MUNIN, which triggered a wave in Europe, and various companies rapidly launched other concept ships (figure 3) (Rødseth, Ørnulf Jan et al., 2021; Wariishi, 2019). The MUNIN project concluded that crewless and autonomous ships could and will be used when they are safer and cost-effective (Felski & Zwolak, 2020; Rødseth, Ørnulf Jan, 2018). According to Szelangiewicz & Żelazny (2020) initially, crewless ships are being employed for small-scale transport activity⁸. As

⁷ In 1898, Nikola Tesla patented “method of and apparatus for controlling mechanism of moving vessels” (Guerra, 2017)

⁸ Short distance car-passenger ferries, Port and technical vessels, Inspection and testing ships (hydrographic), Tugboats

technology improves and legal regulations develop, ocean-going AS will emerge (in 15-20 years) (Szelangiewicz & Żelazny, 2020).

Projects with Industry-Government-Academia Collaboration	
MUNIN (Maritime Unmanned Navigation through intelligence in Network)	- Implemented from 2012-2015 - With the support of the EU, the Fraunhofer Institute took the lead in developing the concept of unmanned vessels and conducting pilot program - Announced the effect of improving fuel efficiency by 10% or more and reducing the risk of collisions and sinking
AAWA (Advanced Autonomous Waterborne Applications 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 realisation of autonomous ships, and conducted research based on conceptual studies
Efforts by Companies (primarily efforts toward practical applications)	
Yara International (major Norwegian fertiliser maker) and Kongsberg (maritime division of a Norwegian public-private enterprise)	- Unmanned electric container ship 'Yara Birkeland' scheduled to be put into service in 2022 - Development is supported by a subsidy from the Norwegian government
Rolls-Royce Commercial Marine (now a part of Kongsberg Maritime)	Under the SVAN (Safer vessel with Autonomous Navigation) project, demonstrated autonomous operation of a freight and passenger ferry (coastal ship) owned by Finland's Finferries in December 2018
Wärtsilä (Finnish marine engine manufacturer)	Demonstrated autonomous operation of a freight and passenger ferry (coastal ship) owned by Norway's Noried in November 2018

Figure 3. European initiatives in development of autonomous ships (Wariishi, 2019)

Leading companies have promised to deliver their crewless vessels by 2025 and envisaged that fully autonomous ships would be operating by 2035 (figure 4) (Emad et al., 2020; UNCTAD, 2018).

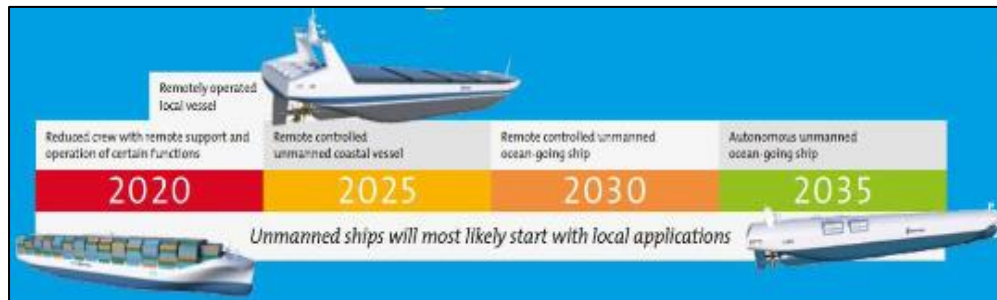


Figure 4. Autonomous ship future development timeline (Emad et al., 2020)

1.2 IMO MASS Initiatives

In order to cover the advancing technologies by the international regulatory framework, IMO embarked on a RSE in 2017 to “determine how safe, secure and environmentally sound MASS operations might be addressed in IMO instrument”. The RSE involves two steps. The first step is

to ascertain whether an autonomous vessel remains safe and environmentally viable within present IMO conventions and future goals. The second step is to analyse how the MASS operation can be addressed, considering human, technological and operational factors (IMO, 2018). The Maritime Safety Committee (MSC), at its 103rd session, has completed the first step⁹, which outlines number of high-priority issues¹⁰ that span multiple instruments, and is needed to be addressed at a policy level to determine future work. MSC also commented that the best way forward for addressing MASS in the IMO regulatory framework would be to design a goal-based MASS instrument¹¹ in a comprehensive manner (IMO, 2021b).

1.3 Problem statement

The maritime transport industry serves about 90% of global trade and significantly contributes to global economic development (UNCTAD, 2020). In this era of highly complicated technology, conventional ships are prone to maritime threats and then comes the question for autonomous unmanned vessels. Non-state actors, criminals/terrorists could use the vulnerability of AS to perpetrate maritime crime. As the application of unmanned ships advances, it is obvious that there will also be repercussions for the global legal framework in place to strengthen maritime security (Klein, 2019). It is critical to review AS vulnerability and assess the impacts of AS on maritime security. At the same time, it is fundamental to seek the most appropriate mitigation measures to address these vulnerabilities.

Further, it is the responsibility of the coastal state for maintenance of law enforcement and maritime security inside the territorial sea. The maritime threats are countered by the conduct of frequent constabulary patrols and maritime security operations by law enforcement agencies, coast guard and naval forces, including peacetime boarding operations per maritime zones and navigational regimes reflected in the UNCLOS Article 110¹² (Kraska, 2010). A State's right to

⁹ MSC.1-Circ.1638

¹⁰ MASS terminology and definitions, Functional and operational requirements of remote control station/centre, Possible designation of remote operator as seafarer

¹¹ MASS Code

¹² A warship or military aircraft or duly authorised ships and aircraft on government service towards law enforcement exercise powers to visit, board, search and seizure (VBSS) on the high seas 'right of visit' under UNCLOS article 110.

engage in such activities is based on its exercise of sovereignty, sovereign rights, or jurisdiction over its maritime zones (Klein et al., 2020). Law enforcement agencies may also undertake boarding on foreign-flagged vessels for various reasons. The advent of AS in the maritime domain will create operational and practical challenges for law enforcement agencies who act on behalf of the respective coastal state to maintain governance at sea. Thus, exploration of AS implications on maritime law enforcement is considered indispensable.

1.4 Objectives of the study

The following are the research's objectives: -

- To critically study autonomous unmanned ship (s) impacts on maritime security and discuss the mitigation measures.
- To examine autonomous unmanned ship (s) implications on maritime law enforcement and explore the way forward.

1.5 Research questions

The research study will answer the following research questions:

- What are the likely impacts of autonomous unmanned ships on maritime security and what mitigation measures should be adopted to address these impacts?
- What are the challenges anticipated by maritime law enforcement agencies in the autonomous shipping, and how should these challenges be addressed?

1.6 Research methodology and methods

The nature of research is a deciding factor in choosing an appropriate research methodology. The research is about autonomous ship technology and its implications on maritime security for which nil historical data (relevant cases) is available. The researcher plans to address the identified research questions through maritime security incident scenarios. A mixed-method approach (triangulation) is utilised to gain inputs from experts and survey to understand the research problem best. Figure 5 shows the approach of the study.

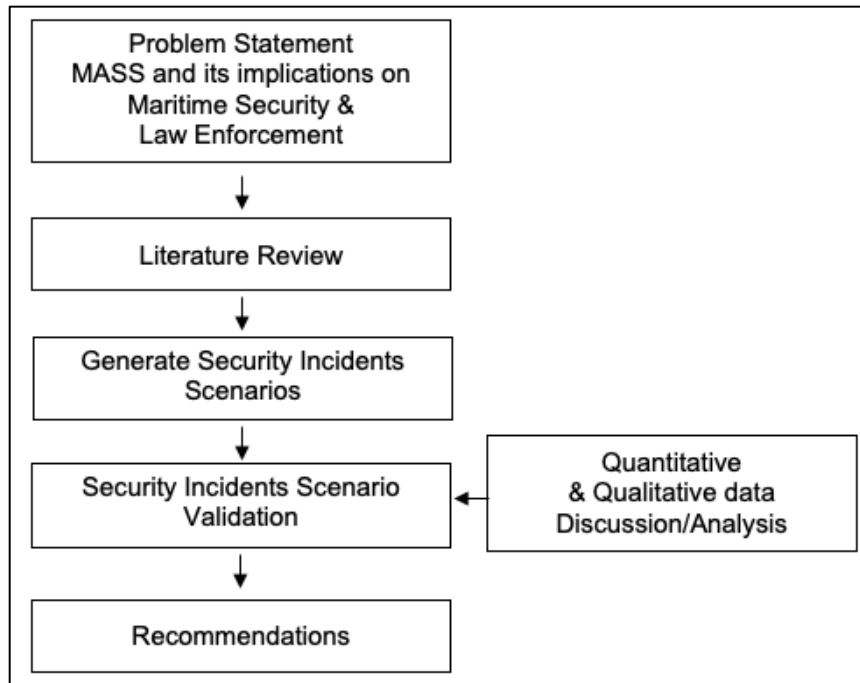


Figure 5. Process of Research Methodology (prepared by Author)

1.7 Expected outcomes

The expected results out of this study are appended below:

- The research will identify the possible implications of autonomous (unmanned) ships for maritime security and law enforcement.
- The research will familiarise about vulnerabilities of autonomous ship (s) operations.
- The research may serve as a tool for coastal state (s)/ law enforcement agencies to deal with security incidents involving autonomous ships in future.
- To stimulate involved maritime stakeholders¹³ to take cognisance of security challenges that may emerge for autonomous ships and simultaneously develop effective mitigation strategies for secure maritime transportation.

¹³ Regulatory bodies {IMO, Coastal state (s)/ law enforcement agencies, designers, owners/operators)

1.8 Scope and limitations

MASS is a new technology and evolving. The lack of historical data or research on MASS implications on maritime security and law enforcement is considered one of the primary limitations. Thus, maritime security incidents (scenarios) are analysed through mixed-method (triangulation) to fill the necessary research gaps.

1.9 Structure

The dissertation is divided into five chapters. Chapter one covers an introduction to the research topic, problem statement, establishes the objectives, research questions, the methodology adopted and mentions the scope of the research work. Chapter two is a literature review focusing on the AS opportunities and uncertainties. It further discusses the maritime security, selected security incidents (scenarios) and law enforcement aspects of AS. Chapter three discusses the methodology for this study and explains the approach, the questionnaires survey and personal interviews of the participants. Chapter four describes and analyses the selected security scenarios and present individual scenario analyses. Finally, chapter five provides a conclusion and recommendations for the research.

Chapter 2 - Literature Review

2.1 Introduction

The UNCLOS, regarded as the “constitution for the ocean”, establishes a legal framework within which states parties must act, but it does not define maritime security and makes only a few references to it (Cook, 2020). IMO progressively strive to introduce higher safety and security standards in shipping. Higher impetus on maritime safety, in fact, become a major proponent for businesses to invest in autonomous ship or MASS underpinned by transformational technologies (Komianos, 2018; Kretschmann et al., 2017). However, operating autonomous commercial ships also implies that risk profiles, responsibilities and accountabilities will be different compared to conventional ships (Kim & Mallam, 2020). MASS will fundamentally restructure the operational concept of shipping operations, signifies the surfacing of new hazards, risks and security concerns which calls for new measures to mitigate or eliminate them. In regard to the physical security of MASS, it is envisaged that AS operations may involve higher boarding and robbery (Honekamp, 2018). Moreover, the absence of crew creates a significant security gap that necessitates a risk mitigation strategy. In future, security teams in pre-determined geographic zones may inspect the AS to ensure it is safe to leave or enter the port (Komianos, 2018). The following sections explore elements of MASS opportunities and uncertainties, introduction to maritime security, law enforcement and security incident (scenarios) identification.

2.2 MASS - Perceived Opportunities and Uncertainties

2.2.1 Opportunities

Autonomous ship (s) is a possible answer to many shipping issues. That is why various developers are embracing the MASS concept. Moreover, few countries tie it to the objectives of sustainability (de Klerk et al., 2021). “Human errors are responsible for 96 per cent” of the incidents at sea. Advanced automation is expected to reduce human-related errors and marine accidents. Undoubtedly, MASS is expected to support tedious and dangerous maritime activities (Porathe et al., 2018). The other primary motivation for the development of AS is to reduce manning cost¹⁴ for seafarers which accounts for at least 40 per cent of vessel operating cost. Also, the popularity

¹⁴ Includes wages, provisions, travel and repatriation, pensions, insurance, and litigating personal injury claims.

of the seafaring profession has been reduced significantly, and only selected labour supply countries are supplying maritime force (Pribyl & Weigel, 2018). Replacing seafarers will definitely lead to reduction in the risk factor of piracy and the hostage situation for vessels operating in HRA and cut insurance coverage costs (Carey, 2017; Kobyliński, 2018).

2.2.2 Uncertainties

Several risks would accompany the benefits of autonomous ship technology (Komianos, 2018). MASS would be controlled from a remote control station. Thus, opens the third dimension in vessel controlling mechanism other than ship itself and ports. In addition, handling a vessel in the harbour will also pose a challenge (Pribyl & Weigel, 2018). Van Hooydonk (2014) likewise identifies drawbacks of technology, and considers that shore controllers would be significantly constrained in their intuition for adequately assessing and deciding about situations at sea.

Another central issue is cyber threats that are expected to increase when a vessel eventually operates purely remotely or in autonomous mode (Kobyliński, 2018; Tam & Jones, 2018). Kobyliński (2018) and Habdank (2019) speculate a potential risk that pirates may hack a ship and electronically take control. As a result, a situation may arise wherein pirates remotely sail a ship to a specific destination and transfer valuable freight from the vessel. Pirates or terrorists may also use the ship's navigating power to blackmail and threaten society by deliberately directing vessels into port or other vital locations. MASS may also be used by criminals to carry out attacks and transport contraband in concealment (Kim et al., 2020).

2.3 Shipping and Maritime Security – A background

As highlighted above, MASS will influence the maritime domain, and mentioned threats will have visible implications on maritime security. Maritime security has been a focus amongst influential global security actors since the beginning of the 1990s (Bueger & Edmunds, 2017). Piracy, trafficking and environmental crime at sea are increasingly viewed as a significant challenge for the human security of coastal nations and are also considered threats to global commerce and energy security (Bueger et al., 2020). Currently, the primary focus of many nations in maritime security is on piracy, terrorism, weapon proliferation, drug trafficking, and illicit trafficking (Bueger et al., 2020). However, maritime security is not optimum at all levels and in all areas. It has been relatively easy for some countries (mainly developed) to implement the global measures,

particularly those with an effective maritime administration. Few countries face more significant problems, and these relate to physical security provisions for the ships and ports and security in the maritime surroundings (Herbert-Burns et al., 2019). The advent of AS in commercial shipping and its maritime activity raises questions of these vessels fitting into existing ocean governance structures (Kim et al., 2020; Klein, 2019).

2.3.1 What is Maritime Security?

As the research is primarily focused on MASS and its impacts on maritime security, it is indispensable to discuss maritime security in detail. There are several definitions, meanings, and connotations for “security¹⁵” and “maritime security¹⁶”(Andritsos, 2013). Natalie Klein (2011) as well states that word maritime security has diverse connotations for different actors. The military's view differs from that of the shipping industry. US naval operation concept highlights it as “Ensuring the freedom of navigation, the flow of commerce and the protection of ocean resources, as well as securing the maritime domain from nation-state threats, terrorism, drug trafficking and other forms of transnational crime, piracy, environmental destruction and illegal seaborne immigration” (Klein, 2011, p.8).

In contrast to military definitions, maritime security for ship owners implies a transport system and relates to the safe transport of cargo without interference or being subjected to criminal activity (Klein, 2011). Jones (2006) explains ship owners view and professes the concept of maritime security as “the state of a shipping company/vessel/crew/port, being of feeling secure”, or “the safety of a shipping company/vessel/crew/port against such threats as terrorism, piracy, and other criminal activities”. Maritime security is a buzzword that draws attention to looming threats and prepares support for legislation to address them. However, no definitive definition of maritime security has yet developed. Maritime security has been commonly discussed, pointing to ‘threats’ that prevail in the maritime domain (Bueger, 2015).

¹⁵ “The set of means/actions through which safety is ensured, in particular against intentional threats; it encompasses all measures, actions or systems aiming at preventing intentional threats from compromising safety”

¹⁶ “The combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts.”

In the future, integration of IT and OT systems will result in Cyber-Physical Systems (CPS) on which the safe operation of contemporary and future ship depends (Kavallieratos et al., 2020). AS will be operated remotely from a third location i.e. SCC. In addition, the fundamental change is that these ships will be crewless. Overall, AS and SCC alongwith existing maritime transport system (conventional ships and ports) will play a significant role in establishing new framework of maritime security (figure 6).

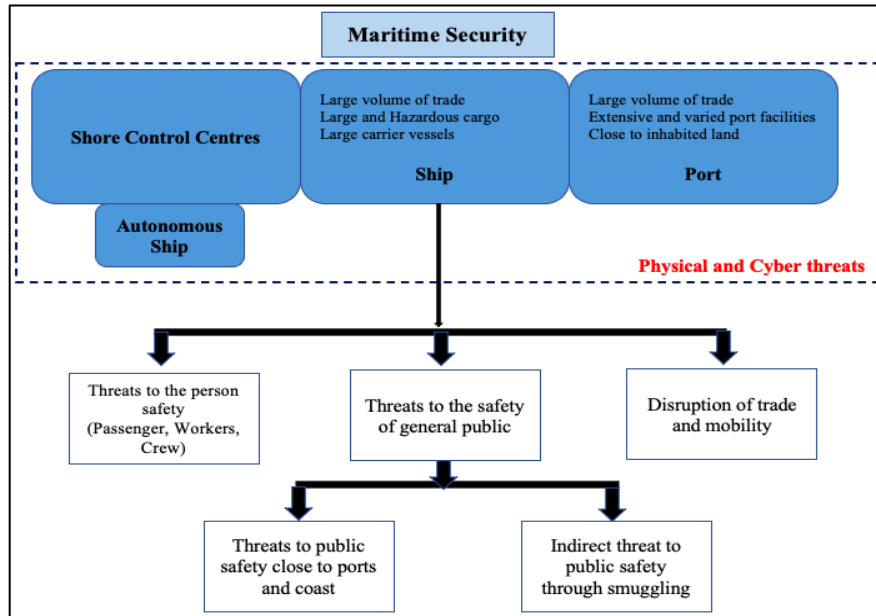


Figure 6. Schematic breakdown of the maritime security threats in context of AS. Prepared by Author based on information from Andritsos (2013)

2.3.2 Maritime Security Instruments – International Shipping

For decades, various low-intensity and substantial security incidents in the maritime domain were reported, which served as the foundation for developing security instruments for global shipping. The current security measures for the maritime domain are introduced at the international, regional, and national levels (Herbert-Burns et al., 2019; Metaparti, 2010). In following sections, most relevant IMO and global measures (instruments) for maritime security are discussed (figure 7).

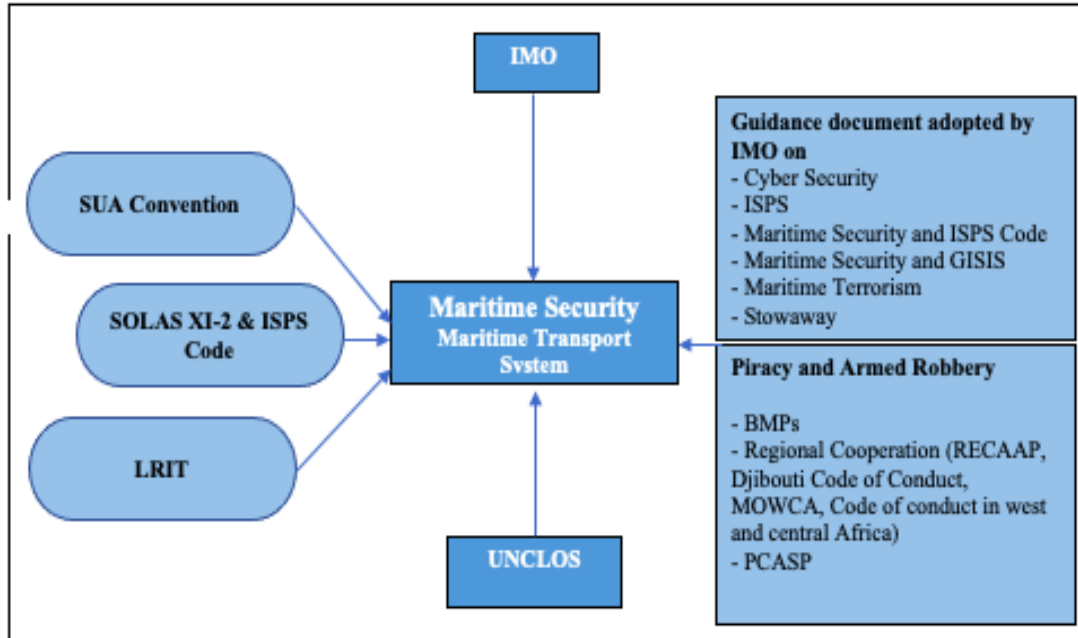


Figure 7. IMO and global measures for maritime security. Prepared by Author based on information from IMO (2021a)

2.3.2.1 SUA Convention 1988 and 2005 SUA Protocol

The 1985 hijacking of the Italian cruise ship Achille Lauro sparked international outrage, and the IMO passed a resolution in response A.584(14)¹⁷ and MSC/Circ.443¹⁸. Following the adoption of resolutions, the UNGA adopted resolution 40/61, calling on all states to :

“Take all appropriate measures at the national level with a view to the speedy and final elimination of the problem of international terrorism, such as the harmonization of domestic legislation with existing international conventions, the fulfilment of assumed international obligations”

Pursuant to the Achille Lauro incident, the IMO adopted the first security convention in March 1988, the Convention for the Suppression of Unlawful Acts against the Safety of Maritime

¹⁷ Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crew.

¹⁸ Measures to prevent unlawful acts against passengers and crew onboard ships.

Navigation (SUA), which was duly amended in 2005 and adopted in the form of Protocols to the SUA treaties (the 2005 Protocols) (Attard, 2014; Cook, 2020).

2.3.2.2 ISPS Code

The 9/11 terrorist attacks in the United States provoked a substantial shift and spurred regulatory authorities to investigate security aspects in shipping. As a result, International Ship and Port Facility Security (ISPS) Code was proposed and adopted in 2004, designed to prevent ships from being used as weapons by terrorists (Metaparti, 2010). A new maritime security regime was incorporated in SOLAS, chapter XI-2 on special measures to enhance maritime security, including the ISPS code. Part A of the code is mandatory, while part B contains guidance. The regulations in this chapter also require all ships to be equipped with a ship security alert system (Komianos, 2018).

The ISPS code objective is to identify security threats and implement security measures and create obligations for governments, administrations, and ships on a national and international level (Dalaklis, 2017). In order to fulfil these objectives, the ISPS code requires that the vessel operator designate a Company Security Officer (CSO) and Ship Security Officer (SSO). In addition, a ship must create Ship Security Plan (SSP), obtain a vessel International Ship Security Certificate (ISSC) after Ship Security Assessments (SSAs). Almost the same procedures are also needed for a ISPS complied ports. The application of the ISPS code involves three major phases (Figure 8) (Komianos, 2018; Progoulakis & Nikitakos, a2019).

Many researchers recommend that ISPS should be amended to have adequate security measures in crewless ships since it is expected that it will be difficult to apply current regulations (Dalaklis, 2017; Kim, H. & Yang, 2019). Technical and institutional considerations should take place to strengthen the security since the absence of “security officers/personnel” in the case of an autonomous (crewless) ship is a significant challenge (Kim et al., 2020; Komianos, 2018). The recently concluded RSE classified several IMO instruments as “High Priority” including SOLAS chapter XI-2 which needs to be addressed before all other instruments (IMO, 2021).

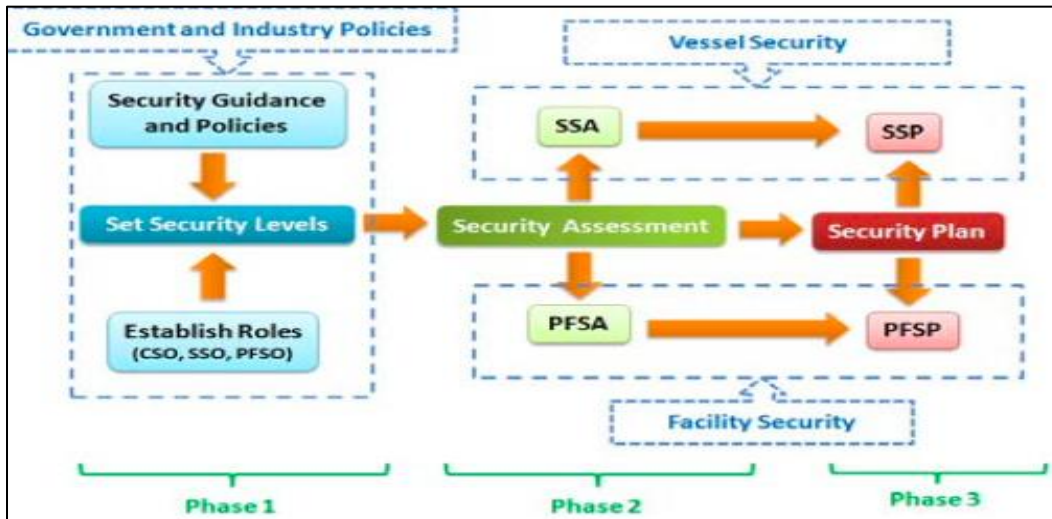


Figure 8. ISPS Code Process Phase (Progoulakis & Nikitakos, 2019)

Also, the ISPS code defines security incidents, particularly in connection to ships. The ship security assessment should evaluate all conceivable threats, according to ISPS (part B), which may include the following security incidents (Table 2) (IMO, 2021a).

Table 2. List of security incidents. Prepared by Author based on information from IMO (2021a)

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 systems or ship's stores
4	Unauthorised access or use, including presence of stowaways Smuggling weapons or equipment, including weapons of mass destructions
5	Use of ship to carry those intending to cause a security incidents
6	Use of ship itself as a weapon or as a means to cause damage or destruction
7	Attacks from seawards whilst at berth or at anchor
8	Attacks while at sea

2.3.2.3 Maritime Security in non-IMO treaties

The third UN conference on the law of the sea featured maritime security including violation of territorial sovereignty and piracy. UNCLOS recognise three important navigational regimes¹⁹. Each of these regimes attempts to strike a balance between two vital competing interests of coastal states for economic and security reasons, the other being the interests of states who strive to maintain freedom of navigation and overflight. UNCLOS part VII contains vital provisions dealing with maritime security, particularly article 88²⁰. Maritime security is seen as a shared concern among many countries. Furthermore, UNCLOS also contains provisions (article 100) to combat piracy, and deliberates on the collaboration of all states in combating piracy on the high seas or in any other location outside of any state's jurisdiction (Attard, 2014). Osinuga (2020) suspects that AS would be targeted by cyber-pirates who would most likely be ashore and may not be considered pirates in the traditional sense, and suggests that UNCLOS may be expanded to assimilate and absorb the variants of piracy which may cover cyber pirates.

2.4 Security Incident (Scenario) – MASS

MASS is likely to alter the pattern of pirates, terrorist and criminal activities. The number of hostage situations is likely to decrease. The lack of crew, on the other hand, would enhance attempts to seize the entire vessel for its precious cargo. Furthermore, there is a potential that MASS will be utilized for illegal cargo shipments, including arms and drugs. In addition, port security also needs to be reviewed in the MASS era (Kim et al., 2020).

AS, in addition to traditional security threats, will also be affected severely by cyber-security threats. AS and SCCs both can become target of cyber-attacks. There could be multiple maritime security incident scenarios. However, the researcher considers cyber or physical attack on SCCs, hijacking of AS by pirates or cyber-hackers, cases of armed robbery in harbour or at anchorages, stowaways incidents and transnational maritime crime/drug trafficking as relevant maritime threats, having direct implications on maritime security in the context of MASS. In subsequent

¹⁹ Innocent passage applies in the territorial sea and archipelagic waters, transit passage applies to straits used for international navigation, and archipelagic sea lanes passage applies to archipelagic waters.

²⁰ UNCLOS article 88 referred to reservation of the high seas for peaceful purposes “the high seas shall be reserved for peaceful purposes”

sections, a detailed review has been undertaken on selected threat (incidents) in the context of MASS.

2.4.1 Cyber-security threats

Cyber-attack is a hidden threat that can have very serious consequences for the maritime transport industry. In May 2021, a cyber-attack crippled a US colonial oil pipeline that connected 30 oil refineries. The heavy ransom paid by the company to the hackers to restore the system shows its far-reaching implications for critical industries, including shipping. The success of such attacks may encourage similar attacks globally (Allianz, 2021). It is alarming as such attacks can also be planned and executed by non-state actors using autonomous ships or by attack on SCC.

The interconnectivity between a ship and shore, a core requirement for an autonomous ship to work, may increase potential cyber-attacks on maritime vessels (Tam & Jones, 2018). IMO defines *cyber risk* as a “measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised” (IMO, 2017). RSE as well identified connectivity and cybersecurity as potential gaps that are required for MASS operations (IMO, 2021).

Honekamp (2018) speculates that the security issues about communication and IT systems of an AS would be an essential aspect that needs to be considered. (Kim et al., 2020) recognize the threat of cybercrime as a source of worry. Cyber terrorists can compromise the communication link used by MASS to control the function from afar.

A study conducted by (Kunz & Ó hÉigearthaigh, 2020) provides a general insight into possible uses of robotics and AI, which would affect global security in different spaces, including civil aviation, shipping including autonomous shipping and ground vehicle safety and security. The study contemplates that the deployment of autonomous ships may be the most significant robot-related threat to global security from civil waterborne vehicles. It would be a likely transport for terrorists as a drone carrying explosives or biological, chemical or radioactive bombs, and since many large cities are situated along coasts or rivers, it may be disastrous.

The cyber threats would not only affect AS, but will also have equal implications on SCC infrastructure. Shore or Remote Control Centre will play a relatively important role for MASS

(Rylander & Man, 2016). These centres will be modern virtual bridge or machinery control rooms for navigators, virtual captains, and engineers to operate these highly cyber-physical sophisticated ships. There would be a requirement to have reliable connectivity²¹ and infrastructure (Kutsuna et al., 2019). SCCs will be equipped with essential components including a two-way communication system (terrestrial and satellite connectivity), connectivity with sea/land-based actors, sensor suites (weather, remote sensing), and last critical component is the operator (human element) itself (Wróbel et al., 2020). In RSE outcome, potential gap in respect of SCC or Remote Control Centre (RCC) is regarded as high priority issue that cut across several IMO instruments. However, SOLAS chapter XI-2 has not been included as common potential gaps for RCC (IMO, 2021).

In future a single SCC may operate several vessels to economise the efforts. In terms of a security hazard, SCC-ship communication or SCC itself may be attacked by cyber pirates or criminals to meet their agendas.

2.4.2 Hijacking and piracy

The Gulf of Guinea has emerged as the world's piracy hotspot²², and it is threatening since vessels are being targeted at high seas (Allianz, 2021). Although, it is speculated that, MASS will not be targeted view absence of crew however, this view is refuted by many (Habdank, 2019).

The use of maritime assets, including merchant ships in malicious activities have been highlighted in several studies (Klein, 2011). Further, many incidents were observed wherein criminals/pirates embarked on ships and overpowered crew and took control of the ship (Jiang & Lu, 2020a).

Rødseth & Burmeister (2015) considers that terrorists using an autonomous crewless ship as a remotely controlled weapon is a very high-risk scenario and an unlikely event as long as communication systems, position sensing and onboard control systems are appropriately designed.

²¹ With maritime regulators, business partners (shipping company and agents), VTS, port authorities, the Coast Guard/ Navy, Pilots

²² 22 separate incident recorded in 2020

Osinuga (2020) as well anticipates that AS would most likely not be susceptible to conventional maritime piracy. However, it may be hijacked by “cyber pirates.”

On the other hand, Van Hooydonk (2014) considers it would be unrealistic to expect pirates and terrorists to vanish from the high seas in the age of AS. He further thinks these ships to be a softer target for the criminals.

Klein (2019) escalated this viewpoint by speculating the use of AS by non-state actors to commit a crime like a terrorist attack against subsea infrastructure, including oil and natural gas pipelines or telecommunication cables or the shipment of illicit cargo across national boundaries. According to Petrig (2020), criminals have already started embracing new technology to compromise maritime security. There is a real chance that criminals in the future will use autonomous vessels frequently and in a variety of ways to fulfil their missions. In her opinion, despite the rather apparent maritime security dimension of expanded automation in shipping, the relevant doctrinal analysis is still in its primary stage. Further, the potential use (and abuse) of autonomous technologies, including ships concerning maritime security, has received very little scholarly attention so far. Coito (2021) warned that the crewless vessel would be more exposed to transnational criminal activity, such as theft and piracy.

2.4.3 Stowaway

Van Hooydonk (2014) contemplate that apart from the possible passenger onboard an unmanned ship, the only person who retains his maritime law status is the stowaway²³ and it would be illusory to think that stowaways will not board them.

Stowaways can be categorised as refugees, asylum-seekers, economic migrants, illegal migrants, criminals and terrorists. Criminals and terrorist as stowaways are probably the most threatening. Terrorists look for easy access to reach their targets to plan clandestine attacks. Stowaways represents a global concern, not just a problem for one country (Aguocha, 2018).

23 According to FAL convention, a stowaway is "A person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the shipowner or the Master or any other responsible person and who is detected on board the ship after it has departed from a port, or in the cargo while unloading it in the port of arrival, and is reported as a stowaway by the master to the appropriate authorities"

For the same purpose, deck watches in ports and search of the ship are undertaken to prevent persons from embarking in ports and hiding onboard and to ensure that stowaways are detected if any succeed to embark on board. The obligation for an autonomous ship (remote controlled and fully autonomous without crew) implies that physical manning is needed in port since appropriate deck watch and search of the vessel would not be utterly feasible through cameras and sensors.

2.4.4 Transnational Organised Crime/ Drug Trafficking

According to Bueger & Edmunds (2020), transnational organised crime²⁴ or described as “blue crime” (figure 9) is on the rise and recently been recognised as a significant security issue.

	Crimes against mobility	Criminal flows	Environmental crimes
Relation to the sea	On the sea	Across the sea	In the sea
Ideal-type of object	'ships' & 'ports'	'societies' & 'communities'	'nature' & 'installations'
Subcategories	<ul style="list-style-type: none"> • Kidnap and ransom • Ship/cargo seizure • Robbery and theft • Crimes in and against ports • Stowaways • Cyber crimes 	<ul style="list-style-type: none"> • People Smuggling • Human Trafficking • Small arms and WMD • Narcotics • Illicit goods • Counterfeits • Wildlife • Waste 	<ul style="list-style-type: none"> • Fisheries crimes • Pollution • Illegal mining/resource extraction • Crimes against critical infrastructure • Crimes against cultural heritage
Forms of harm and victims	<ul style="list-style-type: none"> • Maritime trade • Supply chains • Seafarers • Coastal economies • Port facilities 	<ul style="list-style-type: none"> • Formal economy • Public health • Environmental destruction • Trafficked persons • National security 	<ul style="list-style-type: none"> • Environmental destruction • Biodiversity • Legitimate coastal economy • Coastal livelihoods • Food security
Cross-cutting/facilitating activities	Bribery, blackmail and corruption; slavery, forced and child labour; insurance, cargo and document fraud, money laundering, obstruction of justice, other forms of support for criminal groups.		

Figure 9. Categorization of three blue crimes (Bueger & Edmunds, 2020)

The maritime domain has been a locus of activity for transnational criminal and terrorist organisations in addition to other related benefits²⁵, which try to exploit mare liberum for ill-gotten

²⁴ Maritime piracy, the illicit trafficking of people, narcotics, arms or waste by the sea, and environmental crimes such as pollution

²⁵ Food, Energy and trade benefits

gains. Maritime drug trafficking is a sophisticated and well financed network (Coito, 2021). Klein (2019) also anticipates that AS will be used by criminals to undertake smuggling.

According to (Rødseth, Ørnulf Jan & Burmeister, 2015), the use of (civilian) MASS in any illegal activity or a transnational crime is expected to be very low but cannot be completely overruled. Coito (2021) foresees that transnational criminal organisations will seize upon the same technology and exacerbate illicit drug trafficking. He further speculates practical difficulty in prosecuting a remote, anonymous operator even after a successful interdiction of a remote-controlled or fully autonomous drug trafficking vessel.

Bueger & Edmunds (2020) further illustrates adaptability in blue crime, which is dynamic and adaptable. Criminals operating in one form of crime may also engage in others simultaneously or shift from one type to another. Three motivations for change and evolution in maritime crime can be identified: countermeasure driven inspirations, opportunity-driven motives, and those that originated from unintended outcomes. The criminal also shifts to crimes where countermeasures are less intense and the risk-reward balances more favourable, and the phenomenon has been described as displacement. The counter-piracy measures off the Somali coast resulted in the decline of piracy. However, it is believed that pirate organisational structure remains intact, and their leaders remain at large and are now involved in other forms of maritime crime to which their network, resources, and skills are well suited, including arms and people trafficking (Bueger & Edmunds, 2020).

It is likely that, criminals will shift their focus to autonomous technologies to undertake blue crimes. Leuprecht et al. (2016) conducted a qualitative study and observed that transnational organized criminals and terrorists consider the global economy ideally equipped to meet illicit goods and service demands. Figure 10 illustrates data on the seized narco vessels between 1993-2013, by United States which also include submersible and semi-submersible vessels (Ramírez & Bunker, 2015).

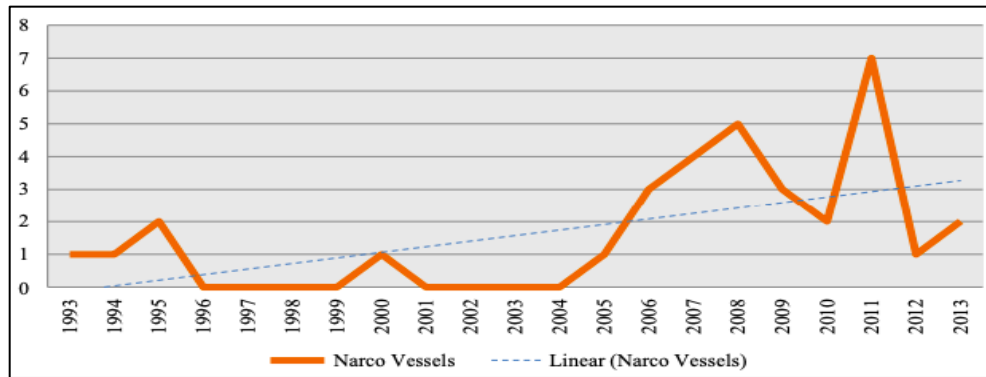


Figure 10. Data on seized narco vessels between 1993-2013 (Ramírez & Bunker, 2015)

2.5 Law Enforcement at Sea

Maritime law enforcement is vital for states to maintain maritime security. It gets reflected in every maritime strategy, which keeps them an effective means of preventing and suppressing illegal activities at sea. Law enforcement operations include surveillance, stopping and boarding, search and inspection, reporting arrest or seizure of persons or vessels, detention and imposition of sanctions (Galani & Evans, 2020). The practical nuances of AS are of particular concern to maritime security experts. The maritime law enforcement community considers AS an asset and a threat vector that criminals would be exploiting to avoid detection (Allen, 2018).

In respect of high seas, UNCLOS article 110 govern the Visit Board Search Seizure (VBSS) operations in cases of reasonable suspicion that a vessel is engaged in piracy, the slave trade or without nationality. Under Article 110(3), a law enforcement vessel may “send a boat under the command of an officer to the suspected ship”, and the boarding party inspect the ship’s documents and conduct further examination²⁶ (Guilfoyle, 2017; Klein, 2019).

Klein (2019) critically discusses the case of suspect AS, where the requirement to determine if the AS is a “ship” that is flagged to a state and, if so, that State’s consent must be sought for any possible boarding. However, she considers it to be problematic (Klein, 2019).

²⁶ Conduct search onboard, if suspicion remains

Further, under UNCLOS, all state parties are to cooperate to suppress illicit traffic in narcotic drugs and psychotropic substances in the high seas²⁷. 1988 Drug convention elaborated this cooperation for law enforcement purposes. According to article 17 of said convention, the right of visit may be exercised by law enforcers onboard vessels involved in illicit trafficking (Klein, 2019).

2.6 Literature Review Summary s

From a broad discussion and literature review on AS and elements of maritime security, it can be inferred that AS may have certain implications on maritime security and law enforcement. However, exact implications cannot be accrued since there is no historical or incidental data available. In the next chapter, the researcher discusses methodology employed to study the impacts of AS on these two aspects which are then analysed in chapter-4.

²⁷ UNCLOS article 108

Chapter 3 – Methodology

3.1 Introduction

The chapter gives an outline of employed methodology for the research. The subsequent sections provide insight about adopted methodology, reasons for its selection, research approach, process, data collection, ethical issues, validity/ reliability and limitations.

3.1.1 Adopted Research Methodology

Effective design and carrying out research can be complex activities. Research may incorporate various methods which categorically depends on their suitability to achieve the research aim and objectives (Verschuren et al., 2010). A mixed-method (concurrent triangulation design) approach has been selected, citing the peculiarity of the research about autonomous unmanned ships and its implications on maritime security and law enforcement. The researcher pragmatically utilised open-ended (qualitative) and close-ended (quantitative) data gathering methods and involved both forms of data analysis in a mixed-methods approach to elucidate the research objectives (Creswell, 2021). Johnson & Onwuegbuzie (2004) illustrate mixed method as “the class of research where the researcher mixes or combines quantitative and qualitative research techniques, methods, approaches, concepts or language into a single study” (p.17). The overarching purpose of mixed-method research is to enhance and improve a study's result by integrating qualitative and quantitative research components (Schoonenboom & Johnson, 2017).

3.1.2 Rationale for Research Methodology

The freedom to apply the best procedures, regardless of their paradigm, in more complex circumstances is a major benefit of the selected methodology. Certain research topics warrant investigation by multiple methods spread across different paradigms, and mixed methods are likely to provide such freedom and flexibility (Kumar, 2018). The technology for autonomous ships is fast evolving. Its impact on numerous maritime disciplines is still in its early stages and difficult to predict.

3.1.3 Research Approach

The researcher used the literature review to generate relevant security incident scenarios for AS and validated/analysed through surveys and personal interviews of experts. A survey is inexpensive, provide anonymity and obtain information from relevant individuals. Whereas, interviews are appropriate for complex situations and helpful in extracting in-depth information. The scenario generation and validation are considered an apt tool for establishing the basis given the uncertainty and lack of historical data on AS and its implications on maritime security and law enforcement. Researcher-driven scenario generating processes might be quantitative, qualitative, or mixed (Star et al., 2016). Figure 11 illustrates the process.

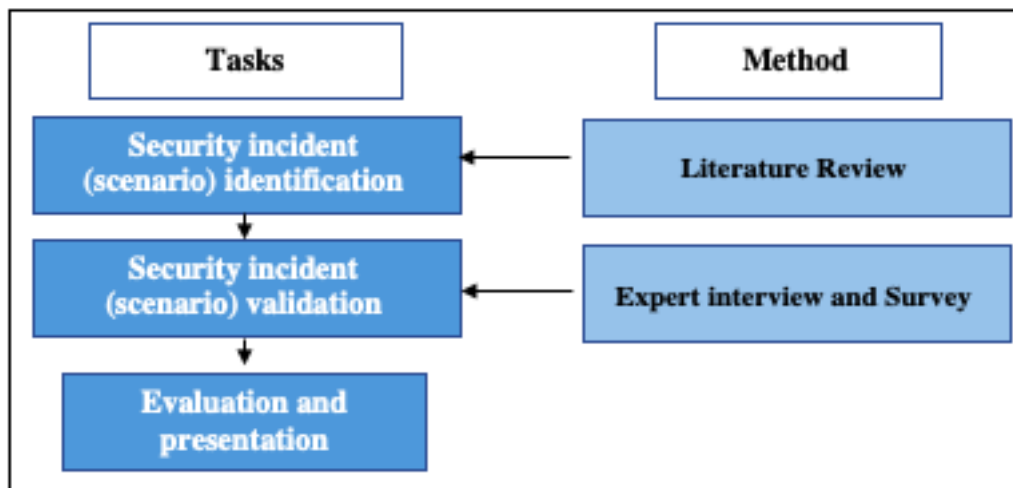


Figure 11. Flowchart of the methodology, (prepared by Author)

3.2 Research Process

3.2.1 Literature Review

The goal of the review was to find, select, and critically appraise appropriate literature on MASS and its implications on maritime security, as well as to analyse the data gathered from the reviewed literature. The process of doing a literature review might be iterative. Unexpected complications may occur throughout the review, necessitating changes to the research topic or review process. The literature review identified certain uncertainties/vulnerabilities of AS for maritime security and law enforcement. Each of these security threats are regarded as a scenario and analysed to address research objectives.

3.2.2 Scenario Validation

The current era characterised by uncertainty, innovation, and disruptive change demands scenario planning techniques for their known effectiveness in uncertainty and complex conditions. Scenario planning incites strategic reasoning and overcomes thinking barriers by generating multiple futures. Scenarios are considered a valuable tool that encourages organizations to prepare for possible eventualities and become more innovative (Amer et al., 2013). Furthermore, the scenario method allows for the development of future strategies and solutions. Scenario analysis examines what is likely to happen by considering various outcomes (Kim, Y. & Cha, 2012). The study utilised scenarios to look into AS vulnerabilities for maritime security by analysing/validating selected security incidents.

3.3 Ethical Issues

This study necessitated the inclusion of a human component. Considerations of 'ethical issues' takes precedence during the data gathering process. The survey and interviews have to be approved after a thorough assessment to ensure that they met the highest ethical standards. Before any action involving human activity was undertaken, the WMU Ethics Committee evaluated every component of the survey and interview questions. In addition, to preserve the participant's rights and privacy, factors such as secrecy, anonymity, data protection, and the flexibility to withdraw from participation were closely adhered to.

Moreover, all of the participant's contributions were voluntary, and no fees were charged for participating in the research. No changes or additions to the received data were made, and all material will be deleted after the dissertation's final submission deadline. Appendix A contains the protocol for the WMU Research Ethical Committee.

3.4 Data Collection

Data collection for personal interviews and questionnaire surveys began on 18 Aug 2021 and was completed on 17 Sep 2021. Both methods are described in the subsequent section.

3.4.1 Personal Interviews

A total of 11 personal interviews of Maritime Experts viz maritime academician and researchers, law enforcement agency officials were carried out via Zoom/Google meet/Microsoft meeting applications. Maritime researchers with wide experience in the MASS research projects and

maritime security participated whose perspectives were vital for the research. Interviews of senior law enforcement agency officials who also hold requisite experience in MASS concept participated. Such blend was considered most suitable for the research objective. The personal interviews of the experts were composed of 20 questions. The consent form and question templates for interviews are placed in [Appendix B](#).

3.4.2 Questionnaire survey

The survey has been developed on basis of security incidents selected as scenarios to achieve research objectives. The survey aims to maximize the participation of maritime professionals and maritime security experts, including Naval and Coast Guard officials. The questionnaire survey was composed of two parts :

- Section 1 – The first section (6 questions) focussed on the personal information of the participants
- Section 2 – The second section (23 questions), including 3 questions focused on participant’s familiarity with the concept of MASS, maritime security and law enforcement, was obtained. Subsequent questions gathered opinions on various security incidents (scenarios) and law enforcement involving MASS.

To best capture the diverse viewpoints, the responses were rated on a Likert scale in a multiple-choice question format. For the most part, the scaled responses 'Strongly disagree,' 'Disagree,' 'Neutral,' 'Agree,' 'Strongly agree,' and 'Don't know' were used. Electronic data collection, notably the survey monkey platform, was utilized to save time and participant's ease. The survey was also hosted on IMarEST²⁸ Special Interest Group (MASS SIG) to get a global response. In addition, the survey questionnaire was forwarded to various law enforcement agencies. The questionnaire survey template is placed in [Appendix C](#).

3.5 Limitations

The researcher observed many practical limitations as the concept of MASS is still evolving, and there is no empirical security incident data or cases available. The participant's responses are based

²⁸ The Institute of Marine Engineering, Science, and Technology (IMarEST) is an international membership organization and learned community for maritime professionals

on their perception and may be biased due to their professional attitude and one-sided knowledge in the field. The time limit was one of the significant limitations, which drastically reduced the scope of the research. The participation level was also affected due to the nature of research and competing interests. Also, the expertise in the inter-disciplinary domain was crucial, and access to such experts within a limited timeframe was scarce.

3.6 Brief Summary of the chapter

The chapter gives an overview of the research methodology to achieve the research objectives. The researcher employed a mixed-method approach to explore the research questions. The process involved selecting relevant security incidents (scenarios) through literature review, followed by validation of selected security incidents by personal interviews and survey questionnaires to study the impacts of MASS on maritime security and law enforcement.

Chapter 4 - Data Description and Analysis

4.1 Introduction

The chapter contains statistical findings, transcribed extracts, and analyses to address research questions.

4.2 Survey questionnaire and interviews

Survey

A total of 105 respondents, predominantly male (90%) from 25 countries, participated in the questionnaire survey conducted from 18 Aug 21 to 17 Sep 21. Overall, the respondents reflect a broad spectrum of different parts of the maritime sector, including representation from law enforcement agencies. The participant's knowledge on three areas was also assessed to analyse and extract accurate findings: the concept of AS, the concept and relevance of maritime security, and law enforcement at sea. Mostly all participants found familiar with the concept of maritime security (except 3) and with the concept of law enforcement (except 4), whereas 6 and 15 reported not at all familiar or not so familiar with the concept of MASS. Out of 105 participants, only 96 were found valid as nine skipped section-II of the survey. Finally, to maintain the quality of results, 32 respondents have been excluded from the evaluation. Accordingly, 73 remaining respondents were only considered for evaluation. The demographic data and result of survey is placed at Appendix D.

Interviews

A total of 11 semi-structured interviews were carried out, during which participants responded with their opinions based on interview questions on selected scenarios. The participants were maritime experts and significant stakeholders connected with MASS projects, law enforcement officials, shipping experts, classification societies, insurance companies and experts from academia. An overview of participants is appended in Table 3.

Table 3. Overview of interview participants (prepared by Author)

No	Respondent Nomenclature	Maritime Experience
1	Respondent-1 (R-1)	Leading expert who is highly active in the MASS projects with more than 2 decades of experience
2	Respondent-2 (R-2)	Academician in a leading University of Science and Technology with more than 25 years of experience. Actively involved in various MASS projects
3	Respondent-3 (R-3)	Expert from IMO. Hold comprehensive experience in maritime field including maritime security with more than 30 years of experience
4	Respondent-4 (R-4)	Expert from IMO with vast maritime experience and specialised in maritime security
5	Respondent-5 (R-5)	Senior officer in law enforcement agency with 2 decades of experience in the field. In addition, holds master's degree in maritime affairs with research background in MASS
6	Respondent -6 (R-6)	Senior officer in law enforcement agency with more than 20 years of experience. Also, holds master's degree in maritime affairs with research background in MASS
7	Respondent-7 (R-7)	Experts from Maritime Insurance club with requisite experience and specialist in MASS and maritime security
8	Respondent-8 (R-8)	Experts from Maritime Insurance club with requisite experience and specialist in MASS and maritime security
9	Respondent-9 (R-9)	Executive Director, having vast experience with Master's in Industrial Risk Management. Also, has contributed on MASS and security issues through various journals
10	Respondent-10 (R-10)	Head of training in a maritime solutions firm. In addition, holds master's degree in maritime affairs with research background in MASS
11	Respondent-11 (R-11)	Area manager of a leading IACS. More than 20 years of experience in the field

4.3 Study of Impacts on Maritime Security and challenges for law enforcement using Security incidents (scenarios)

In order to critically study the impacts of the AS on maritime security and challenges anticipated by maritime law enforcement agencies, security incidents are selected as scenarios on criteria discussed in para 2.4, and described in Table 4 in descending order of severity consequences. In each section, the researcher has described a particular scenario briefly (pure assumptions of the researcher for the discussion/analysis) which then analysed using themes namely Vulnerability of technology and Mitigation measures.

Table 4. Selected security incidents (Scenarios) (prepared by Author)

Security Incidents	Scenarios SI
Intrusion/attack on SCC	Scenario-1
Hijacking of AS by pirates/non-state actors	Scenario-2
Armed robbery or theft onboard AS	Scenario-3
Stowaway onboard AS	Scenario-4
Transnational organised crime involving AS	Scenario-5

4.4 Scenario – 1

Scenario-1 relates to intrusion/attack on SCC which is operating/monitoring several AS (figure 12). In order to attack military installations in the area, a banned non-state actor group plans and undertakes intrusion into the SCC. Upon gaining control, the group direct one AS toward vital military installation/ships in the port.

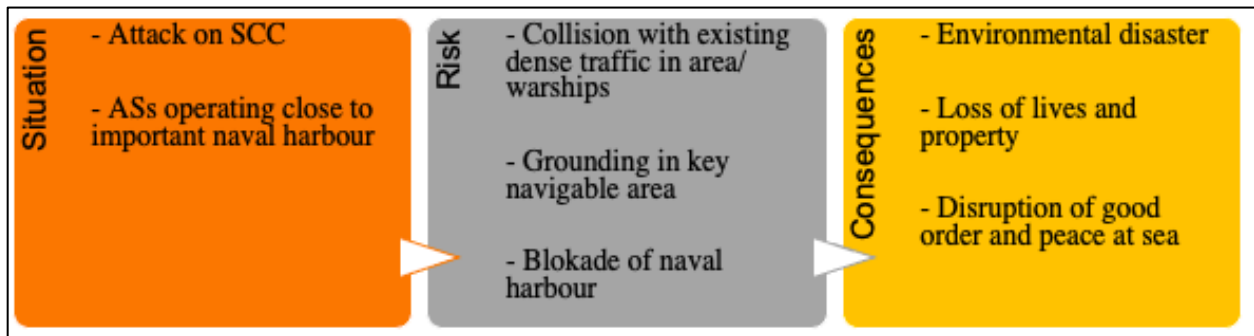


Figure 12. Scenario-1 “Intrusion/attack on SCC”

Analysis

Vulnerability of technology

In higher level of ship autonomy, the control of AS is handed over to a dedicated Shore control center (SCC), and an operator is able to monitor the operation of several vessels simultaneously and intervene remotely. The growing usage of networked ICT technology, opens up possibility of accessing the system virtually and to exploit the system. SCC is also subject to multiple security threats including possibilities of cyber and physical intrusion. All interviewees have major concerns about security of SCC-ship communication. R-3 comments, “Risk surely cannot be ignored, but it’s too early to anticipate.”

According to R-7, “Given the rapid change in the threat scenario and the technology (hacking methods), unique security challenges will be posed in context of unmanned operability, where cyber infiltration element would be prominent.” On the contrary, R-8 considers, 5G would be a leap for communication and harder to gain access illegally, so is the control centre. However, cyber-security being a known risk, could potentially make it a target.

In response to SQ23²⁹ (figure 13), majority of participants concurs with vulnerability of SCCs against cyber-risks.

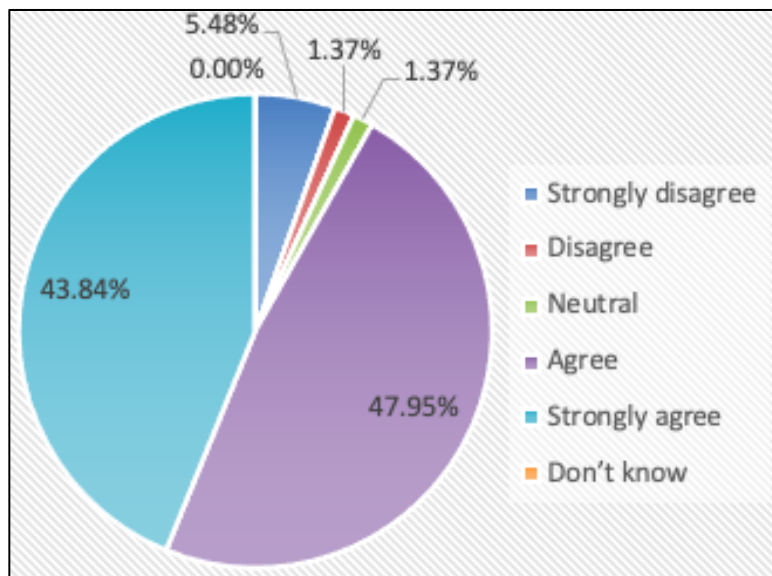


Figure 13. Participants response to SQ23 (prepared by Author)

Next to these examples, it may also be that non-state actors attack directly on any SCC. In AS, SCC, is crucial in ship operation. Physical security of SCCs, wherever located, would also become paramount. R-1 and R-2 also considers cyber as well as physical intrusion as a possibility.

²⁹ Communication and networking infrastructure of MASS shore control centres may also be vulnerable to cyber threats

R-1 in response to IQ 13³⁰,

“SCC being a critical component in MASS operation, needs special attention in terms of safety. The presence of unwanted person inside an SCC implies illicit control of ships being operated by the SCC” and further commented *“if I was a criminal, I would go for the SCC”*

Most participants concurs with SQ24³¹ (figure 14) statement in survey as well.

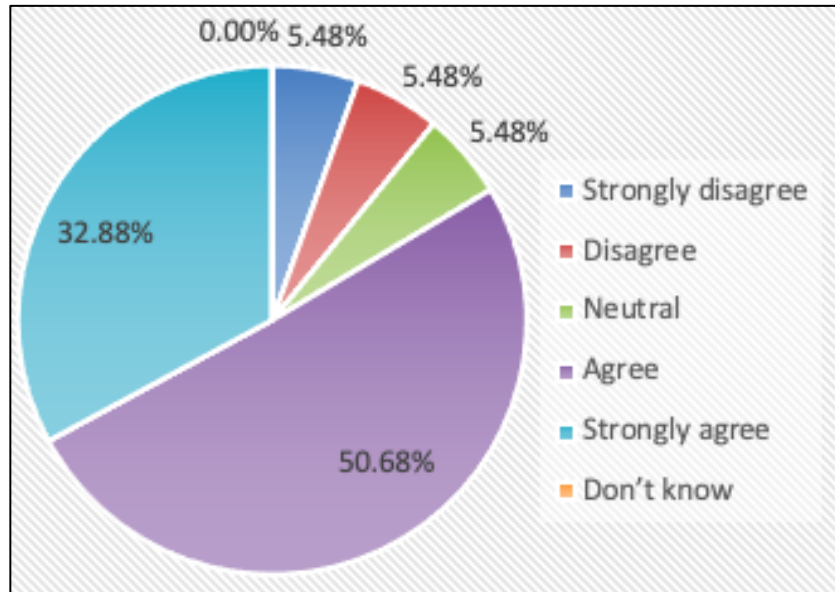


Figure 14. Participant response to SQ 24 (prepared by Author)

SMEs in a qualitative study by Roberts et al. (2019) also raises question that hackers who takes over SCC control may instruct the vessel to go to a place where it could be boarded by attackers. Thus, sealing off an autonomous ship from physical attack would appear to be a lot less helpful in these scenarios (Carey, 2017). Moreover, a SCC can be located in any part of the world, it can either be a highly developed state with lesser crime rate and security vulnerability or in some state(s) with higher security threats. As a result, if any of these centers are vulnerable to such

³⁰ Is there any possibility that the shore control centres may also be attacked (cyber pirates or physical attack) by criminals/non-state actors to fulfil their goals?

³¹ Non-state actors may also attack shore control centres for using MASS as a weapon against sensitive targets

threats, maritime security cannot be considered complete. What could go wrong, if a SCC is attacked?

As per R-2, there is security dimension into SCCs, and probability of both physical as well as cyber threats. In case these centres are hijacked by hacking, there may be repercussions including stopping the vessel in the middle of the ocean for purposes such as for loading illegitimate cargo, for entering the port by terrorist or to crash into a warship.

Mitigation measures

Cyber-security is evolving as a major proponent against variety of cyber-attacks and all experts considers higher standards to be implemented for AS and SCCs to deter any threats. R-7 perceives that malicious cyber actors may hack the communication link, and stressed on the system and processes resilience to prevent such attacks. Therefore, impetus must be given to regular training (personnel employed at SCCs), drills, audit regimes and vulnerability assessment (penetration testing or red teaming).

Post 9/11 disaster, government worldwide and in particular United States implemented stringent measures for better protection of ports and maritime transport. Consequently, higher security standards were introduced in ports and ships through implementation of ISPS and other measures such as Container Security Initiatives (CSI).

A state with a higher security environment would like to have proactive security control measures at these centres. R-2 imagine that state like US would enforce such measures at SCCs.

The SCC as a control room can be compared with aircraft cockpit unlike VTS or ATC which although directs the safe movement of aircrafts and ships respectively but, do not have the controls.

In the same context, R-2 compared AS/SCC with Germanwings flight³² which was deliberately crashed by its own co-pilot into mountains. He raised concern over the final authority for override button for an AS in such case? Therefore, there is clear need to define the procedures for contingencies, and states would like to enforce higher security barriers in these centres. As a

³² On 24 March 2015, flight 9525 (Germanwings) crashed 100 Km from Nice (French Alps) was a deliberate caused act by the co-pilot.

mitigation measure, R-2 suggested availability of redundancy or override options in other locations to take over/hand over facilities for these ships. Therefore, there would be a need of standby SCCs, which is not only a standby option for intrusion but for other emergencies, and again cyber-security is important into these process. In order to protect against cyber threats, there should be security protocols, passwords and encrypted lines to protect the system. He also highlighted training of professionals as an important aspect.

R-1 and R-2 suggests suitable physical barriers for SCCs. Also, R-2 quote an example of a remote control station that is closely guarded to avoid any calamity at one of the offshore oil pumping facilities in the north sea. Similarly, R-1 concurs, “SCC is a high risk asset” which really need high security both physically and from cyber-attacks.

Since, the role of IMO is also crucial in maintaining maritime security, R-5 suggests that these centres should comply with IMO standards. In addition, he further suggests IMO to regulate standards to make uniform policies and requirement for all coastal states. R-6 also concurs with these threats³³, however believes that SCCs would be the responsibility of individual state. He also mentioned that these threats are arising from the non-state actors and even they are transboundary in nature. So he considers it to be beyond the IMO control and hence would require attention of other institutions too.

SCC is regarded as high priority issue as far as revising IMO instruments are concerned in RSE outcome (IMO, 2021). However, SOLAS chapter XI-2 has not been considered as potential theme for it.

R-3 somewhat maintain same opinion and reiterate that IMO has been regulating ships under its mandate, although there are few exceptions under ISM³⁴ and ISPS³⁵ codes, which are clearly defined³⁶ and limited. Also, IMO has issued some guidance for matters which are beyond its prime

³³ Cyber and Physical attacks on SCCs

³⁴ Shore management responsibilities

³⁵ Port facilities

³⁶ Definition of port facilities (not port)

remit such as non-SOLAS ships or for mooring personnel in ports. He furthered on the complexity of IMO regulations governing SCC as shore-side infrastructure which is subject to national jurisdiction and laws seems to be less likely at the moment. However, there could be some regional solutions³⁷.

Indeed, the SCCs will influence the maritime security atmosphere in the future, and these centres must be secured against all kinds of security threats, cyber or physical. A single hijacked SCC can serve hackers several autonomous platforms that can probably be used as per their wish and fancy. IMO certainly will have a role in securing high standards for these centres.

4.5 Scenario – 2

Scenario-2 relates to the hijacking of unmanned ocean-going AS by pirates or non-state actors (figure 15). The AS is exiting an international strait in the wee hours and suddenly lose contact with SCCs. The SCC crew is assimilating it to be a minor communication/network issue, but all efforts to restore the connection are futile. The SCC crew consequently suspect the hijacking of the vessel.

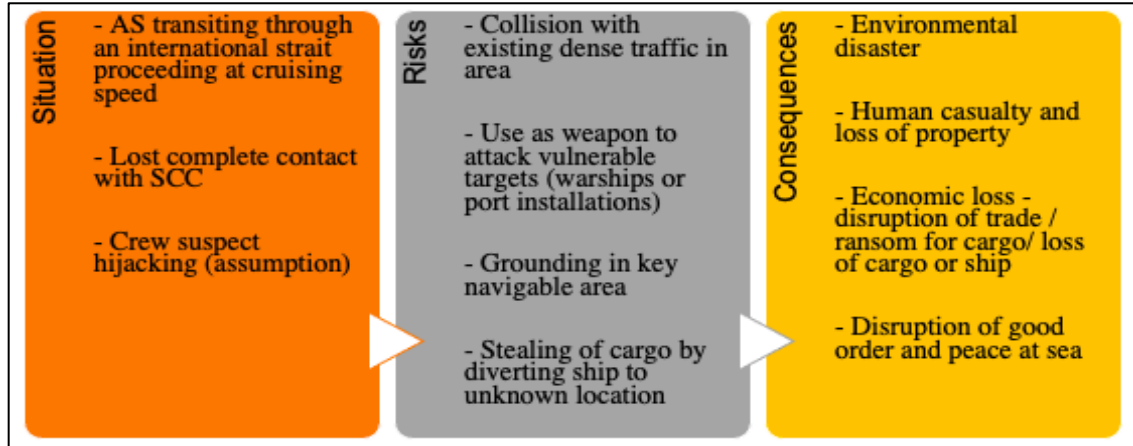


Figure 15. Scenario – 2 “Hijacking of AS by pirates/non-state actors”

Analysis

³⁷ The EC of the EU, for example, has through its directives direct power for matters passed on to the EC by EU Member States which includes ISPS implementation

Vulnerability of technology

One of the major security threats for AS is hijacking, which may result in devastating consequences affecting its public perception as well (Fan et al., 2020). The hijacking of an AS can be attempted by a traditional pirate (motivation financial gains) or an ideological/politically motivated non-state actor group (use as weapon), and both can employ either physical or cyber means to undertake the same.

The act of "piracy" has two distinct offences: the first is robbery or hijacking, with the goal of stealing a ship or its cargo. The alternative is kidnapping, which involves threatening the crew and vessel until a ransom is paid (Tumbarska, 2018).

An autonomous ship is highly technological, fully dependent on networking, AI, and satellite communication, and being a new technology, brings new risks. When in operation, AI technologies may introduce security vulnerability (Heikkilä, 2018). Vulnerability to computer hackers hijacking control is one of the major disadvantages of AS (Li & Fung, 2019).

For unmanned AS, the option for kidnapping and ransom is no longer feasible. So, will traditional piracy be still a threat for AS? According to maritime executive (2019), pirates still have reasons to board a ship: the cargo, the vessel and the potential use of both as smuggling tools or as a weapon. Pirates in Southeast Asia attempt to hijack the ship mainly for its cargo, where crews occasionally suffer serious injuries (Jiang & Lu, 2020b). Since, no one is onboard, AS is an easy target for hijackers partly for stealing information and for taking control of the ship. And, at the hands of hijackers, it will be at their mercy, they may just steal the cargo or do acts of terrorism on a global scale or drive into an oil rig (Eriksson & Gevriye, 2018).

R-4 anticipates that though the chances of pirates using the ship for ransom is less, one cannot underestimate the ability and the ingenuity of the pirates to determine alternative methods by which they can extort money and via take over the AS.

According to R-7, "Probability of physical attacks will be much lower than a cyber event as AS concept is largely dependent on IT systems onboard and ashore. If security aspects are categorised into three elements- people, processes and technology, then technology among these three, is improving considerably whereas people may be considered as a weakest link in security

chain.” R-8 though considers it to be an evolving risk, but maintains same opinion as R-7. On the other hand, R-3 considers that MASS will be more vulnerable to physical attacks by pirates and armed robbers than conventionally crewed ships. Also, almost half participants in survey agreed to SQ10³⁸ (figure 16).

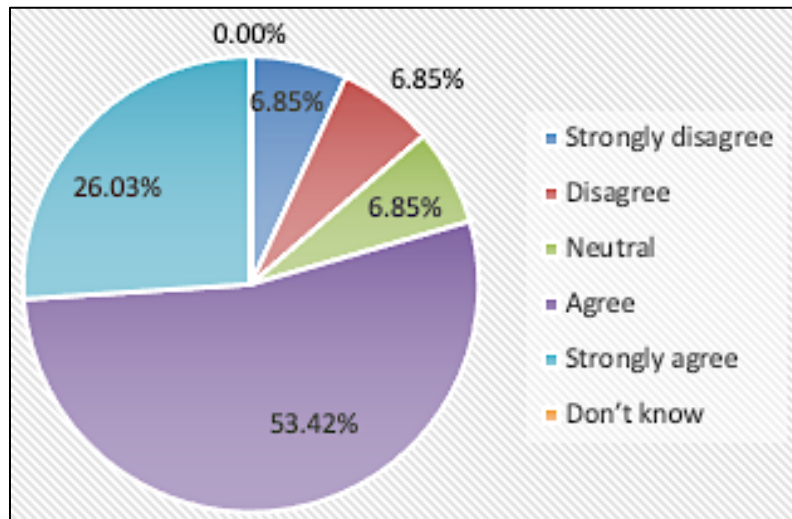


Figure 16. Participants response to SQ 10 (prepared by Author)

One strong reason of pirates targeting AS would be the absence of crew, as, in case of AS, we can assume that there is no resistance from embarking the ship. Whereas, in conventional ships, the crew becomes first line of defence although their life in this case is at stake.

Traditionally, ships operating in high risk areas (HRA) adhere to strict measures including guidance³⁹, BMPs⁴⁰, industry counter-piracy guidance⁴¹ promulgated by IMO. A fundamental advice in one of these circular on piracy or hijacking is “If attackers cannot board a ship, they cannot hijack it”, which is significantly true in the case of conventional ship. However, in order to understand vulnerability of AS, whether, in first place, can it be boarded by attackers or pirates. If answer is ‘Yes’, then whether it can be controlled from onboard positions. And again if answer is

³⁸ Despite the absence of the crew, traditional piracy attacks will affect MASS.

³⁹ MSC.1/Circ.1333/Rev.1, MSC.1/Circ.1334, MSC.324 (89)

⁴⁰ Res.MSC.324, MSC.1 -Circ.1506

⁴¹ MSC.1/Circ.1601

‘Yes’, what else they need. However, if the answer is ‘No’, what else can be done by them. Will they leave peacefully keeping everything intact. These are some of the questions which definitely need answers before AS undertake ocean passage. R-3 explains that though MASS projects are in developing stages, the scene will quickly change in years to come, and it is likely that shipowners/operators will not envisage to opening up routes where risk of piracy or armed robbery is high or observed incidents in recent past.

Nearly all experts during the interview stated that design features of the AS is very crucial factor in avoiding such incidents. R-1 commented to IQ-1⁴²,

“It isn't easy to do something if a ship is designed to not operate from onboard positions. And, it would be tricky to take the ship somewhere since means of steering would not be available onboard, except pirates can try to make it inoperative by shutting down the engines, but then pirates need to have a seagoing tug to steal the ship.”

R-2 as well highlighted the design features of AS, and mentioned about potential MASS designs⁴³ in future .“Ships can be built in a way that even if someone gets onboard, it’s difficult to get into them”. However, it would also be required to facilitate easy access for those to attend emergencies or mechanical failures to tug them easily. And, if a ship can be connected for a good reason, it can very well be connected for a bad reason too.

Jiang & Lu (2020) in their study on piracy in SE Asia highlights importance of influencing factors (ship’s characteristics, environmental conditions, anti-piracy measures) against maritime piracy (Table 5). However, in case of hijacking of AS, all these factors would also change drastically. An autonomous ship may likely have a high freeboard and enclosed structure but is likely to be slow-moving with a limited allowance for increasing speed. Also AS will not have appropriate anti-piracy measures such as lookouts and provision of physical defence measures may have to be provisioned for automatic deployment.

⁴² Do you think there are high possibilities of MASS being hijacked by pirates (physical or cyber) to ask for ransom for cargo/ launch attacks on vulnerable assets or port installations (collision with warships/grounding in navigable areas)?

⁴³ Rolls Royce AS designs

Table 5. Influencing factors of Piracy. Prepared by Author based on information from Jiang & Lu (2020)

Ship Own Risk	Ship type and speed. Low freeboard and slow speed provides favourable conditions for the pirates
External Environment Conditions	Rough weather (monsoonal conditions) poses restrictions on use of small skiffs by pirates. Time is also an important variable, and most attacks are undertaken between 0 and 6.00 in the early morning.
Anti-Piracy Measures	Surveillance by additional personnel as lookouts. ISPS code ²⁴ takes into account additional workload incurred in the implementation of the Ship Safety Plan (SSP). Physical defence measures including barbed wire, bumping drums, propeller arresters, armed protection or remote acoustic devices are some anti-piracy protection measures

R-3 in this context, mentions that :

“Anti-piracy measures which are set out in the current BMPs almost exclusively require the crew to set them up and without any crew on board AS would have to activate automatically, which adds another layer of automatization”

According to IMB (2021), 195 piracy and armed robbery incidents were reported against ships worldwide in 2020, higher than 2019 incidents, and included three hijacked vessels, 20 attempted attacks, and 161 boarding by pirates.

There are real chances that modern pirate will change their tactics with this ultra-technological change. If the pirates board the AS somehow, will they be able to take over the ship? There would not be any accommodation, but there is still a kind of bridge and a “AI control room” and an engine room. So, how will they access into the AS control room?.

According to R-6:

“To hijack the vessel by entering in its control system or network demand higher knowledge on IT skills/ hacking capability which is less likely to possess by ordinary pirates or hijackers.”

Whereas, R-8 had different opinion on this aspect who believe *“There will always be some point of access for a human to interact physically even on fully autonomous ship”*

R-7 believe that accessibility to AS will depend on degree of autonomy, and with proper preventive measures and controls, there are ways for an AS to raise alarm in the event of security breach.

In August 2021, an attempt of potential hijacking of Panama flagged vessel Asphalt Princess was reported in Gulf of Oman 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. On the same day, 5-6 tankers in the region also reported problems with their navigation equipment which led to the speculation of a possible cyberattack on vessels in area (Maritime Executive, 2021). R-3 also anticipate higher risk of terrorist attacks using the MASS as a weapon than conventional ships, especially in waters of strategic and economic importance (Suez, Panama canal) or where, the risk of an environment disaster is very high. Whereas, he thinks that intentional collision with warship is not very likely due to higher alertness and maritime awareness⁴⁴ on a warship than on merchant ships.

In same context, R-6 anticipates

“The situation is different in the case of maritime terrorism, in which ideologically and politically driven non-state actors can recruit skilled IT personnel, and MASS can provide them with a window to attack vulnerable targets. A terrorist organization can identify skilled individuals among its cadre/sympathizers and hijack MASS without even sending their forces to do so. Moreover, it will cut their preparation time and the chance of being discovered by security personnel and law enforcement agencies, and they will be able to conduct an assault anywhere in the world as per MASS operational reach”

The biggest concern that was raised by almost all experts was cyber-security or threats of cyberpiracy as compared to physical pirate attacks citing the design features of an AS, which most of them feel is impenetrable.

Cyber-attacks exploit communication network vulnerabilities, which jeopardise the integrity or availability of data and ship control systems (Bolbot et al., 2019). AS will be vulnerable to cyber-attacks, and the most serious risks may not be related to the ship or its cargo, but rather to the threat

⁴⁴ Surveillance equipment and manning state

to infrastructure along the coast and offshore if the ship is under alien command. When traveling at maximum speed, even relatively small AS have a significant kinetic energy and hence pose a serious threat. A cyber-attack could be compared to the terrorist attack on the USS Cole, a guided missile destroyer of the US Navy. 17 sailors were killed as a result of an attack by a tiny fibreglass boat carrying explosives and two suicide bombers (Vinnem & Utne, 2018).

In survey almost 50% respondent strongly agreed and 38% agreed with SQ11⁴⁵ (figure 17), making cyberattacks as a major threat for AS.

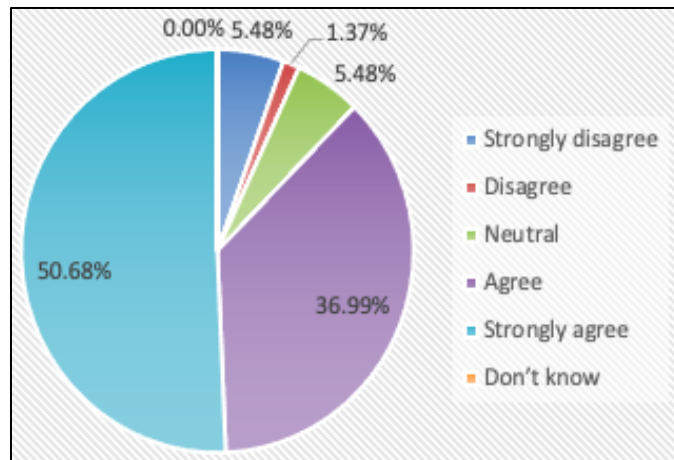


Figure 17. Participant response to SQ 11 (prepared by Author)

According to R-6,

“Cyberattacks will be a strong possibility with the potential of gaining control of a MASS for misuse.”

Whereas, R-1, considers :

“For cyber security, sufficient technology is existing, and only system has to be correctly designed and subsequently proper crypto solutions to be used”

Another aspect which was highlighted is jamming and spoofing, which can be used by criminals/non-state actors against these ships. According to R-1, jamming is one of the significant concern other than cyber-security, which should be managed. R-2, however consider that jamming

⁴⁵ MASS activities may be more vulnerable to cyber-attacks, including cyber piracy

can still be managed with suitable AI software which can detect signal anomalies. But, spoofing on the other hand can confuse AI to undertake undesired evasive maneuvers.

Further, hacking the AIS transmission would be 50% of the job to take control of the ship, which are not easy to fix as well, and would take a considerable amount of time and money (Eriksson & Gevriye, 2018). SMEs in Roberts et al., (2019) study anticipates issues with jammers effects on heat or pressure or gas sensors onboard, which may lead to an explosion as well. And, if the goal of the attacker is psychological impact, they would do it within a port or near the coast.

All in all, technology vulnerability will decide fate of these ships against security threats. R-5 feels that : “systems overall needs to be resilient to withstand any form of attack”. Figure 18, depicts a systematic diagram of hijack attack on AS with associated variable.

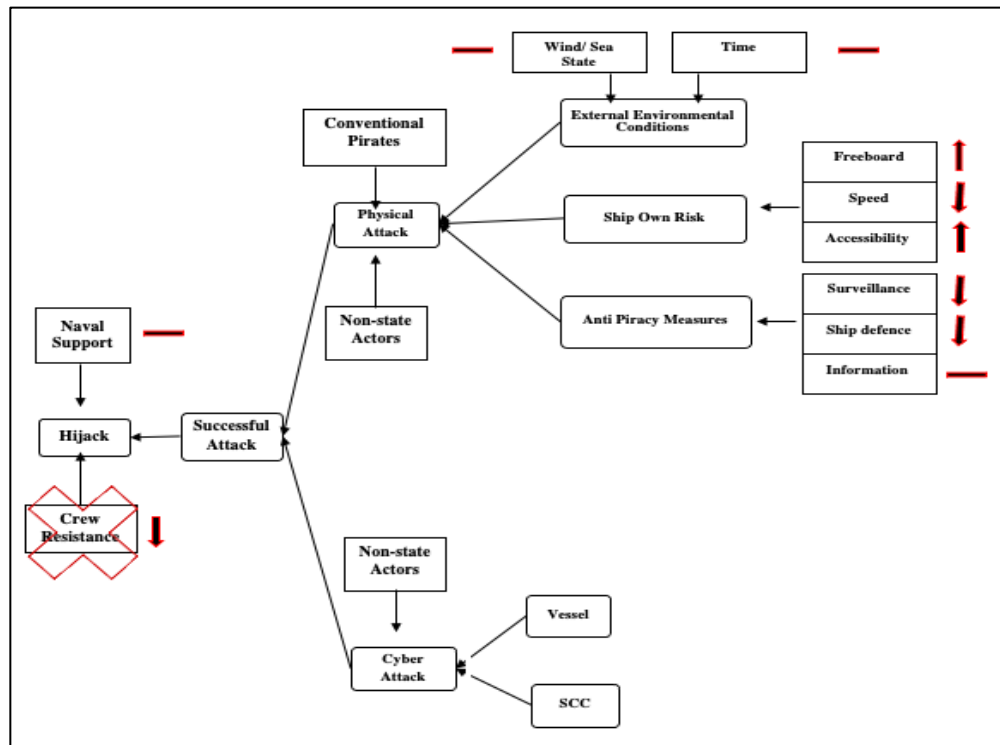


Figure 18. A systematic diagram of Hijack attack on AS. Adopted by Author based on information from (Jiang & Lu, 2020; Tam & Jones, 2018b)

Mitigation measures

AS is being considered as potent solution against pirates, biggest proponent for this is the likely design features of the ship. The unmanned state, invariably make it easier to recapture the ship. In emergency, SCC can take evasive actions, seek assistance from law enforcement authorities. However, there are still dilemmas associated with it. What if, pirates or hijackers set ship on fire, then here would still be several serious consequences. Stopping a cyber-hijacked vessel would also be difficult as it may act under alien command.

Design is the central factor to prevent any unauthorised element onboard these ships, which is highlighted by maximum interviewees. R-3 speculate that MASS may be designed so that any unauthorised person trying to take over a hijacked ship will not succeed due to the security regime in place. Any prudent MASS operating shipping company will ensure a high state of access control.

As discussed in the previous scenario, once a ship is hijacked through cyber means, sealing off AS structure will probably not be a single solution, and local measures are needed to prevent misuse of AS.

Like BMPs for conventional ships, R-1 and R-7 considers enhanced measures for AS, such as motion detectors, heat sensors and additional barriers to detect and prevent physical attacks. R-1 also suggest implementation of better cooperation with local authorities. R-5 as well feels that, there is a need to develop partnerships, establish cooperation in which various states and law enforcement agencies should be involved in the development of AS. All states in a role of coastal state should acquire capabilities to control a MASS.

R-9 considers that in the first place, AS should avoid passage through designated HRAs and as protection measures, current methods⁴⁶ as per BMPs may be employed. However, autonomous fire defence system or use of firearms as an option may not be viable as it would not be accepted by shipping owners and regulators.

A cyber-attack response and prevention plan based on vulnerability identification must be maintained for cyber-security. To avert a hacker assault, IT and security specialists may need to

⁴⁶ Barbed wire, and use of non-lethal weapons

conduct regular incident tests to detect weaknesses and upgrade the onboard security program (Li & Fung, 2019).

Whereas, R-3 opined that

“Key concept is risk assessment, therefore, any mitigating measure will depend on identified risks.” And also stresses on use of IMO approved guidelines⁴⁷, recommendations⁴⁸ for effective cyber security.

R-4 was also skeptical in commenting on the actual solution until the ship actually starts operating but adds that there will be a requirement for more through ISPS cyber guidelines that relate to MASS.

4.6 Scenario - 3

Scenario-3 relates to an incident of armed robbery or petty theft onboard unmanned AS (figure 19). The AS, a small container ship is scheduled to enter a riverine feeder port in the high tide and has been ordered by port control to drop anchor in the outer anchorage on arrival. While maintaining at anchorage in the night, SCC crew observe several boats in the vicinity. Later, the crew detects some unusual movement onboard ship, and immediately alerts the port authorities. Consequently, a patrol vessel arrives on the scene, but is unable to locate any boat alongside AS or in vicinity. On arrival at the port, the AS operator’s and port authority detects theft of some valuable cargo and damage to several equipment.

⁴⁷ MSC-FAL.1/Circ.3/Rev.1 – Guidelines on maritime cyber security assessment , MSC.1/Circ.1639 – Guidelines on cyber security onboard ships , ISO/ IEC 27001 – Standard on Information Technology

⁴⁸ IACS recommendations on cyber resilience (Rec.166)

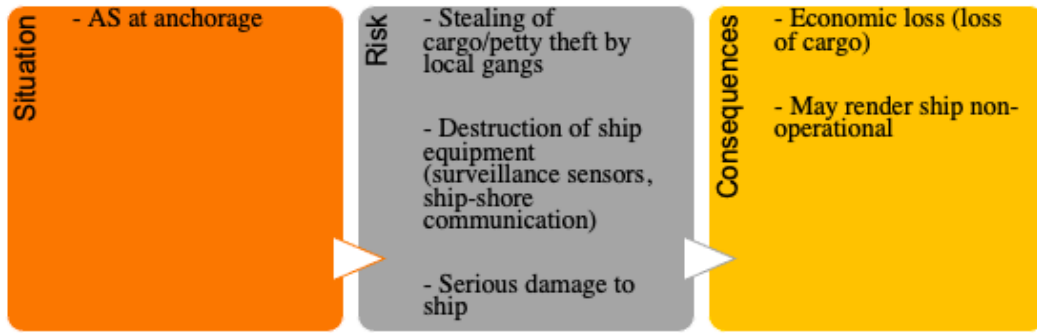


Figure 19.Scenario -3 “Armed robbery”

Analysis

Vulnerability of technology

It is very likely that many future attacks on maritime transport system will be multi-modal including both a cyber and a physical component. Thus a cyber-attack can also become precursor to a physical attack and vice versa (Roberts et al., 2019).

Armed robbery on ships is a contemporary challenge to shipping, and it has a global influence on maritime trade and security. IMO’s Resolution A.1025 (26) “Code of practice for the investigation of the crimes of Piracy and Armed Robbery against ships” defines armed robbery (IMO, 2021a).

(a) “Any illegal act of violence or detention or any act of depredation, or threat thereof, other than an act of piracy, committed for private ends and directed against a ship or against persons or property on board such a ship, within a State's internal waters, archipelagic waters and territorial sea”

(b) “Any act of inciting or of intentionally facilitating an act described above”

Since the reward value is low, maritime robbery related crimes are opportunistic, occurring when the vessel is at port or anchorages. In typical robbery cases, a few men with knives easily

overpower the crew and take their belonging and ship's items (Tumbarska, 2018). In response to SQ 15⁴⁹, a rather mix reaction was observed (figure 20).

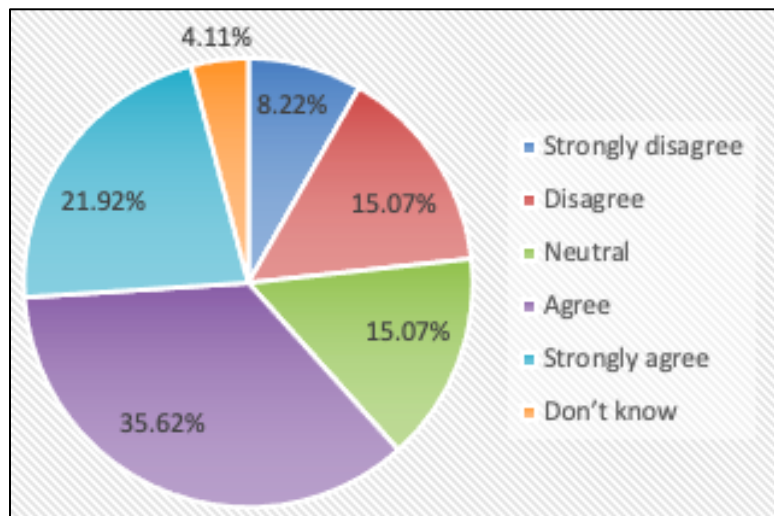


Figure 20. Participants response for SQ15 (prepared by Author)

Dehart (2013) identified two types of pirate attacks in Southeast Asia. Small-scale attacks by "opportunistic sea robbers" or "sea-faring hooligans" that occur while ships are at anchor. The other being the major attacks for hijacking the ship. Experts also had varying opinion on this aspect, and believe that crew absence may influence armed robbery and would depend on security environment in which AS is operating. R-1 and R-2 consider that to some extent these threats may increase marginally in comparison to normal conventional ships where crew and guard presence may deter these incidents.

Moreover, Jin et al. (2019) described that vessels at berth or anchor are more vulnerable as most attacks occur during such conditions, especially at night and in good weather. In addition, crew actions against these attacks are some positive factors to deter the attacks.

⁴⁹ SQ 15 - The absence of crew may encourage criminals to undertake armed robbery/petty theft onboard MASS

R-3 on IQ-5⁵⁰ as well, pointed that the ship is more susceptible to armed robbery when it is stationary or drifting. Further, the vulnerability of a ship is more when it is outside the port as it is harder to employ shore services.

According to Roberts et al. (2019), the criminals can hack into a cargo management system and identify valuable cargo locations on a ship. It may enable them to make a very short and efficient raid on a vessel, going right to the container of interest. The cyber attacker can even influence the loading of containers so that those of interest are placed to be accessible.

According to R-2, it would be a major challenge for port authorities and law enforcement agencies. Whereas as per R-5, there would be possibilities of such incidents. However, it will be less and will be determined by the coastal state's maritime security measures and security situation in such locations. If the coastal state's law enforcement is inadequate, occurrences like piracy, armed robbery, and burglary will continue to occur. R-2, R-4 and R-7 have different views than other experts, and they consider that due to difficult access, probability of such incidents might be quite low.

Mitigation measures

IMO resolutions, circulars and guidelines over the years aimed to prevent and suppress armed robbery against ships. In addition, IMO acknowledges that positioning of privately contracted armed security personnel (PCASP) has become an accepted industry. However, IMO still stresses on other protective measures including BMPs.

In case of AS, other suitable means would be employed to suitably secure maritime security. AS security will heavily depend on technology and cooperation.

R-2 mentions to IQ-6⁵¹, “Access to ship should be made difficult”. According to R-1 and R-7, “AS would be equipped with variety of surveillance equipment so that SCC can monitor the aspects. With strict hardening measures implemented for surveillance (motion detectors, heat sensors) and alarms, the breach can be detected easily and responded”.

⁵⁰ Would you consider a higher probability of MASS being boarded at anchorage or in ports by armed robbers?

⁵¹ What solutions, in your opinion, could prevent such possibilities and have adequate security of vessels?

In the same context, Hoem et al. (2018) point out to drawbacks and limits of automation. AI or programmed technology can only deal with simple, complicated situations, whereas shipping is regarded as complex, with unforeseeable factors that need infinite solution space. Moreover, “The dynamic maritime environment with sea, current, weather, topography, manned and autonomous ships is such a complex environment and will for a very long time need a human to step in and resolve problems out of the range of automation” (Hoem et al., 2018, p.423). This viewpoint also brought forward by Kobylinski (2018), who feels that maritime situations are hardly predictable. The unpredictable marine conditions can seriously impede the design of a serviceable surveillance system and electronic measures onboard AS.

R-3 on the other hand opined that measures depends on the risks posed. Therefore, two fold approach may be maintained by operator’s which include security measures which are quickly to implement and equipment to use in case of a general higher risk of attack. The measures can be implemented well in advance prior a MASS enters service on a particular route⁵². The second layer would be to have a constant monitoring for dynamic threat. This could for example, mean a MASS operator avoids a port call for which there is a security level 2 (avoiding the risk altogether). The other dynamic measure would be the employment of PCASP where the port, coastal and flag state permits.

R-6, firmly believes that “*scarcity of sources*” and “*state’s interest*” to implement measures may influence these factors. R-5 and R-6 both considers law enforcement effectiveness as a major proponent to address these issues.

Van Hooydonk (2014) and Wrobel (2017) as well pointed at the drawbacks of technology in terms of situational awareness and reliable functioning of technical components. Notwithstanding port security and other measures, the security of the AS will be purely managed by technological means, whose vulnerability as well as security situation in area will decide numbers and severity of these incidents onboard AS.

⁵² For example, a ship which is planned to transit the Red Sea, measures may be implemented in advance with latest BMPs.

4.7 Scenario - 4

Scenario-4 relates to an incident of stowaway onboard unmanned AS (figure 21). An ocean-going AS is on a voyage to Europe. During routine visual inspection of the engine room, the OOsW in SCC observe three person inside the engine room. On close examination of the situation, it confirms that all three are looking desperate, agitated, and trying to escape from the engine room to other compartments.

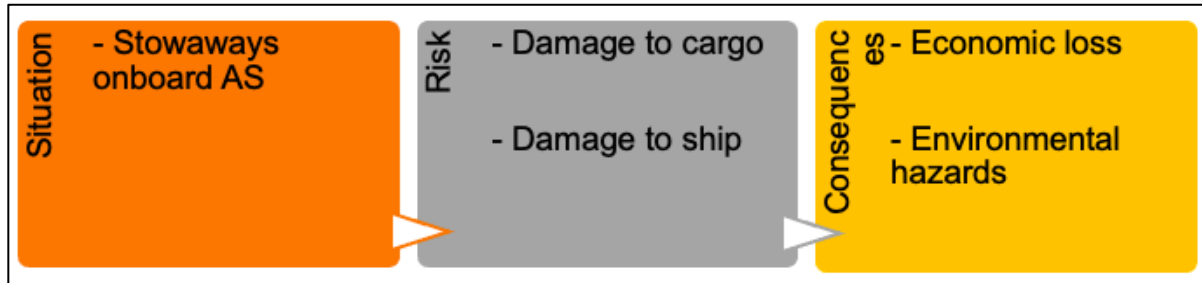


Figure 21. Scenario-4 “Stowaway onboard MASS”

Analysis

Vulnerability of technology

Stowaways are a hazard to maritime security and the shipping industry since they have the ability to endanger ships and cargo, as well as disrupt shipping operations (Aguocha, 2018).

For AS, stowaways seems to be a major concern for most of the participants who were interviewed. According to R-1, R-2 and R-7, this is one of the aspect which needs to be considered strongly with AS, and R-1 consider it as a higher risk for MASS. However, considers that it may be a liability issue for the ship owner rather than a security hazard. R-7 expect the stowaway issues to be bigger threat than piracy. In contrast, R-5 and R-6 think other way round. One thought that R-6 shared.

“The lack of crew onboard MASS, creates a difficult/unfavourable situation for stowaways because there will be fewer or no life-supporting systems onboard. Furthermore, after loading or unloading the cargo, these ships can be sealed off, and all entry points can be closed. Access points can also be monitored remotely at the same time. However, the expert believes that stowaway (s) can sneak into a MASS with the assistance of shore-based workers and stringent access control to the harbour facilities, including MASS, is the only viable solution”

R-4 opines that the chances of stowaway getting onboard are low as MASS is anticipated to maintain the highest ISPS code requirements. However, searches must be continued as the present system for stowaways before departure.

As discussed in scenario 3, technology and automation has its own limitations. Moreover, majority of ISPS complied ports are served with high end surveillance systems to detect presence of unwanted or unauthorised person in port facilities. In addition, physical security measures are also seemingly integrated with electronic surveillance systems in these ports. Despite strict measures in ports around the world, stowaways somehow finds their way onboard ships.

Certainly, stowaways are capable of creating major security hazards. In Oct 2020, an incident involving 07 stowaways onboard MT Nave Andromeda created a major security fiasco in UK waters, and local police, coast guard and navy had to respond to control the situation. It was a major security concern that British special forces (16 member boarding team) were tasked with securing the ship and detaining several violent stowaways (Maritime Executive, 2020).

Stowaways may pose a risk to the ship as well. In *United Brands Co. v M. V. Isla Plaza*, stowaways destroyed the ship by lighting a fire. In another case, In *American Home Assurance Co. v Sletter M/V*, the entire food-based cargo was tainted by stowaways urine and faeces, and the cargo had to be destroyed, resulting in a significant financial loss for the cargo interests. Cargo risks are not always physical, they can arise as a result of a long voyage in which the ship diverges to disembark stowaways (Aguocha, 2018).

The examples mentioned in conventional ships above are also anticipated in AS view the infiltration can still happen through cargo from ports, at anchorages or while underway view human instinct to escape their squalid living conditions. Assuming a AS laden with dangerous cargo, serious damage to environment and human may also be caused. In survey, just less than a quarter strongly agree, 38% agree whereas 7% strongly disagree and 16% strongly disagreed, with the SQ16⁵³ statement (figure 22).

⁵³ There is a significant probability that stowaway will target MASS more than regular ships

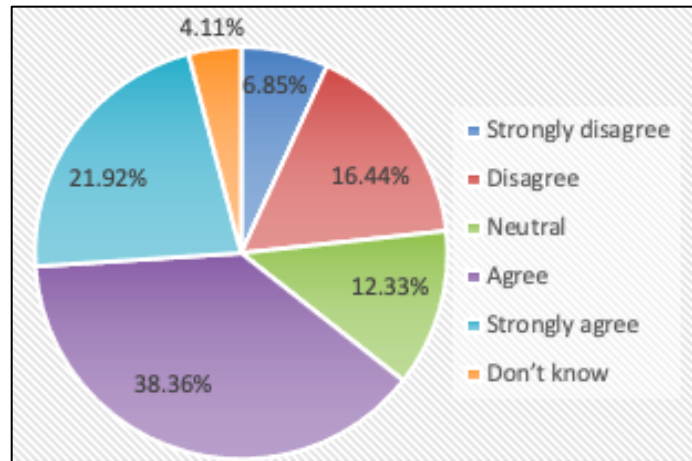


Figure 22. Participant response to SQ 16 (prepared by Author)

Under ISPS, security level-1, provision is made for control of access to ships⁵⁴, control of embarkation of persons and their effects⁵⁵, and monitoring of restricted areas to ensure that they are accessed only by authorised personnel⁵⁶. The presence of stowaways on ships is a breach of the Ship Security Plan (SSP) and a clear violation of the ISPS Code. Despite ISPS measures, the stowaways persistently manage to board ships using ingenious techniques (Aguocha, 2018). R-3 also highlights this as a problem of unauthorised access to ports and port failures to prevent unauthorised people to enter port facilities. However, maximum stowaways cases are observed in African continent where operation of MASS is less likely.

For AS, R-2 believe that,

“The problem will continue to exist because even though the ships are designed to prevent ingress, people may sneak into containers, lorries or through other means”

Stowaways have their preferences⁵⁷ and mostly target vessels which make short trips, have short transit period and operate at high speed (Aguocha, 2018).

⁵⁴ Section 7.2.2

⁵⁵ Section 7.2.3

⁵⁶ Section 7.2.4

⁵⁷ Ro-Ro cargo ships, followed by ferries, containerships and general cargo ships

R-6, for IQ7⁵⁸, mention

“AS will be slower and have a longer journey period, requiring the stowaway to carry more provisions (s).” And contemplate that stowaway probably would not target these ships due to longer travel period.

Mitigation measures

Most stowaway incidents are organised activities by local or international human or drug trafficking groups. In some cases, port security may also be involved in the racket (Aguocha, 2018).

In order to avoid stowaways incidents onboard AS, According to R-7,

“There would be certain natural defence such as lack of gangway, restricted or no access, still stowaway can enter the ship with various other means. Therefore, there is a greater need for shifting focus from the ship side to the port due to absence of crew. The port would be required to strengthen their security measures specially on those terminals where these ships will be berthed”

R-5 also highlights the importance of port and law enforcement:

“Implementation of a pre-departure check could ensure the safety of the vessel from any unneeded objects or personnel (stowaways). These procedures could be implemented in collaboration with a MASS operator by port state authorities (PSC)”

In response to SQ22⁵⁹, majority of participants polled in favour of compulsory security checks prior leaving a port, which can be initiated by the MASS operator, and ensured by the port authority under their AS departure check list (figure 23).

⁵⁸ In your opinion, to what extent non-presence of the crew may render MASS a soft target for stowaways?

⁵⁹ MASS security clearance including nil stowaway must be made compulsory prior leaving a port

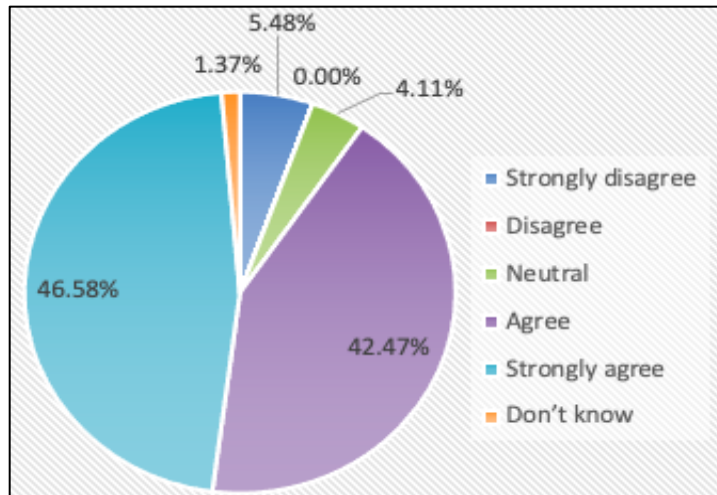


Figure 23. Participant response SQ 22 (prepared by Author)

In addition, port may also have to re-evaluate their port security assessment under ISPS code for AS terminals.

4.8 Scenario – 5

Scenario-5 relates to an incident of an unmanned AS carrying illicit material in cargo (figure 24). The law enforcement agency in a coastal state gets an input regarding the AS carrying a large shipment of drugs. Consequently, a law enforcement vessel proceeds to the location of the ship to investigate. However, fails to communicate with the AS's SCC. A VBSS team is launched to board and inspect the AS on existing suspicion and inputs.

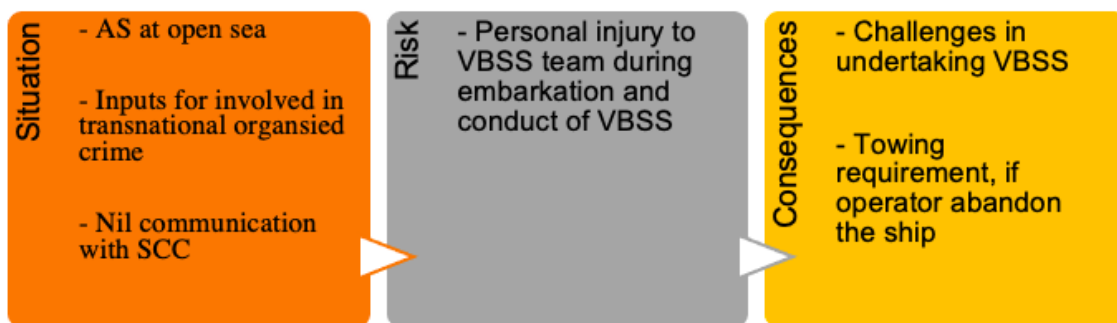


Figure 24. Scenario-5 “AS involved in transnational organized crime”

Analysis

Vulnerability of technology

The use of AS for illegal objectives, particularly smuggling commodities, is one of the new technologies that has international law implications. The criminals may also turn to AS to further their operation in different ways, and small AS may be used to transport good illicitly.

The interviewees state their concern. However, has varying opinions on the subject.

R-1 in response to IQ10⁶⁰,

“Due to design features, autonomous unmanned ship would not be a viable option for such transnational organised crimes and probably it is easier to do that with a conventional manned vessel than an autonomous vessel. Further, with appropriate surveillance, it would be difficult to do that. But, it is an open question and hence difficult to judge at the moment”

Again, like stowaways, drug traffickers are found to be extremely ingenious. Moreover, they will not be having scarcity of money unlike stowaways. They are likely to find several ways and means to hide big consignment of illicit materials and will also escape jurisdictional purview of any state. McLaughlin & Klein (2021) highlighted the practical nuances in apprehending the culprits in such cases.

R-7 mentions, *“MASS may change the pattern of criminal activities, the current practices⁶¹ will however depend on level of port facility security.”* In addition, R-8, raised issue of accessibility by port workers and said, *“The other factor which is likely to influence is how AS is going to be berthed as a vessel can be accessed by the port personnel including stevedores.”*

According to (McLaughlin & Klein, 2021) two possibilities contemplated in use of AS to further drug-trafficking operations, first the small submersibles or semi-submersibles (currently in use) altered for autonomous operation, which may or may not be registered to a particular flag. The

⁶⁰ Do you think there are high possibilities of MASS being used by criminals for transnational organized crimes?

⁶¹ Exploitation of human element (through stevedores, contractors, and by involving crew members) and other using covert divers to attach waterproof packages of drug to hull surface.

other case, is use of usual cargo AS being used for drug trafficking, which is transporting containers, may also has illicit cargo on board.

R-2 and R-5, hold similar opinion about use of AS for drug trafficking including usage of containers. R-5 further consider potential abuse of AS,

“MASS can be used for such purposes including transportation of WMD or can be used like a bomb when it is controlled by unnecessary entities who may use it for disturbing economic activities of some coastal state”

In response to SQ 14⁶², a rather mix reaction was observed (figure 25).

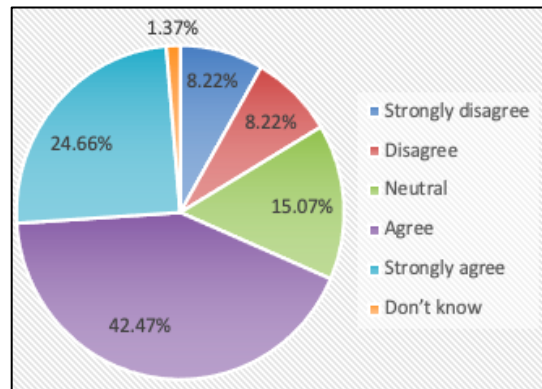


Figure 25. Participant response SQ 14 (prepared by Author)

R-4 also envisages this as an excellent opportunity for drug smugglers since no one can get captured, and criminals can transport drugs anonymously. R- 6 in this context believes that :

“It may be difficult to use MASS in commercial shipping as a platform. Nevertheless, culprits can use their own automated, autonomous craft for such activity.”

R-3 contemplates it to be a matter of enforcement, willingness and capabilities of port, coastal, and flag state to prevent criminal activity. The absence of crew including master may however raise other concerns including that of liabilities.

⁶² SQ 14 - Autonomous (crewless) ships, in comparison to conventional ships, would become a preferred choice for criminals to undertake transnational organized crimes (arms/drugs/human trafficking)

The LEA while proceeding for interdiction of drug smuggling AS, may have to deal with both legal and technical challenges. In first instance, LEA have to secure concurrence of flag state (if registered), deal with jurisdictional issues⁶³ (McLaughlin & Klein, 2021). Allen (2018) has also observed the crucial nature of VBSS operation in the case of AS. He raises a valid question “how to conduct a boarding when there is no master or crew to answer questions regarding the craft’s nationality, to manoeuvre the craft to accommodate the boarding, or to present the necessary documents once a team is on board” (p.491).

Mitigation measures

All participants considers greater role of port security. R-7 consider that the current trends of exploiting human element or covertly attaching waterproof packets to underwater hull can be checked through effective port facility security, and expect a paradigm shift in responsibility of LEA and the concerned port authorities .

“A shift in security strategy is expected and agencies may have to strengthen their infrastructure within port facilities and adapt according to changing environment based on the operation of these ships”

R-4 also consider security and checks prior to departure is important for MASS.

Law enforcement at sea will also be affected accordingly. If a vessel carrying illicit material need to be boarded outside territorial waters (TW), there would be an expectation of taking prior authorisation from flag state to board the ship. Within, TW, consent would not be essential to take action against foreign flag AS in the exercise of criminal jurisdiction under article 27 of LOSC. However, in each case, LEA is to wrest control of the vessel and technological intervention (McLaughlin & Klein, 2021).

R-2 shared his perception on control of AS:

“As a matter of fact, the law enforcement agencies would always like to have certain override control mechanism wherein they can control MASS to probably stop, manoeuvres, heave to in a

⁶³ “Extra-territorial reach of the relevant drug-trafficking offences as incorporated in State’s national law”, legal issues in exercising control of AS.

position to undertake boarding.” R-2 anticipates some form of control, based on radio line of sight which can be used by different agencies including pilots during berthing of ships. However, foresees legal, responsibility issues during such control as ship owner may be reluctant to involve other agencies with AS operation. This may however be exploited by culprits as well. R-4 also acknowledges that LEA can access the ship in a similar way as pilots in ports.

Once AS start operating in the international waters, the issues of law enforcement and inspection will come up, and AS operators have to allow LEA inspection teams to even board in some cases prior making port call to check and prevent security threats. On this aspect R-1 predicts that international MASS traffic is expected, which may be based on mutual bilateral agreement between the flag states and coastal state, and these agreements would probably regulate the inspections regime onboard AS. The flag state in such cases have to provide enough assurance about security measures to the coastal states. The use of VBSS or boarding will also restrict view nil crew onboard MASS, and this may further pose higher risk for boarding teams as these ships are not constructed for such operations. However, this requires implementation of other types of regulations to avoid need for boarding in open waters.

R-8 anticipate:

“There could be some kind of digital passport for these ships, which might obviate need of boarding of AS. However, I still believe the physical inspections will take place”

High level of coordination is expected during MASS operation, between flag state, respective coastal state and AS operator. LEA may have to maintain sufficient readiness to deal with MASS security contingencies, if any.

R-5 suggest that a common infrastructure for operation of AS would be essential for better cooperation. Further, anticipate that “VBSS would not be possible and essential as far as CS would be cooperating with MASS operator.”

The LOSC anticipates that States may exercise jurisdiction over foreign-flagged vessels on the high seas consistent with either the right of visit⁶⁴, or the right of hot pursuit⁶⁵. Each of these rights is tightly circumscribed in deference to exclusive flag State jurisdiction (Fink, 2018; Kraska & Pedrozo, 2013).

During any VBSS, which either complied or non-complied has certain procedures and even a simple boarding operation, can go wrong under hostile conditions. A boarding team, having suspicion on a AS, may have to proceed with utmost caution. R-2 state:

“Practical challenges will be experienced by law enforcement agencies including communication issues with SCC operators during such operations”

R-3 believe that any armed intervention onboard AS would not take a risk as far as human life on board the ship itself is concerned. Overall, R-3 don't foresee any adverse impacts on maritime security and law enforcement but expect change in measures for MASS operators and port receiving MASS. Also, LEA dealing with any crewless ships, new procedures and protocols will need to be developed by IMO and national administrations to ensure ships operate under a legal framework.

⁶⁴ Article 110

⁶⁵ Article 111

Chapter 5 – Conclusions and Recommendations

5.1 Introduction

This chapter summarises the study's findings of the implications of MASS on maritime security and law enforcement in form of conclusion. Accordingly, recommendations are suggested for effective management of maritime security in MASS era. Finally, the limits of the study and the scope of future research are covered.

5.2 Conclusion

From analysis and data processing, the conclusion for RQs is as follows:

RQ-1: What are the likely impacts of autonomous unmanned ship on maritime security and what mitigation measures should be adopted to address these impacts?

The result indicated that there will be visible impacts of AS on maritime security. The present day conventional piracy may see a downward trend due to anticipated structural design of MASS and also due to less technical expertise of traditional pirates as well as low bargaining capacity to secure financial gains. However, this cannot be completely predicted. Moreover, initially, AS will be used only in Europe, northern America and few parts in Asia. However, the risk cannot be completely zero, and there may be attempts by pirates to embark AS. Cyber threats on the other hand will become major risk for the maritime security through AS which need to be managed effectively to prevent severe consequences. Opportunity may be explored by non-state actors, terrorists by hiring technically superior persons to launch attacks and disrupt trade. The criminals may use jammers to disrupt GNSS signals, which may require considerations. However, system or AI can be developed which can detect such anomalies. Cyber attackers may also use spoofing techniques to confuse the AS, where AI may undertake actions which may also result in security hazard.

The threats of armed robbery or petty theft may be higher onboard AS due to absence of crew. Similarly, the exploitation of AS by stowaways is considered to be a bigger threat which need to be dealt appropriately. The use of AS for transnational organised crimes would remain relatively same as criminals may continue to use other means to embark drugs or illicit items in

containers and hiding it in cargo. However, the unmanned state of ship will prevent criminals to approach crew and exploit human element to undertake the same. On the contrary, human error or involvement may still persist since AS will be embarked by port personals and workers who can embark these illicit items onboard AS. On a higher scale, criminals may employ or operate independent AS to undertake their activity.

The other major aspects that emerged out of AS is SCCs, which are considered to be a vulnerable target, and will need special attention from both physical as well as cyber security. SCC will influence future maritime domain. Any form of infiltration means the infiltrator has direct access to the AS being operated from the centre. SCC communication infrastructure as well can be targeted by the hackers. Further, the human element would shift from ship to shore and may still influence security aspects.

Despite all concerns, there are chances that overall maritime security may improve as MASS would be relatively complex with expensive systems, and only serious owners and operators with more considerations to security will invest in such ships.

The mitigation strategy to address AS impacts on maritime security may involve high level of coordination and cooperation between involved stakeholders including flag states, coastal states, SCCs, the ship owners, operators, the port facilities, or the law enforcement. It is critical to understand what kind of remote craft is being operated and a uniform coordinated approach is adopted to assess the security.

Overall, the inclusive measures including onsite surveillance (motion detectors, sensors, camera and alarms), difficult or impenetrable access, would act as mitigation measure to detect and prevent any infiltration. Further, the responsibility will shift from seafarers to shore authorities. Therefore, effective maritime security and law enforcement by port authorities, coastal states and law enforcement agencies will be essential to prevent incidents onboard AS.

RQ-2: What are the challenges anticipated by maritime law enforcement agencies in the autonomous shipping, and how should these challenges be addressed?

The analysis of literature, survey as well as opinions of experts clearly points out towards enhanced role of law enforcement agencies in ensuring security of MASS in their coastal waters and deal with the implications of MASS operation on maritime security. It is estimated that MASS will introduce new challenges for the coastal states, port authorities, and law enforcement agencies in managing maritime security within their operational areas. Therefore, clear shift in responsibility will be seen in future where role of even SCCs crew would be restricted due to poor situational awareness. Considerable requirement may also exist to upgrade the technological competency onboard law enforcement platforms (ships) to interact (handle) or in some cases control these vessels. As mentioned by experts, there would be a paradigm shift how security of these ships and maritime security will be managed in future. The conduct of VBSS operations will also be affected, and by and large would be difficult to undertake onboard MASS due to access constraint, absence of crew and liability issues. However, at times, these requirements need to be fulfilled where suspicion exist that the ship is being used in illicit activity for which procedures and protocols need to be formulated. Alternate arrangement in form of bilateral agreements shall be undertaken with states employing MASS which also involves other coastal states. Therefore, there will be clear need for agencies to promote high level of cooperation and coordination with various stakeholders.

5.3 Recommendations

Following recommendations are suggested to effectively manage maritime security threats, and strengthen law enforcement in autonomous ship(s) era :

- A high level of participation from regulatory bodies, member states (element of law enforcement agencies), and the MASS developers is needed to develop global strategy to facilitate MASS operations. Research efforts may be directed for establishing potential gaps to make AS operations secure and resilient against man made threats.

- A careful look is needed by the MASS developers to construct ships to prevent maritime security incidents while keeping law enforcement perspective in mind. In order to have a situation where a risk is maintained as low as possible, strict access control, effective surveillance techniques, higher grade of cyber security solutions needs to be used, which needs to be regularly upgraded.

- Enhancement of port security measures including security risk assessment should be undertaken by those ports which are planning to operate AS.

- IMO, and other member states must impose regulations to mitigate new security risks so that unmanned shipping gains the trust of the maritime transport industry.

- SCC emerging out to be a critical component needs to be protected with stringent measures from both physical as well as cyber angle. Also, redundancy is to be maintained for each SCC.

5.4 Limitations and future research

Indeed, there are limitations of this research, which signifies that suggestions for future study can be made. In the absence of historical data or significant research in this area, AS exact implications on shipping maritime security and law enforcement may not be effectively quantified. Moreover, the concept of AS is vast and expanding rapidly. Its impact on maritime security found in this study can only be a jigsaw piece of a much larger puzzle.

In future, research efforts may be directed towards a specific scenario. In particular, MASS operators may have to conduct a security risk assessment for autonomous ships and SCCs employing the requisite tool since these centres will now significantly influence the maritime domain. The other significant aspect is the redundancy of SCCs and the feasibility of local controls with law enforcement agencies or coastal state(s) to manage exigencies at sea. Nevertheless, these steps are not simple and need thorough investigation and deliberations by each stakeholder.

Reference

- Aguocha, N. M. (2018). No title. *Stowaways: A Threat to Maritime Security and the Curse of Shipowners.*,
- Allen, C. H. (2018). Determining the legal status of unmanned maritime vehicles: formalism vs functionalism. *J.Mar.L. & Com.*, 49, 477.
- Allianz. (2021). Safety and Shipping. Review 2021.
- Amer, M., Daim, T. U., & Jetter, A. (2013). A review of scenario planning. *Futures*, 46, 23-40.
- Andrew, S., & Halcomb, E. J. (2012). Mixed methods research. *Navigating the Maze of Research: Enhancing Nursing and Midwifery Practice*, , 147-166.
- Andritsos, F. (2013). EU port security & growth. Paper presented at the *Proceedings of the 8th Future Security Research Conference*, 267-274.
- Attard, F. (2014). IMO's contribution to international law regulating maritime security. *J.Mar.L. & Com.*, 45, 479.
- 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)*,
- Bueger, C. (2015). What is maritime security? *Marine Policy*, 53, 159-164.
- Bueger, C., & Edmunds, T. (2017). Beyond seablindness: a new agenda for maritime security studies. *International Affairs*, 93(6), 1293-1311.
- Bueger, C., Edmunds, T., & McCabe, R. (2020). Into the sea: capacity-building innovations and the maritime security challenge. *Third World Quarterly*, 41(2), 228-246.
- Carey, L. (2017). All hands off deck? The legal barriers to autonomous ships.
- Chang, C., Kontovas, C., Yu, Q., & Yang, Z. (2021). Risk assessment of the operations of maritime autonomous surface ships. *Reliability Engineering & System Safety*, 207, 107324.
- Coito, J. (2021). Maritime Autonomous Surface Ships: New Possibilities—and Challenges—in Ocean Law and Policy. *International Law Studies*, 97(1), 19.
- 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.
- Dehart, J., 2013. Pirates of the Southeast Asian Seas. Neptune P2P Group. <https://thediplomat.com/2013/07/pirates-of-the-southeast-asian-seas/>.
- 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.
- Eriksson, A., & Gevriye, S. (2018). The biggest challenges with autonomous costal ferries.
- 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.
- Fink, M. (2018). *Maritime interception and the law of naval operations: A study of legal bases and legal regimes in maritime interception operations*. Springer.
- 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.
- Guerra, S. (2017). Ready about, Here Comes AI: Potential Maritime Law Challenges for Autonomous Shipping. *USF Mar.LJ*, 30, 69.
- Guilfoyle, D. (2017). Maritime Law Enforcement Operations and Intelligence in an Age of Maritime Security.
- Habdank, J. (2019). No title. *Exploring the Barriers and Opportunities of the Trend Towards Autonomous Shipping*,
- Halcomb, E. J., & Hickman, L. (2015). Mixed methods research.
- 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 2017*, 19, 211.
- Im, I., Shin, D., & Jeong, J. (2018). Components for smart autonomous ship architecture based on intelligent information technology. *Procedia Computer Science*, 134, 91-98.
- IMB. (2021). *Piracy and Armed Against Ships*. https://www.icc-ccs.org/reports/2020_Annual_Piracy_Report.pdf
- IMO. (2017). Maritime cyber risk. <https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx>
- IMO. (2018). *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. (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)*. (). MSC.1/Circ.1638
- Jiang, M., & Lu, J. (2020a). The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. *Transportation Research Part E: Logistics and Transportation Review*, 139, 101965.
- Jiang, M., & Lu, J. (2020b). The analysis of maritime piracy occurred in Southeast Asia by using Bayesian network. *Transportation Research Part E: Logistics and Transportation Review*, 139, 101965.
- Jin, M., Shi, W., Lin, K., & Li, K. X. (2019). Marine piracy prediction and prevention: Policy implications. *Marine Policy*, 108, 103528.
- Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, 33(7), 14-26.
- Jones, S. (2006). *Maritime security: a practical guide*. Nautical Institute.
- 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, M., Joung, T., Jeong, B., & Park, H. (2020a). Autonomous shipping and its impact on regulations, technologies, and industries. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 4(2), 17-25.
- Kim, M., Joung, T., Jeong, B., & Park, H. (2020b). Autonomous shipping and its impact on regulations, technologies, and industries. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, 4(2), 17-25.
- 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.
- Klein, N., Guilfoyle, D., Karim, M. S., & McLaughlin, R. (2020). Maritime autonomous vehicles: New frontiers in the law of the sea. *International & Comparative Law Quarterly*, 69(3), 719-734.
- Kobyliński, L. (2018). Smart ships—autonomous or remote controlled? *Zeszyty Naukowe Akademii Morskiej W Szczecinie*,
- 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)
- Kraska, J. (2010). Broken Taillight at Sea: The Peacetime International Law of Visit, Board, Search, and Seizure. *Ocean & Coastal LJ*, 16, 1.
- Kraska, J., & Pedrozo, R. (2013). *International maritime security law*. Martinus Nijhoff Publishers.

- 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. *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.
- Leuprecht, C., Aulhouse, A., & Walther, O. (2016). The puzzling resilience of transnational organized criminal networks. *Police Practice and Research*, 17(4), 376-387.
- Li, S., & Fung, K. S. (2019). Maritime autonomous surface ships (MASS): implementation and legal issues. *Maritime Business Review*,
- Liwång, H. (2016). Conditions for a risk-based naval ship survivability approach: a study on fire risk analysis. *Naval Engineers Journal*, 128(3), 87-101.
- Maritime Executive. (2020, October.). SBS Boarding Team Detains Stowaways After Confrontation Aboard Tanker. <https://www.maritime-executive.com/article/sbs-boarding-team-detains-stowaways-after-confrontation-aboard-tanker>
- Maritime Executive. (2021). *UK Warns of Potential Hijacking of Tanker Off Oman*. <https://maritime-executive.com/article/uk-warns-of-potential-hijacking-by-iran-of-tanker-off-oman>
- McLaughlin, R., & Klein, N. (2021). Maritime Autonomous Vehicles and Drug Trafficking by Sea: Some Legal Issues. *The International Journal of Marine and Coastal Law*, 36(3), 389-418.
- 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.
- Osinuga, D. (2020). Unmanned ships: Coping in the murky waters of traditional maritime law. *Poredbeno Pomorsko Pravo*, 59(174), 75-105.
- Petrig, A. (2020). The commission of maritime crimes with unmanned systems: an interpretive challenge for the United Nations Convention on the Law of the Sea. *Maritime Security and the Law of the Sea* (). Edward Elgar Publishing.
- Porathe, T., J. Prison, and Y. Man (2014). *Situation Awareness in Remote Control Centres for Unmanned Ships*. Paper presented at the Proceedings of Human Factors in Ship Design & Operation, 26-27 February 2014, London, UK.
- 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.

- Ramírez, B., & Bunker, R. J. (2015). Narco-submarines. Specially fabricated vessels used for drug smuggling purposes.
- 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*, 18
- Rødseth, Ø J., & Nordahl, H. (2017). No title. *Definition for Autonomous Merchant Ships. Version 1.0, October 10.2017. Norwegian Forum for Autonomous Ships*,
- 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. (2015). Risk assessment for an unmanned merchant ship. *TransNav: International Journal on Marine Navigation and Safety of Sea Transportation*, 9(3), 357-364.
- 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.
- Rylander, R., & Man, Y. (2016). Autonomous safety on vessels. *Lighthouse Swedish Maritime Competence Centre*,
- Saha, R. (2021). Mapping competence requirements for future shore control center operators. *Maritime Policy & Management*, , 1-13.
- 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.
- Schoonenboom, J., & Johnson, R. B. (2017). How to construct a mixed methods research design. *KZfSS Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, 69(2), 107-131.
- 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.
- 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. *Zeszyty Naukowe Akademii Morskiej W Szczecinie*,
- 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.
- Trump, B. D. (2020). Security and Resilience for a 4.0 Ship. *Cybersecurity and Resilience in the Arctic*, 58, 92.
- 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.*, https://unctad.org/system/files/official-document/rmt2018_en.pdf

- UNCTAD. (2020). Review of maritime transport.(Geneva: UNCTAD secretariat. Geneva-New York.)
https://unctad.org/system/files/official-document/rmt2020_en.pdf
- 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*,
- Wariishi, K. (2019). Maritime Autonomous Surface Ships: Development Trends and Prospects-how Digitalization Drives Changes in Maritime Industry. *Mitsui & Co.Global Strategic Studies Institute*,
- 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.
- 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.



WMU Research Ethics Committee Protocol

Name of principal researcher:	Aditya Pratap Singh
Name(s) of any co-researcher(s):	None
If applicable, for which degree is each researcher registered?	Maritime Safety and Environmental Administration
Name of supervisor, if any:	Professor Dr. Jens-Uwe Schröder-Hinrichs
Title of project:	"Autonomous Ships (MASS) uncharted era - A critical evaluation of maritime security perspective in the backdrop of current IMO regulations"
Is the research funded externally?	No
If so, by which agency?	No
Where will the research be carried out?	The research will be carried out in Sweden. The participants are from various countries including maritime professionals, Maritime administrations, Navy and Coast Guard officials and experts on the subject.
How will the participants be recruited?	The participants will be recruited by email on a voluntary basis.
How many participants will take part?	Interviews 10-12, Survey around 80-100 participants
Will they be paid?	No
If so, please supply details:	No
How will the research data be collected (by interview, by questionnaires, etc.)?	The research data will be collected by survey questionnaire and personal interviews using semi structured interview by zoom and document analysis.
How will the research data be stored?	The research data will be stored on my personal computer with protected passwords.
How and when will the research data be disposed of?	All the research data will be deleted from my PC by the end of my MSC degree (31 October 2021).
Is a risk assessment necessary? If so, please attach	No

Signature(s) of Researcher(s): ...Aditya Pratap Singh..... Date: 16 Aug 21

Signature of Supervisor: .. Dr. Jens-Uwe Schröder-Hinrichs... Date: 16 Aug 21

Please attach: -

- A copy of the research proposal
- A copy of any risk assessment - NA
- 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 - NA

Consent Form



Dear Participant,

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

The topic of the Dissertation is "Study on the implications of autonomous ships on maritime security and law enforcement by reviewing selected maritime security incidents"

The information provided by you in this interview or survey 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 the interview is highly appreciated.

Student's name Aditya Pratap Singh
Specialization Maritime Safety and Environmental Administration
Email address w2005522@wmu.se

* * *

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

Name:

Signature:

Date:

Interview Questions

Personnel information

Name of participant :

Company or institution :

Position :

Year of experience :

The questions to be asked to participants will be selected from the following list:

1. Do you think there are high possibilities of MASS being hijacked by pirates (physical or cyber) to ask for ransom for cargo/ launch attacks on vulnerable assets or port installations (collision with warships/grounding in navigable areas)?
2. Do you also consider any possibility of abuse of GNSS or AIS data onboard these ships?
3. Do you consider cyber security threats to be higher than physical pirate threats, and why?
4. What solutions, in your opinion, could prevent such possibilities of cyber and physical attacks?
5. Would you consider a higher probability of MASS being boarded at anchorage or in ports by armed robbers?
6. What solutions, in your opinion, could prevent such possibilities and have adequate security of vessels?
7. In your opinion, to what extent non-presence of the crew may render MASS a soft target for stowaways?
8. What types of challenges or barriers do you see to prevent stowaway ingress onboard MASS?
9. What solutions, in your opinion, could prevent such possibilities?
10. Do you think there are high possibilities of MASS being used by criminals for transnational organized crimes?
11. What challenges and barriers do you see to prevent such incidents or attacks?
12. What solutions, in your opinion, could prevent such possibilities?
13. Is there any possibility that the shore control centres may also be attacked (cyber pirates or physical attack) by criminals/non-state actors to fulfil their goals?
14. What solutions, in your opinion, could prevent such possibilities?

15. What measures do you consider for the security aspects of Shore Control Centers? Should these centres be covered under the security umbrella of IMO regulations?
16. Do you foresee any adverse impacts of MASS towards maritime security and law enforcement?
17. Do you feel any possible change in maritime interdiction/ boarding (VBSS) procedures involving MASS?
18. What do you think, would be the biggest challenge to deal with such ships (autonomous and unmanned) involved in any illicit crime (terrorism/ trafficking/ stowaway/ illegal immigrants)?
19. Do you anticipate any possible changes in security agencies methods/procedures while dealing with such ships?
20. What security initiatives should be considered from the planning stage (design phase) of MASS?

Survey Questionnaire

Dear participants

In this survey, I want to assess how the introduction of autonomous (crewless) or Maritime Autonomous Surface Ships (MASS - Degrees of automation 3 & 4) in the maritime transport industry would affect maritime security and law enforcement. This is part of my Master's dissertation at the World Maritime University (WMU).

This questionnaire includes two sections, in which, the participant is invited to answer a range of questions, as per the scale indicated. 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 optimise the quality of the survey, genuine and unbiased choices are requested from the participant. It will take about 10 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

1. Gender

Male/Female/ Preferred not say

2. Age

Under 25 years / 25-35 years/ 36-45 years / 46-55 years / Over 55 years

3. Job

Maritime Administration/ Maritime Academician / Maritime Expert / Seafarer /Navy / Coast Guard

4. Position

Top manager/ middle manager/ Senior officer/ Junior officer/ Master/ Chief officer/ Second officer/
Professor / Associate professor/ Assistant professor / others

5. Years of Experience

Less than 5 years/ 5-10 years/ 11-15 years/ 16-20 years / Over 20 years

6. Nationality

Section – II

7. How familiar are you with the concept of Maritime Autonomous Surface Ship (MASS)

Not at all familiar/ Not so familiar / Somewhat familiar / Very familiar / Extremely familiar

8. How familiar are you with Maritime Security and its importance in maritime transport industry

Not at all familiar/ Not so familiar / Somewhat familiar / Very familiar / Extremely familiar

9. How familiar are you with the concept of law enforcement at sea

Not at all familiar/ Not so familiar / Somewhat familiar / Very familiar / Extremely familiar

10. Despite the absence of the crew, traditional piracy attacks will affect MASS.

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

11. MASS activities may be more vulnerable to cyber-attacks, including cyber piracy

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

12. A deliberate denial of the Global Navigation Satellite System (GNSS) service or the use of misleading signals to deceive the GNSS receiver may be fatal for MASS

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

13. There are chances that non-state actors will employ MASS as a weapon to attack sensitive targets (warships, port or coastline installations etc.)

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

14. Autonomous (crewless) ships, in comparison to conventional ships, would become a preferred choice for criminals to undertake transnational organised crimes (arms/drugs/human trafficking etc)

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

15. The absence of crew may encourage criminals to undertake armed robbery/petty theft onboard MASS

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

16. There is a significant probability that stowaway will target MASS more than regular ships

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

17. There is a higher possibility that crewless autonomous ships may also pose a threat to the security of other conventional ships

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

18. The absence of crew onboard MASS may weaken the ship's security under the ISPS code

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

19. Deputation of security crew onboard MASS will be essential to provide equivalent level of security in ports

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

20. Deputation of security crew will be essential to provide equivalent level of security at anchorage to avoid armed robberies/petty thefts

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

21. Ports that would handle MASS may have to re-evaluate their port security assessment under ISPS code

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

22. MASS security clearance including nil stowaway must be made compulsory prior leaving a port

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

23. Communication and networking infrastructure of MASS shore control centres may also be vulnerable to cyber threats

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

24. Non-state actors may also attack shore control centres for using MASS as a weapon against sensitive targets

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

25. The implementation of MASS may present new challenges for maritime law enforcement organisations (such as Coast Guard and Navy)

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

26. The adoption of MASS in shipping will significantly influence law enforcement agencies use of Visit Board Search and Seizure (VBSS)

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

27. Document verification/inspection at sea onboard MASS during VBSS would require alternate arrangements

Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

28. The search operation onboard MASS (without crew) as part of VBSS will cause a challenge for law enforcement agencies

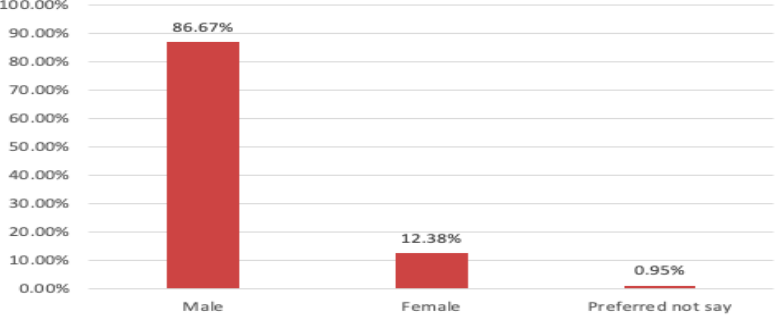
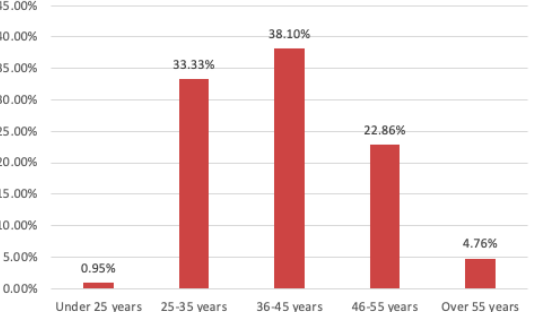
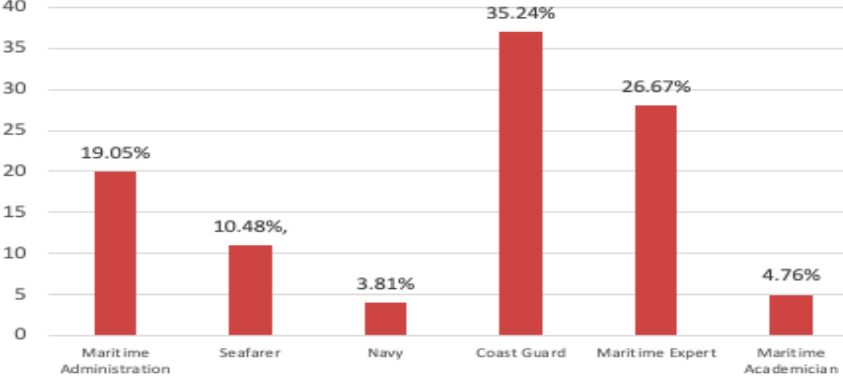
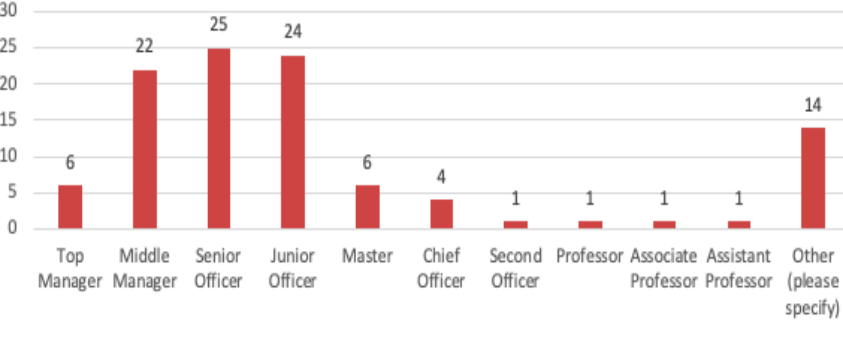
Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

29. Enhancement of maritime security in MASS era is unavoidable

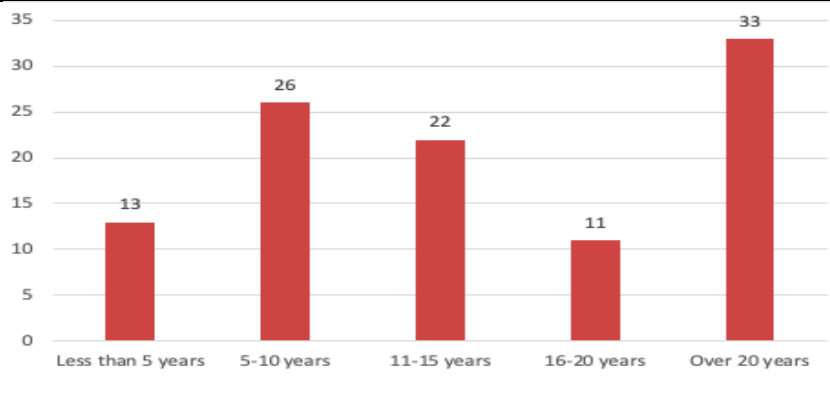
Strongly disagree/ Disagree/ Neutral /Agree /Strongly agree / Don't know

Survey Questionnaire Result

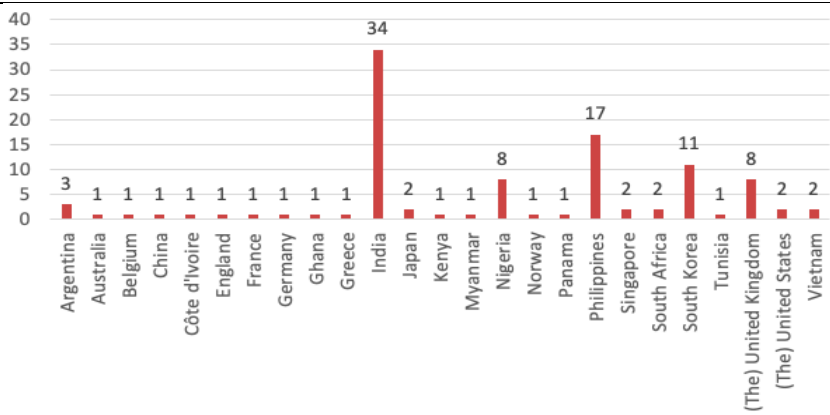
Section – I and II

<p>1. Gender</p>	 <table border="1"> <thead> <tr> <th>Gender</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Male</td> <td>86.67%</td> </tr> <tr> <td>Female</td> <td>12.38%</td> </tr> <tr> <td>Preferred not say</td> <td>0.95%</td> </tr> </tbody> </table>	Gender	Percentage	Male	86.67%	Female	12.38%	Preferred not say	0.95%																
Gender	Percentage																								
Male	86.67%																								
Female	12.38%																								
Preferred not say	0.95%																								
<p>2. Age</p>	 <table border="1"> <thead> <tr> <th>Age Group</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Under 25 years</td> <td>0.95%</td> </tr> <tr> <td>25-35 years</td> <td>33.33%</td> </tr> <tr> <td>36-45 years</td> <td>38.10%</td> </tr> <tr> <td>46-55 years</td> <td>22.86%</td> </tr> <tr> <td>Over 55 years</td> <td>4.76%</td> </tr> </tbody> </table>	Age Group	Percentage	Under 25 years	0.95%	25-35 years	33.33%	36-45 years	38.10%	46-55 years	22.86%	Over 55 years	4.76%												
Age Group	Percentage																								
Under 25 years	0.95%																								
25-35 years	33.33%																								
36-45 years	38.10%																								
46-55 years	22.86%																								
Over 55 years	4.76%																								
<p>3. Job</p>	 <table border="1"> <thead> <tr> <th>Job</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Maritime Administration</td> <td>19.05%</td> </tr> <tr> <td>Seafarer</td> <td>10.48%</td> </tr> <tr> <td>Navy</td> <td>3.81%</td> </tr> <tr> <td>Coast Guard</td> <td>35.24%</td> </tr> <tr> <td>Maritime Expert</td> <td>26.67%</td> </tr> <tr> <td>Maritime Academician</td> <td>4.76%</td> </tr> </tbody> </table>	Job	Percentage	Maritime Administration	19.05%	Seafarer	10.48%	Navy	3.81%	Coast Guard	35.24%	Maritime Expert	26.67%	Maritime Academician	4.76%										
Job	Percentage																								
Maritime Administration	19.05%																								
Seafarer	10.48%																								
Navy	3.81%																								
Coast Guard	35.24%																								
Maritime Expert	26.67%																								
Maritime Academician	4.76%																								
<p>4. Position</p>	 <table border="1"> <thead> <tr> <th>Position</th> <th>Count</th> </tr> </thead> <tbody> <tr> <td>Top Manager</td> <td>6</td> </tr> <tr> <td>Middle Manager</td> <td>22</td> </tr> <tr> <td>Senior Officer</td> <td>25</td> </tr> <tr> <td>Junior Officer</td> <td>24</td> </tr> <tr> <td>Master</td> <td>6</td> </tr> <tr> <td>Chief Officer</td> <td>4</td> </tr> <tr> <td>Second Officer</td> <td>1</td> </tr> <tr> <td>Professor</td> <td>1</td> </tr> <tr> <td>Associate Professor</td> <td>1</td> </tr> <tr> <td>Assistant Professor</td> <td>1</td> </tr> <tr> <td>Other (please specify)</td> <td>14</td> </tr> </tbody> </table>	Position	Count	Top Manager	6	Middle Manager	22	Senior Officer	25	Junior Officer	24	Master	6	Chief Officer	4	Second Officer	1	Professor	1	Associate Professor	1	Assistant Professor	1	Other (please specify)	14
Position	Count																								
Top Manager	6																								
Middle Manager	22																								
Senior Officer	25																								
Junior Officer	24																								
Master	6																								
Chief Officer	4																								
Second Officer	1																								
Professor	1																								
Associate Professor	1																								
Assistant Professor	1																								
Other (please specify)	14																								

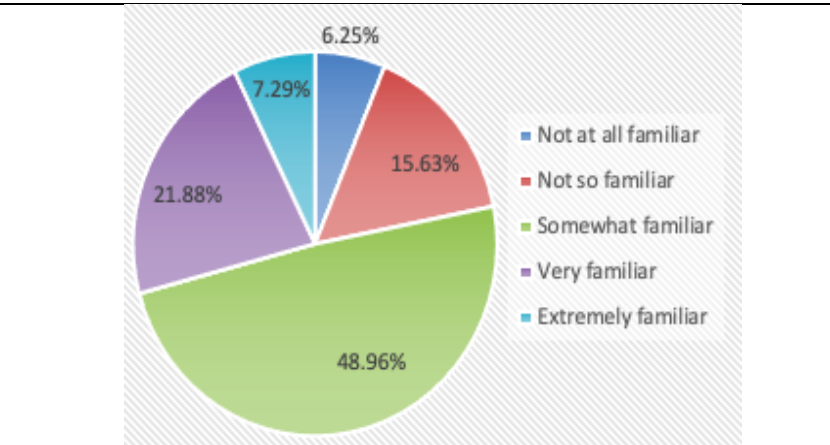
5. Years of Experience



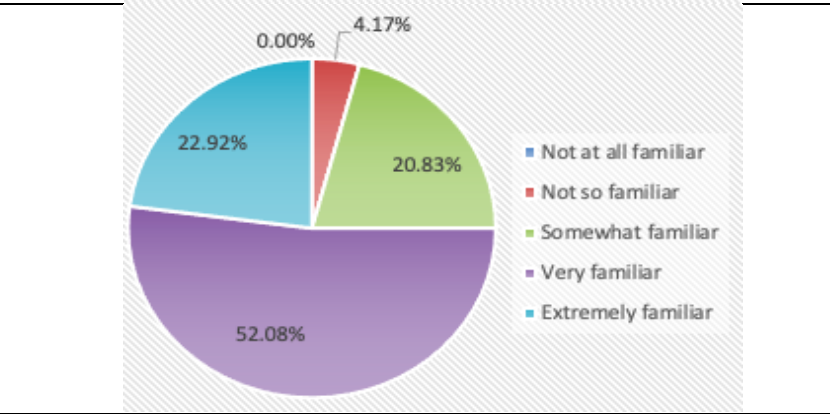
6. Nationality



7. How familiar are you with the concept of Maritime Autonomous Surface Ship (MASS)



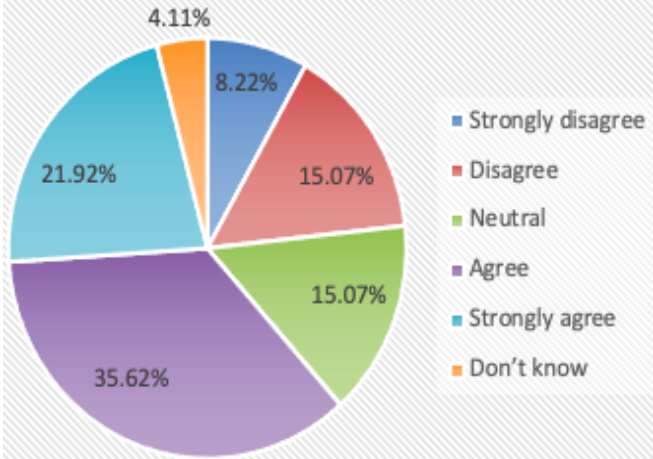
8. How familiar are you with Maritime Security and its importance in maritime transport industry



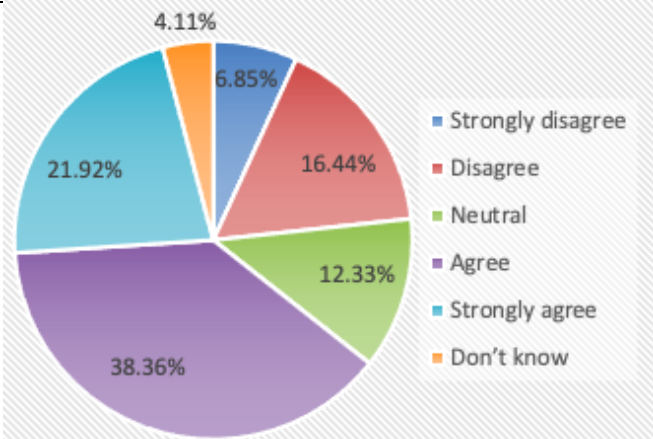
<p>9. How familiar are you with the concept of law enforcement at sea</p>	<table border="1"> <thead> <tr> <th>Familiarity Level</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Not at all familiar</td> <td>1.04%</td> </tr> <tr> <td>Not so familiar</td> <td>2.08%</td> </tr> <tr> <td>Somewhat familiar</td> <td>19.79%</td> </tr> <tr> <td>Very familiar</td> <td>51.04%</td> </tr> <tr> <td>Extremely familiar</td> <td>26.04%</td> </tr> </tbody> </table>	Familiarity Level	Percentage	Not at all familiar	1.04%	Not so familiar	2.08%	Somewhat familiar	19.79%	Very familiar	51.04%	Extremely familiar	26.04%		
Familiarity Level	Percentage														
Not at all familiar	1.04%														
Not so familiar	2.08%														
Somewhat familiar	19.79%														
Very familiar	51.04%														
Extremely familiar	26.04%														
<p>10. Despite the absence of the crew, traditional piracy attacks will affect MASS.</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Strongly disagree</td> <td>0.00%</td> </tr> <tr> <td>Disagree</td> <td>6.85%</td> </tr> <tr> <td>Neutral</td> <td>6.85%</td> </tr> <tr> <td>Agree</td> <td>53.42%</td> </tr> <tr> <td>Strongly agree</td> <td>26.03%</td> </tr> <tr> <td>Don't know</td> <td>0.00%</td> </tr> </tbody> </table>	Response	Percentage	Strongly disagree	0.00%	Disagree	6.85%	Neutral	6.85%	Agree	53.42%	Strongly agree	26.03%	Don't know	0.00%
Response	Percentage														
Strongly disagree	0.00%														
Disagree	6.85%														
Neutral	6.85%														
Agree	53.42%														
Strongly agree	26.03%														
Don't know	0.00%														
<p>11. MASS activities may be more vulnerable to cyber-attacks, including cyber piracy</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Strongly disagree</td> <td>0.00%</td> </tr> <tr> <td>Disagree</td> <td>1.37%</td> </tr> <tr> <td>Neutral</td> <td>5.48%</td> </tr> <tr> <td>Agree</td> <td>36.99%</td> </tr> <tr> <td>Strongly agree</td> <td>50.68%</td> </tr> <tr> <td>Don't know</td> <td>5.48%</td> </tr> </tbody> </table>	Response	Percentage	Strongly disagree	0.00%	Disagree	1.37%	Neutral	5.48%	Agree	36.99%	Strongly agree	50.68%	Don't know	5.48%
Response	Percentage														
Strongly disagree	0.00%														
Disagree	1.37%														
Neutral	5.48%														
Agree	36.99%														
Strongly agree	50.68%														
Don't know	5.48%														

<p>12. A deliberate denial of the Global Navigation Satellite System (GNSS) service or the use of misleading signals to deceive the GNSS receiver may be fatal for MASS</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Strongly disagree</td> <td>6.85%</td> </tr> <tr> <td>Disagree</td> <td>4.11%</td> </tr> <tr> <td>Neutral</td> <td>5.48%</td> </tr> <tr> <td>Agree</td> <td>43.84%</td> </tr> <tr> <td>Strongly agree</td> <td>36.99%</td> </tr> <tr> <td>Don't know</td> <td>2.74%</td> </tr> </tbody> </table>	Response	Percentage	Strongly disagree	6.85%	Disagree	4.11%	Neutral	5.48%	Agree	43.84%	Strongly agree	36.99%	Don't know	2.74%
Response	Percentage														
Strongly disagree	6.85%														
Disagree	4.11%														
Neutral	5.48%														
Agree	43.84%														
Strongly agree	36.99%														
Don't know	2.74%														
<p>13. There are chances that non-state actors will employ MASS as a weapon to attack sensitive targets (warships, port or coastline installations etc.)</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Strongly disagree</td> <td>6.85%</td> </tr> <tr> <td>Disagree</td> <td>2.74%</td> </tr> <tr> <td>Neutral</td> <td>6.85%</td> </tr> <tr> <td>Agree</td> <td>54.79%</td> </tr> <tr> <td>Strongly agree</td> <td>26.03%</td> </tr> <tr> <td>Don't know</td> <td>2.74%</td> </tr> </tbody> </table>	Response	Percentage	Strongly disagree	6.85%	Disagree	2.74%	Neutral	6.85%	Agree	54.79%	Strongly agree	26.03%	Don't know	2.74%
Response	Percentage														
Strongly disagree	6.85%														
Disagree	2.74%														
Neutral	6.85%														
Agree	54.79%														
Strongly agree	26.03%														
Don't know	2.74%														
<p>14. Autonomous (crewless) ships, in comparison to conventional ships, would become a preferred choice for criminals to undertake transnational organised crimes (arms/drugs/human trafficking etc)</p>	<table border="1"> <thead> <tr> <th>Response</th> <th>Percentage</th> </tr> </thead> <tbody> <tr> <td>Strongly disagree</td> <td>8.22%</td> </tr> <tr> <td>Disagree</td> <td>8.22%</td> </tr> <tr> <td>Neutral</td> <td>15.07%</td> </tr> <tr> <td>Agree</td> <td>42.47%</td> </tr> <tr> <td>Strongly agree</td> <td>24.66%</td> </tr> <tr> <td>Don't know</td> <td>1.37%</td> </tr> </tbody> </table>	Response	Percentage	Strongly disagree	8.22%	Disagree	8.22%	Neutral	15.07%	Agree	42.47%	Strongly agree	24.66%	Don't know	1.37%
Response	Percentage														
Strongly disagree	8.22%														
Disagree	8.22%														
Neutral	15.07%														
Agree	42.47%														
Strongly agree	24.66%														
Don't know	1.37%														

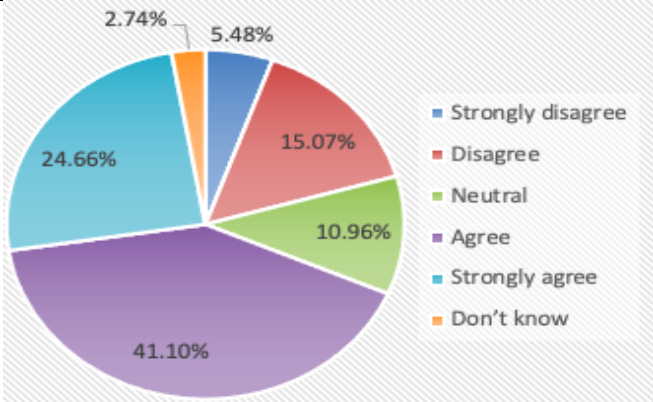
15. The absence of crew may encourage criminals to undertake armed robbery/petty theft onboard MASS



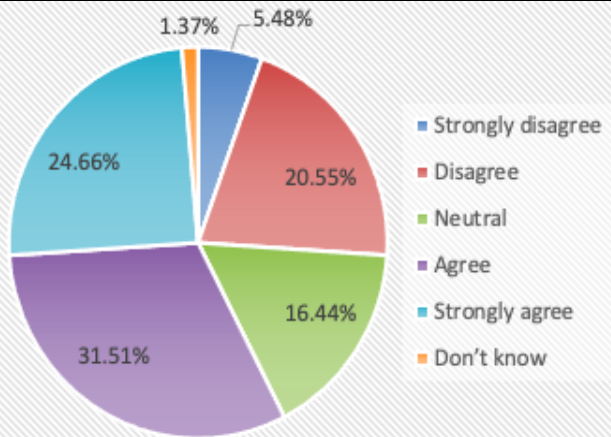
16. There is a significant probability that stowaway will target MASS more than regular ships



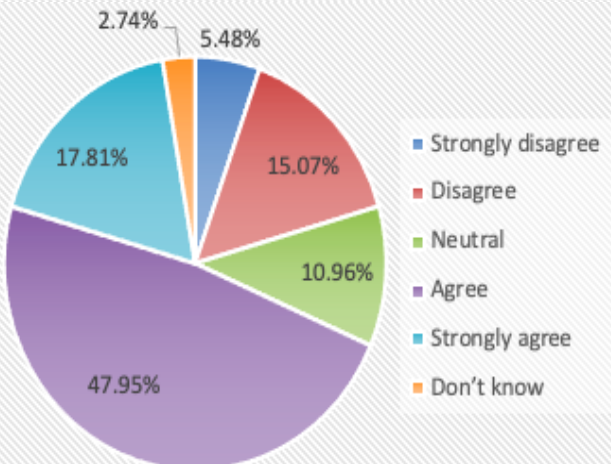
17. There is a higher possibility that crewless autonomous ships may also pose a threat to the security of other conventional ships



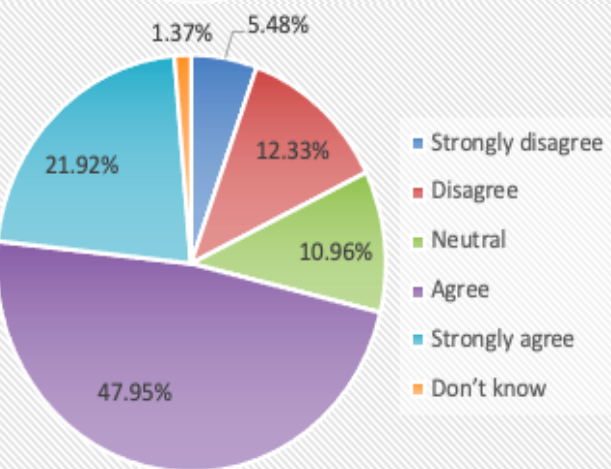
18. The absence of crew onboard MASS may weaken the ship's security under the ISPS code



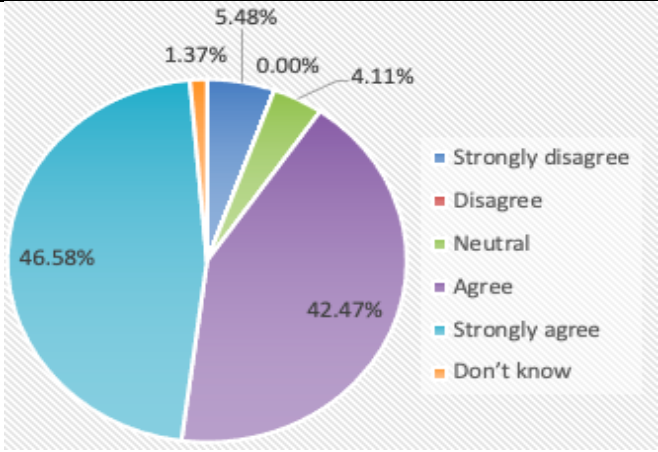
19. Deputation of security crew onboard MASS will be essential to provide equivalent level of security in ports



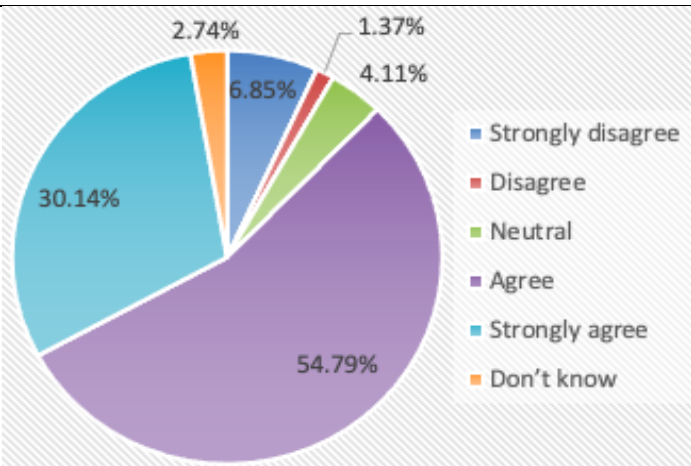
20. Deputation of security crew will be essential to provide equivalent level of security at anchorage to avoid armed robberies/petty thefts



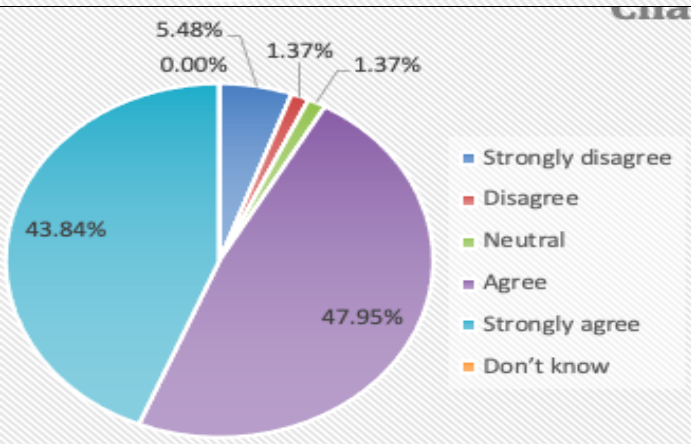
21. Ports that would handle MASS may have to re-evaluate their port security assessment under ISPS code



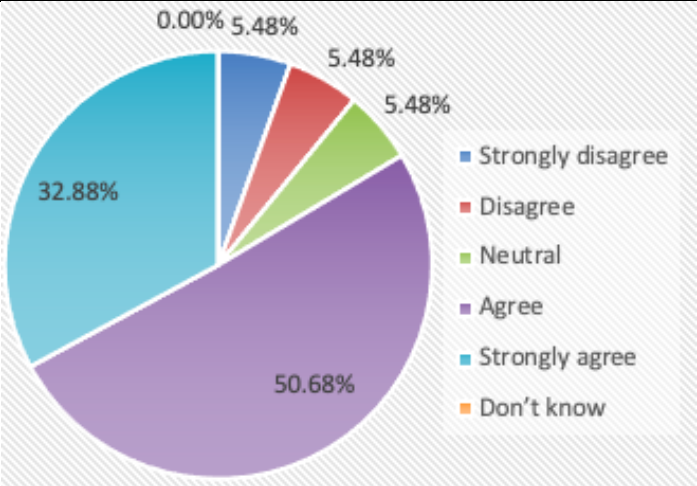
22. MASS security clearance including nil stowaway must be made compulsory prior leaving a port



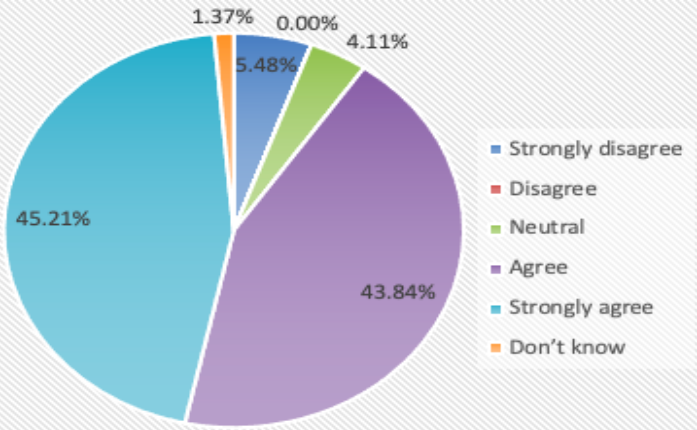
23. Communication and networking infrastructure of MASS shore control centres may also be vulnerable to cyber threats



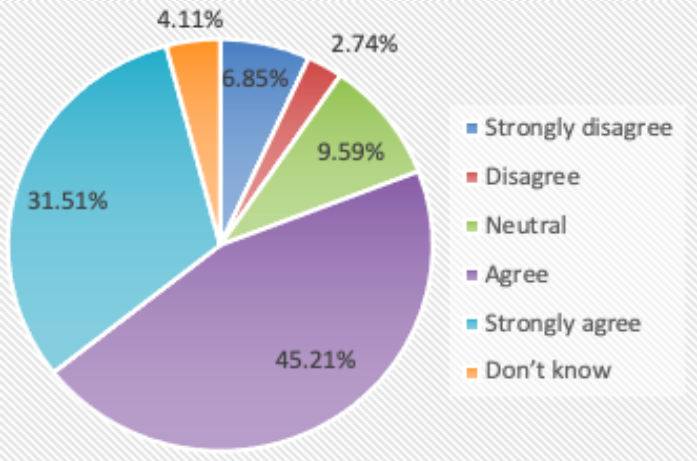
24. Non-state actors may also attack shore control centres for using MASS as a weapon against sensitive targets



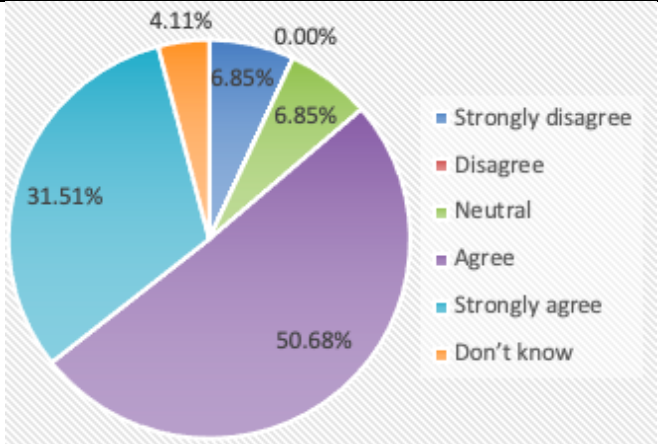
25. The implementation of MASS may present new challenges for maritime law enforcement organisations (such as Coast Guard and Navy)



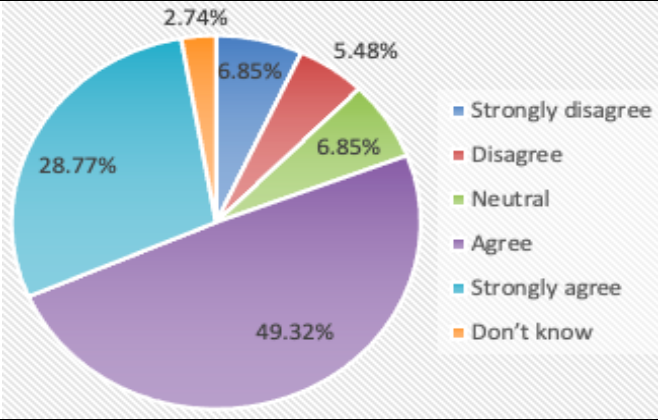
26. The adoption of MASS in shipping will significantly influence law enforcement agencies use of Visit Board Search and Seizure (VBSS)



27. Document verification/inspection at sea onboard MASS during VBSS would require alternate arrangements



28. The search operation onboard MASS (without crew) as part of VBSS will cause a challenge for law enforcement agencies



29. Enhancement of maritime security in MASS era is unavoidable

