2008

The role of technology in maritime security : a survey of its development, application, and adequacy

Bhim S. Kothari
World Maritime University

WORLD MARITIME UNIVERSITY

Malmö, Sweden

THE ROLE OF TECHNOLOGY IN MARITIME SECURITY: A SURVEY OF ITS DEVELOPMENT, APPLICATION, AND ADEQUACY

By

BHIM SINGH KOTHARI

India

A dissertation submitted to the World Maritime University in partial Fulfilment of the requirement for the award of the degree of

MASTER OF SCIENCE

In

MARITIME AFFAIRS

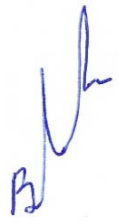
(MARITIME SAFETY AND ENVIRONMENTAL ADMINISTRATION)

2008

DECLARATION

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

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



Signature: …...……..

Date: 25 August 2008

Supervised by:
Dr. Takeshi Nakazawa
Professor
World Maritime University

Assessor:
Dr. Maximo Q. Mejia Jr.
Assistant Professor
World Maritime University

Co-assessor:
Capt. Kjell Grahn
Maritime Consultant
Malmö, Sweden

ACKNOWLEDGEMENTS

At the outset, I would like to thank my country, India and my organization, the Indian Coast Guard for nominating me to this course. My sincere gratitude to Dr. Yohei Sasakawa for endorsing the Sasakawa fellowship without which this study would have not been possible.

I am also thankful to Commodore RS Vasan, NM (Retd), Inspector General SPS Basra, YSM, PTM, TM Deputy Inspector General TS Balasubramanian, TM (Retd) and Deputy Inspector General KR Nautiyal, TM for their professional guidance and advice.

My sincere thanks to Professor Dr. Takeshi Nakazawa, for his academic pursuits, knowledge, supervision, valuable advice and guiding me through the coarsely path of research and successful accomplishment of my work.

Many thanks to Professors Dr. P. K. Mukherjee, Jan-Åke Jönsson, Dr. Maximo Q. Mejia Jr, Dr. Jens-Uwe Schröder and Neil Bellefontaine for inspiring through their dedicated teaching and motivating me to accept the challenge of writing the dissertation. I am also thankful to Professors Sven-Åke Wernhult, Jan Hork, Rajendra Prasad and John Liljedahl for assisting me in collection of survey data during the dissertation.

Thanks to Eric Ponnet, IT Program Officer, for designing the dissertation portal and uploading my questionnaire making the herculean task of compilation of survey data very simple and easy. My hearty thanks to Assistant Professor Inger Battista for enriching the dissertation linguistically.

Special thanks to Captain Inderveer Solanki, Vice President Applied Research International, Captain, Sarabjit Singh Butalia and Commandant Anish Hebber, TM for their immortal support during the writing of the dissertation.

I am thankful to Richard Dennis, head of information services and the library staff Cecilia Denne, senior library assistant, for supporting me in the collection of books and materials for the research work and Christian Wallentin, Network Administrator for retrieving the lost dissertation data.

I am also thankful to my friends and colleagues at World Maritime University who stood by me in the need of the hour, especially, Ji Hoon Suk, Zhiping Ren(Sofie), Arizal Hendriawan, Mohammad Mahbub Morshed Chowdhury, Sandra Samy George Haddad, Karayil Paleri Jayakumar, Cagdas Gurbuz, Azlena Maria Binti Abu Baker, Mohamed Ahmed Mahmoud Essallamy, Young Chan Lee, Xiaohu Chen (Tiger), Ahmad Faizal Ahmad Fuad, Mohd Rosli Bin Abdullah, Yusuf Mohammad Bala and PhD students Abhinayan Basu, Michael Manuel.

I am grateful to the shipping companies, institutions, individuals who promptly replied to my emails, facilitating me with data and their comments on various issues related to my dissertation. Special thanks to all of those for having spared their valuable time for filling out the dissertation questionnaire.

Finally, my profound gratitude to my parents and relatives for their support and to my wife Banita and children Asmita and Ashwin for bearing my absence, encouraging me from time to time and nourishing me with their unbounded love.

"LIFE ON THE PLANET BEGAN IN THE OCEAN. THE OCEAN SUSTAINS IT. UNDOUBTEDLY PERILS OF THE OCEAN WILL HAVE AN EFFECT ON LIVES ON EARTH."

Prabhakaran Paleri, PTM, TM
Director General, Indian Coast Guard (Retd)
In Role of Coast Guard in the Maritime Security of India

ABSTRACT

Title of Dissertation: **The Role of Technology in Maritime Security: A Survey of Its Development, Application, and Adequacy**

Degree: **Master of Science**

Maritime transportation is the most economical mode for mobilizing raw and finished products in bulk. While the dynamics of economics were changing with 'globalization' and countries were opening their closed door policy, the shipping industry stood and supported the changes by rendering the best services to the world. Today, the industry is being threatened of being used by discriminators to fulfil their malicious desire.

To thwart the malice and bring the perpetrators to justice, IMO has adopted instruments in the maritime realm to malign such acts. These instruments fruition, when incidents imperilling maritime security are identified before their impact. The dissertation carries out the retrospection of the legal instruments and does an introspection of the industry and finds that the industry is vulnerable to the maritime crime of which piracy and armed robbery against ships and maritime terrorism poses maximum threats that can maim maritime security.

Technology, in different walks of life has revolutionized and made a herculean task within the human capability. It has also been adopted in the industry to enhance safety and security. Despite quantum leaps in advances to ship and maritime security technology, the threat to life and property remains very real. Effective and optimal utilization of these technologies can facilitate in fostering maritime security manifold. The dissertation critically analyzes these technologies and evaluates possible solutions for optimization. It also makes recommendation for future consideration that may scale a higher degree of maritime security.

KEYWORDS: Maritime Security, ISPS Code, Technology, SOLAS, Piracy and Armed Robbery, UNCLOS, Terrorism, and SUA.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

AIS	-	Automatic Information Systems
ARPA	-	Automatic Radar Plotting Aid
CBP	-	U.S. Customs and Border Protection
CSO	-	Company Security Officer
CSR	-	Continuous Synopsis Record
CTC	-	Counter-Terrorism Committee
CTED	-	Counter-Terrorism Committee Executive Directorate
C-TPAT	-	Customs-Trade Partnership against Terrorism
DSC	-	Digital Selective Calling
ECDIS	-	Electronic Chart Display and Information System
ECS	-	Electronic Chart System
EEZ	-	Exclusive Economic Zones
GISIS	-	Global Integrated Shipping Information System
GMDSS	-	Global Maritime Distress and Safety System
ICAO	-	International Civil Aviation Organisation
ICSO	-	International Container Standards Organization
ILO	-	International Labour Organization
IMB	-	International Maritime Bureau
IMO	-	International Maritime Organisation
ISO	-	International Organization for Standardization
ISPS Code	-	International Ship and Port Facility Security Code
LRIT	-	Long-range identification and tracking
MarNIS	-	Maritime Navigation and Information Services
MoU	-	Memorandum of Understanding
MSC	-	Maritime Safety Committee
PFSA	-	Port Facility Security Assessment
PFSO	-	Port Facility Security Officer
PFSP	-	Port Facilities Security Plan

ReCAAP	-	Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia
RSO	-	Recognized Security Organization
SID	-	Seafarers' Identity Documents
SOLAS 1974	-	International Convention for the Safety of Life at Sea 1974
SSO	-	Ship Security Plan
SUA 1988	-	The Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988
TWIC	-	Transportation Worker Identification Credential
UN	-	United Nations
UNCLOS 1982	-	United Nations Convention on the law of the Sea, 1982
VTMS	-	Vessel Traffic Management System
VTS	-	Vessel Traffic Services
WCO	-	World Customs Organization
STCW	-	Standards of Training, Certification and Watchkeeping for Seafarers

CHAPTER 1

INTRODUCTION

Shipping has been the most economical means of transportation since antiquity and today it is also one of the biggest means of transportation (Mitsatsos, 2005; Mortensen & Rasmussen, 2003). In a true sense shipping is the only international industry that has made globalization possible (Boutilier, 2005; Insall, 2003). Statistics indicates that 90% of the world trade (United Nations Conference on Trade and Development, 2008, p. 14) is carried by 50,525[1] ships registered in about 150 countries, manned by 466,000 officers and 721,000 ratings[2] (Chamberlain, 2008).

Human quests for achieving greater efficiencies have made the shipping industry sophisticated, and ships more efficient and hi-tech. The maritime industry has been growing at a fast pace ("Shipping and World Trade : Key facts") and this boom is expected to continue due to globalization, increased economic liberalization and strong, sustainable growth in Indian, Chinese and other developing countries' economy (Chellaram, 2004; DeSimone, 2008, March). UNCTAD[3] reported a growth of 8.5% at the beginning of 2007 and a corresponding expansion of the merchant fleet to 1.04 billion dead weight tonnage (UNCTAD, 2007). Today the shipping industry has assumed an international character not only because it carries every kind of cargo, but also since the crew that man the ships belong to virtually from every nationality (Sklet, 2006).

If the industry has been growing, so have the perils at sea. Development has been accompanied by two major pathogenic, namely piracy and armed robbery, and maritime terrorism. As shipping grew and became more sophisticated year after year,

---

[1] As on 1st January 2008 source: http://www.marisec.org/shippingfacts/worldtrade/number-of-ships.php, retrieved on July 31 2008.
[2] Source: http://www.marisec.org/shippingfacts/worldtrade/world-seafarers.php, retrieved on July 31 2008.
[3] United Nation Conference on Trade and Development.

these pathogenic also became stronger and more complicated. The maritime industry faces varying levels of threats from different maritime crimes such as piracy, armed robbery, high jacking, stowaways, illegal migrants, narcotics, arms smuggling, fraud and others (Kanev, 2005). The scope of the dissertation has been limited to Piracy and Armed Robbery against Ships, and Maritime Terrorism. The International Maritime Organization was formed to facilitate technical assistance for safety and protecting the maritime environment through its instruments. However, during the 1980s and 1990s, maritime security started to be included in its day to day working (Hesse, 2003). The growing *impendeo* from piracy and armed robbery and terrorism paved the path for new initiatives at IMO, such as establishing an anti piracy program, development of guidelines for the ship security, adoption of the convention for the Suppression of Unlawful acts against the Safety of Maritime Navigation (SUA Convention), 1988 and the International Ship and Port Facility Security Code (ISPS Code).

Being at the helm of maritime affairs, the IMO has actively responded to historic disasters involving safety of life and the marine environment. Adoption of new measures and regular updating of International Convention for the Safety of Life at Sea (SOLAS 74), and International Convention for the Prevention of Pollution from Ships, (MARPOL 73/78) depicts the volume of its initiatives taken in this direction. In the field of maritime security too some progress was made in the 1980's through the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, 1988 (SUA 88).

However, the incidents of 9/11 changed the crime phraseology in all the sectors and the maritime industry could not stay in isolation. The incident sent shock waves all around the world and for a moment it seemed that the time had paused; security agencies did not know how to react to the incident. An unimaginable deed of using a mode of transportation as a weapon of mass destruction became reality. It synergized the regulatory think tanks to scratch their gray matter to view security in a broader

perspective (Kanev, 2005; Richardson, 2007; White, 2003, March 25-26). All agencies evaluated threat perceptions from different angles, giving a relook at the regulatory regime and its effectiveness, and making good the gaps by incorporating technology, both at international and national levels. IMO also reacted in a proactive manner for ensuring secure shipping; converging the port facilities and shipping under its maritime security umbrella by amending Chapter XI of SOLAS and adopting the ISPS code.

Comparing the two means of transportation, while the aviation sector has been at the forefront of induction of new technological innovations, the shipping industry though equally vulnerable to threats, had been turning a blind eye toward it. Shipping's *modus operandi* and growing pace makes it a very soft target and facilitating a secure environment will be a great challenge for the world community (Amirell, 2006).

IMO's continual efforts have made the shipping industry one of the most regulated in the world (Mortensen & Rasmussen, 2003). There are nearly 50 IMO instruments, reinforced by a number of protocols, codes, guidelines, recommended practices and a plethora of circulars, covering different aspects of the maritime industry, namely ship operation, ship design, construction, equipment, maintenance, manning and eventual disposal, literally, from the drawing board to the scrap yard (International Maritime Organization). Maritime security has been an important agenda of IMO meetings, and the incident of 9/11 propelled it to the top. Taking a proactive approach, the former IMO Secretary General, O´Neil immediately submitted to the IMO Assembly, through the council, a draft resolution calling for an urgent review to determine whether there was a need for IMO to take any action to deal with acts of terrorism; and, in the light of the review, to pursue the measures deemed necessary in the circumstances. The review confirmed that shipping was indeed exposed and therefore an intervention by IMO was imperative (International Maritime Organisation, 2002, December 9). The importance of maritime security took deeper roots in the maritime industry when IMO adopted the new motto 'Safe, Secure and

Efficient Shipping on Clean Oceans' in the 89th session of the IMO council meeting (International Maritime Organization, 2002, December 5).

In every commercial sector when security is discussed the first thing that comes to mind is that it is an irretrievable and unproductive investment. But practically, security brings value addition to a commercial entity in many ways. It is important to adopt security management as an integral part of organizational activities and not as a separate entity (Gill, Burns-Howell, Keats, & Taylor, 2007, p. 6). Gill et al., quotes James (1993) saying "security is nothing more than a drain on company resources has got to change …A security Department can have a substantial impact on overall company profitability in a number of ways. Determining this profitability can be very difficult…"(Gill et al., 2007, p. 21).

Shipping too being a commercial entity has seen a conflict between regulatory and commercial interests. The biggest challenge facing the IMO in its endeavour to enhance maritime security is the commercial interest of the industry. A majority in the industry still feel that enhancing security will hamper their growth. It will be difficult to carry out cost-benefit analyses for each and every security measure that the industry implements. One way would be to see the repercussions of not having it (Gill et al., 2007, p. 19). To quote an example on the cost of impact, taken from the incident of M/V *Limburg* in 2002, there were only three deaths, which included the two bombers. However, the incident brought international shipping business in the Gulf to a standstill. The consequence was a 48 cent hike per barrel in the price of Brent crude oil, tripling of war risks premiums, 93-percent drop in container terminal resulting in an approximate loss of $3.8 million a month loss in port revenues to the Yemeni economy (Chalk, 2008b; Herbert-Burns, 2005).

From the above incident, it is clear that a breach in maritime security may not only affect the individual owner but will also affect the global economy and may have grave impact on humanity.

Peleg-Gillai, Bhat & Sept (2006) carried out a study on "Innovators in Supply Chain Security: Better Security Drives Business Value,". Their study reveals that investments in supply chain security lowers risk and raises cargo security and provides significant business value for organizations. It will help them in improving internal operations and strengthening relationship with their customers, which will result in higher profitability. Therefore, it urges shipping companies not to consider security investments as a financial burden; rather they are investments for business justification. It will bring operational improvements, promote cost reduction and culminating in higher revenue and growth.

Intelligence analysts, law enforcement officials, and policymakers have expressed concerns over the likelihood of increased terrorist attacks in future on the maritime industry (Glass, 2003, December 18), since the maritime environment possesses unique characteristics such as extraterritoriality of the high seas and poor or inconsistent security measures that apply in coastal areas and port facilities in many parts of the world. These make the industry vulnerable and attractive to terrorist operations (Richardson, 2004).

In order to boost the liberalization, growth in global trade and meet the energy demands of growing economies and expanding populations (Council, 2007), it is important to secure shipping which is the life line of the world economy. The only way out is by effective utilization of technology and achieving higher degree of maritime security (Abhyankar, 2006).

The dissertation is a sincere approach to contribute to the knowledge of maritime security by evaluating the role that technology can play in fostering maritime security. The approach adopted in this dissertation is qualitative. To facilitate the views of the maritime industry on various issues of maritime security, three sets of Questionnaires (Appendix A) were prepared for,

(a) Maritime Administration (MA) officials who are responsible for overall administration and legal aspects of the maritime sector within a Flag Administration.

(b) The people responsible for enforcing National Maritime Legislation in their maritime zones (MLEA) such as Coast Guard, Navy, Maritime Security Agency (MSA) and Marine Police.

(c) The people who operate and manage ships such as Ships Masters, Shipping Companies, Organizations working for the Maritime Sector and Shipping Associations (Others).

These questionnaires were circulated through the WMU Dissertation Portal with a secure username and password for each questionnaire, to International, Regional bodies, IMO member states and their maritime law enforcement agencies, Master mariners, leading maritime associations and maritime academics experts. The responses received have been critically analyzed and expressed in the dissertation.

The research work of the dissertation has been divided into five chapters. Chapter one is the introductory chapter to the dissertation. Chapter two will take an overview of maritime security, discussing the threats to maritime security and the legal instruments available within the industry for preventing and mitigating them. Chapter three discusses the various developments, legal and technological, that have taken place over the years, especially after the 9/11 incident. It will also cover the issues that need attention for effective implementation of these developments. Chapter four critically analyses the strengths and weaknesses of technology, and brings forth different solutions available for effective utilization of technology for enhancing maritime security. For ease of critical analysis, the technology in the maritime sector has been classified into four categories namely, technology primarily for maritime security, safety based, threat perception based, and systems setup for safe navigation.

The chapter also correlates the effectiveness of technology with the views of the maritime sector obtained through the questionnaire. Chapter five concludes the dissertation making recommendations that the author feels will help pave the path for enhancing maritime security in the years to come.

CHAPTER 2

MARITIME SECURITY - ITS NEED TO INDUSTRY

"It is a curious situation that the sea, from which life first arose, should now be threatened by the activities of one form of that life. But the sea, though changed in a sinister way, will continue to exist; the threat is rather to life itself"- **'The Sea Around us' by Rachel Carson**

Shipping has been the most liberal form of transportation with a high degree of flexibility in its movement. This very nature of shipping inculcated fearlessness in the system, resulting in lack of investment for training of personnel and infrastructure development for maritime security, and a general lack of understanding of the threats posed to the ships and their crews. This chapter will provide an overview of the maritime security and dwell on some definitions, the vulnerability of the maritime sector to the crimes such as piracy, armed robbery against ships and maritime terrorism, and finally the preventive measures that are available in the form of international instruments.

2.1 Overview of Maritime Security and Definitions

2.1.1 An Overview

For ages, shipping has been vulnerable to various maritime crimes. The data in Appendix B (prominent breach in maritime security incidents) collected from the readings undertaken by the author is a clear reflection of the fact that the industry was exposed to various maritime crimes year after year. Threats to the maritime industry were also seen during the Iran-Iraq war days. Numerous ships and maritime infrastructure were targeted during the period 1980- 1988 (Michel, 2006). Hijacking of the Achille Lauro on October 7, 1985, an Italian cruise ship carrying 400 passengers by the Palestinian Liberation Front and killing of 69-year-old Leon Klinghoffer, a Jewish-American exposed the lack of security in the industry. This incident raised the concerns of the International Maritime Organisation is member states, as it involved numerous human lives.

The terrorist attack on the United States in 2001 further drew the attention of the world community to the severity of the crime that may be committed and the motivation level of criminals. Hijacking of an aircraft involves crossing of security barriers in the presence of security officials. However, no such barrier exists when a ship is at sea. Criminals can easily board a ship, overpower the crew and exploit it for achieving their goals. Some security experts (Steve Johns, Peter Chalk) fear that the biggest nightmare would be if a ship carrying explosive cargoes like LNG were to be hijacked to be used as Weapon of Mass Destruction (WMD) by intentionally colliding it with a strategic target [4] (Franson, 2005; Kanev, 2005; Nincic, 2005; Richardson, 2004; Timlen, 2002; Trelawny). The extent of damage that could be caused in such incidents can be seen from the collision between Norwegian steamer, Belgian relief ship Imo and ammunition steamer Mont Blanc[5] on December 6, 1917 in Halifax Harbor. The collision resulted in an explosion that destroyed more than 325 acres of Halifax city, killing more than 1600 people and injuring more than 9,000, and destroyed more than 12,000 buildings ("The Halifax Explosion", 1917).

2.1.2 Maritime Security Definitions

Maritime security has been defined in different ways, some of which are produced below for looking into the objectives of maritime security.

Hawkes (1993, p. 83) defines maritime security as "those measures employed by owners, operators and administrators of vessels, port facilities, offshore installations and other marine organizations or establishments to protect against … any hostile interference with lawful operations".

According to Steven M. Jones (2006, p. 1) maritime security is "the state of a shipping company/vessel/crew/port, being or feeling secure or the safety of a

[4] Such as bridges, oilrigs or other port facilities.
[5] The *Mont Blanc* was laden with 180 tons of TNT, 2,300 tons of picric acid and 10 tons of gun cotton.

shipping company/vessel/crew/port against such threats as terrorism, piracy, and other criminal activities".

Mejia (2007 , p. 5) defines maritime security as,

> …….. the state of being free from the threat of unlawful acts such as piracy, armed robbery, terrorism, or any other form of violence against ships, crews, passengers, port facilities, offshore installations, and other targets at sea or in coastal areas. In maritime studies the term maritime security is differentiated from the term maritime safety which deals with preventing accidents at sea that may be caused by, *inter alia*, fortuitous incidents, substandard ships, unqualified crew, or operator error.

2.2 Fears and Facts in Maritime Security

Maritime security risks to the industry range from terrorizing of crew, hijacking of ships and attacks on ships and port facilities to disrupt the supply chain so as to causing economic losses (Banlaoi, 2005; Mbiah, 2007; Timlen, 2005; Weeks, 2005). Ransom money involved for release of hijacked merchant ships and their crews ranges from $350,000 to $500,000 and some experts estimate that the value of cargo lost per hijacked ship is between $8 million and $200 million (Howland, 2004b).

Shipping relies on economies of scale[6] and as certain cargoes carried are highly volatile their sheer volume causes a high degree of danger. For example, LNG is highly volatile in nature and if exposed to an ignition will result in a big explosion engulfing an area which in some cases may be up to one square kilometer ("LNG

[6] Large volume of goods shipped in one trip.

tanker terrorism", 2007). Therefore, some have named the LNG tankers as "floating bombs" (Jane's Terrorism and Insurgency Intelligence Centre, 2007). Nigel Wilson (2008), energy writer quotes, the U.S. Government accountability Office (GAO)[7] reporting the LNG supply chain being vulnerable to suicide attacks by explosive-laden boats, a "standoff" attack with weapons launched from a distance; and armed assaults.

In the past it has been seen that ships have been used for illegally transporting weapons of mass destruction, explosives, illegal materials and contrabands, and terrorists as stowaways. Confiscation of an assembly line for ballistic missiles, by Indian customs officials at the port of Kandla[8] on June 30, 1999 (Warrick, 2003, p. A01) and seizure of approximately 8,000 assault rifles and automatic weapons from three cargo containers by Italian customs officials in the port of Gioia Tauro on April 10, 2004 (Howland, 2004a) are examples of illegal activities.

Shipping is the most affordable and luxury means of transportations for the more than 12 million passengers cruising each year (Cruise Lines International Association, 2008). Passenger and cruise ships are a high profile target, as any apprehension will raise a huge hue and cry in the society. In the past, it has been seen that such incidents give maximum commercial impetus for media and thus the situation is exploited by them through social amplification of risk frame work[9](Kasperson, 2004; Kasperson, Pidgeon, & Slovic, 2003). The hijacking episode of Achille Lauro in 1985 is an example.

---

[7] The U.S. Government Accountability Office (GAO) is the investigative arm of the Congress and the congressional watchdog. GAO facilitates the Congress in meeting its constitutional responsibilities and to improve the performance ensuring accountability of the federal government for the benefit of the American people.

[8] Kandla is a major seaport in Kutch District of Gujarat state in western India.

[9] Risk is amplified or attenuated due to various dynamic social processes in the society.

The above listed incidents are clear indications that there is a prevalent threat to the maritime assets. Therefore, there is a need to protect the maritime assets from the perils of maritime crime (Yilmazel & Asyali, 2005), (Figure 1). The questionnaire survey results also indicate that the respondents feel there is a need to enhance maritime security for protection of maritime assets and its users (Figure 2). For the purpose of the dissertation the term ship implies those engaged in international voyage[10] as defined in regulation 2 of chapter XI-2 of SOLAS 74.

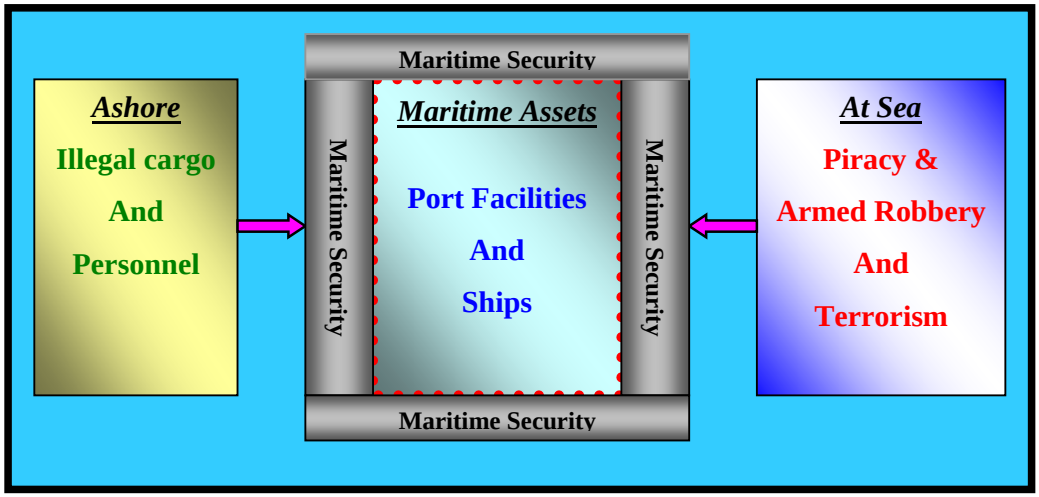


Figure 1: Threat to maritime assets.
Source: Author 2008.

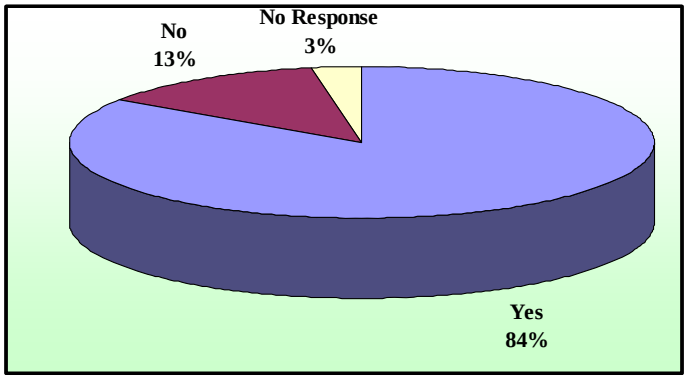


Figure 2: Need for enhancing maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

[10] Passenger ships, including high-speed passenger craft, Cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and mobile offshore drilling units engaged on international voyages.

In order to protect these assets it is important to carry out an analysis of the growth of maritime crimes namely Piracy and Armed Robbery, and Terrorism over the years and the legal instruments developed for enhancing maritime security.

2.3 Threats to Maritime Security

Today threats as to maritime security are posed by maritime crimes shown in Figure3.

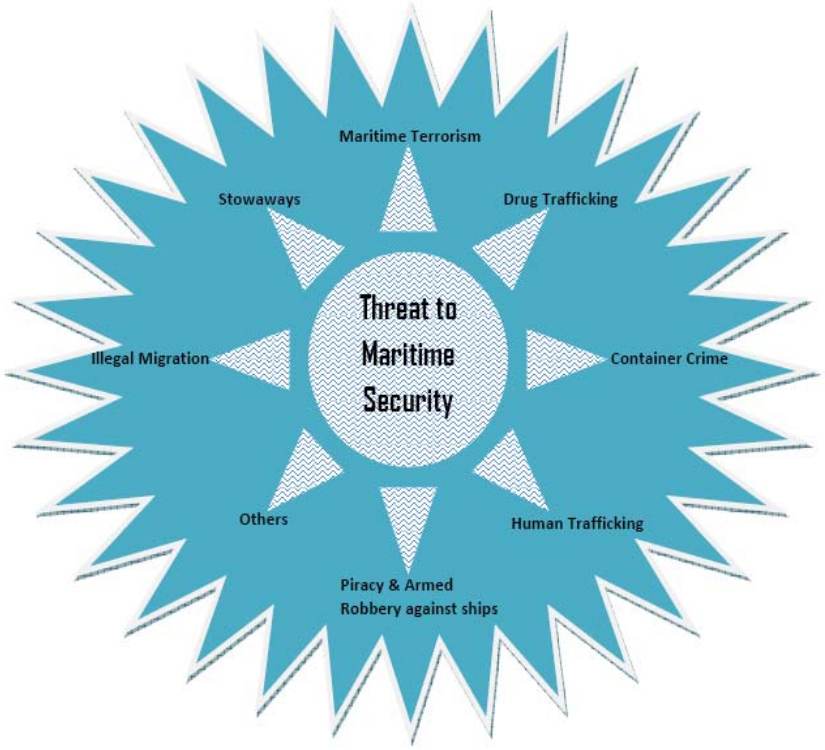


Figure 3: Maritime Crimes posing threat to Maritime Security.
Source: Author 2008.

With rising incidents of piracy and armed robbery against ships and the consequences of maritime terrorism, experts in the field feel that these are the two crimes that pose the greatest threats to maritime security (McNicholas, 2008). The survey results also supplement this view (Figure 4). Hence, the scope of the dissertation is limited to these maritime crimes.

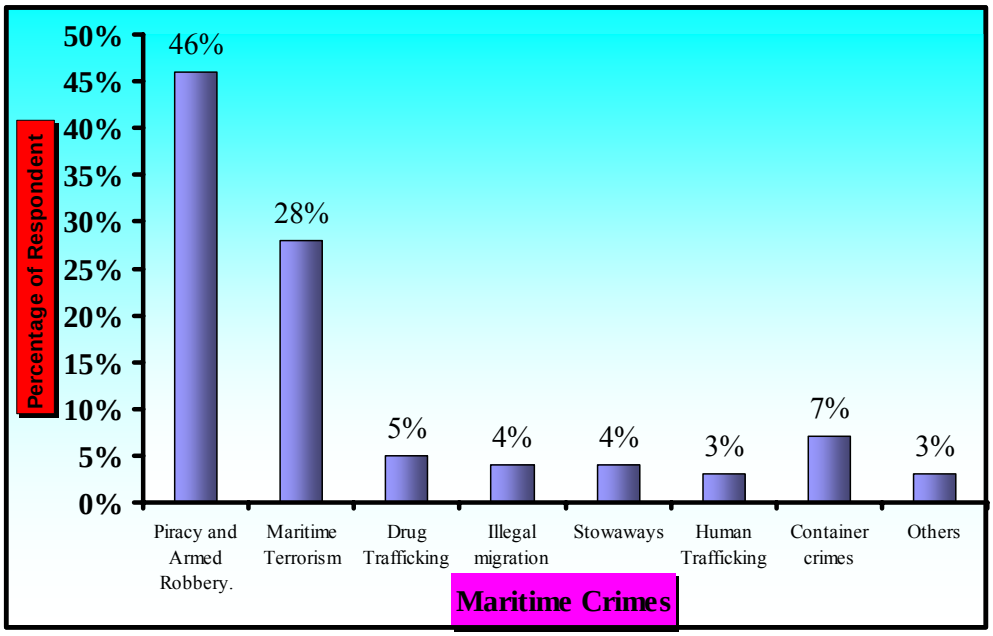


Figure 4: Degree of threat posed by Maritime Crimes to Maritime Security.
Source: Data compiled by author from the responses received from the questionnaire survey.

2.3.1 Piracy and Armed Robbery against Ships

Piracy has been prevailing in some form or the other since ancient times. Thucydides in his book "The History of the Peloponnesian war" which took place in 431 B.C.[11] said "The first person known to us by tradition as having established a navy is Minos. He made himself master of what is now called the Hellenic sea ... and thus did his best to put down piracy in those waters" (Thucydides, 2006, p. 7).

Since antiquity piracy has been posing a threat to ships, its crew and the cargo. It has ridden the tide, becoming a menace at one time and then subsiding during other times (Tomberlin, 2008). Capitalism and technology has assisted in making piracy and armed robbery against ships bloodier and more violent (McNicholas, 2008). Today, the objective of piracy is no longer theft of cash, valuables belonging to crew, and ships store. According to Chamberlain (2008) today's pirates "no longer dress like

[11] Before the common, or Christian, Era.

characters from the Disney film Pirates of the Caribbean, but the buccaneers of the 21st century have lost none of their taste for a bloodthirsty boarding". He further writes "gone are the cannon and cutlass, which have been replaced by rocket propelled grenades and automatic rifles,…… the spirit of Johnny Depp's Captain Jack Sparrow is alive and terrorizing the ocean waves (Chamberlain, 2008). The world community has an image of pirates as colorful swashbucklers from the 18th and 19th century Caribbean. Credit for such a portrait goes to the literary and cinematic world that portrays pirates as romantic and rebellious characters. For some, it is a sea borne version of Robin Hood (Abhyankar, 2006; Frecon, 2006; Mejia, 2003).

Piracy as a menace and its global impact can be seen from the convention on the High Seas, 1958[12] and UNCLOS[13] 1982. These conventions address the acts of piracy at sea and recognize it to be a universal crime, considering it as a crime and *dignus*[14] punishable under the laws of every state.

It is important to note that this menace started as a maritime mugging, wherein the motive was to rob cash and valuables from the ship. However, it grew as an organized crime with hijacking of ships, selling the entire cargo and further operating the ship with fraudulent documentation taking advantage of the administrative lacunae due to lax regulations of the open registers (Mukherjee & Mejia, 2005).

Piracy has flourished in regions marred by political instability or poor economic growth or bear a complex coastal terrain (Abhyankar, 2005). To name such regions, Southeast Asia and Africa today are the hotspots of piracy. Poor economic growth drives the coastal community to resort to theft and robbery from the ships for

[12] *Article 14:* All States shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any State.
[13] United Nations Convention on the Law of the Sea.
[14] Worthy.

livelihood given their familiarity with the seas. Furthermore, the situation becomes more grim due to lack of resources with these governments to provide adequate security to combat such incidences (Eklöf, 2005; Ong-Webb, 2007).

Jones classifies piracy into four categories, depending on the gravity of crime and its planning, namely

- Opportunity Crimes
- Low Level Armed Robbery
- Medium Level Armed Assault and Robbery
- Major Criminal Hi-jacking (Jones, 2006, pp. 16-18)

The International Maritime Bureau (IMB)[15] classifies piracy on the basis of *modus operandi* of attack:

- opportunity theft by persons who manage to gain access to the vessel, in port or at anchor, and steal anything handy such as paint or mooring ropes;
- planned robbery, alongside, at anchor or underway, targeted mainly at money, crews' personal effects, and ships' equipment, often carried out by increasingly organized, determined and well-armed gangs;
- Permanent hijacking of ships and cargoes with crews sometimes being murdered cast adrift or held to ransom (Abhyankar, 2007).

Today piracy covers a wide range of acts of maritime violence starting from petty thefts of ropes, personal belonging of crew, etc to hijacking of ships and operating it

[15] Established in 1981 is a specialized division of the International Chamber Of Commerce (ICC). IMB's main task is to protect the integrity of international trade by seeking out fraud and malpractice Therefore its Main focus is to fight against all types of maritime crime and malpractice. The International Maritime Organization (IMO) in its resolution A 504 (XII) (5) and (9) adopted on 20 November 1981, has inter alia, urged governments, all interests and organizations to cooperate and exchange information with each other and the IMB with a view to maintaining and developing a coordinated action in combating maritime fraud.

under a fictitious name and becoming a phantom ship as shown in Figure 5 (Mejia, 2003, pp. 161-164; Valencia, 2006).

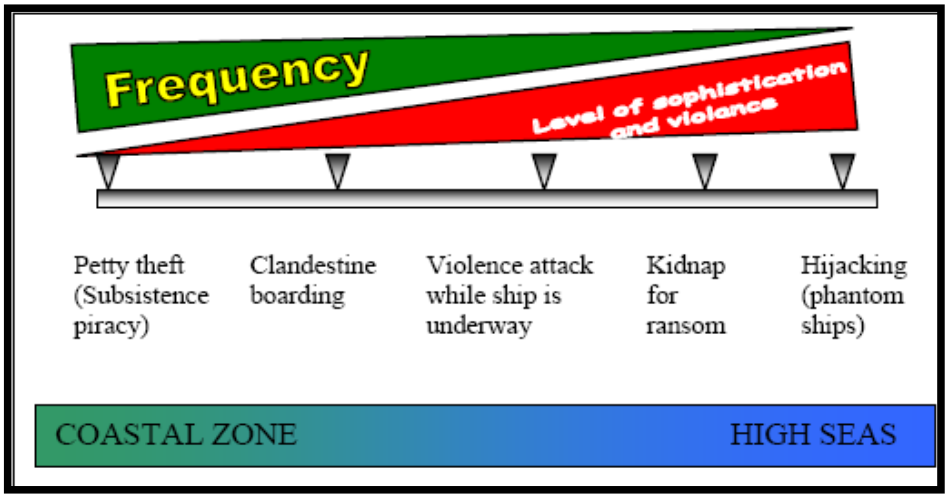


Figure 5: Spectrum of violent act against shipping with varying degree of sophistication in different water with frequency of commitments.
Source: Mejia MQ Jr (2007). *Law and ergonomics in maritime security*. Published doctoral thesis. Lund: Department of Design Sciences, Lund University.

The piratical attacks at the two hotspots of the world today are committed with entirely different motives. In the case of piratical attacks in Southeast Asia, the motive is to attack such ships whose cargo is in great demand so that it can be sold in the black market, whereas in Somalia piratical attacks are primarily for ransom (Abhyankar, 2007). Noel Choong, head of Malaysia's Piracy Reporting Centre, told Fairplay that "It is a commodity that is easily disposable and is yet to hear of pirates seizing VLCCs laden with crude oil" (Prakash, 2008, January 10).

Fairplay reported Somali piracy having links with criminal gangs based at Dubai and the attacks being masterminded by them to raise funds for their operations. These reports are also authenticated by a recent incident, wherein the Danish registered Danica White and its crew was released by Somalia pirates after a reported payout of a ransom of $1.5M ("Somali pirates are tied to Dubai", 2008, January 3). David Osler reported that in seven of the 26 piratical attacks till June 2008, pirates had received an average ransom of over $200,000. This money would be further utilized

for purchasing more AK-47s (Osler, 2008). In the first six months of 2008, a total of 114 incidents were reported to IMB, out of which 71 vessels were boarded, 12 vessels hijacked and 11 were fired upon. A total of 190 crew members were taken hostage, six kidnapped, seven killed and another seven are missing, presumed dead. Osler quotes IMB Director Captain Pottengal Mukundan having stated: "The frequency and level of violence directed at seafarers is cause for alarm. The abduction of crew and the increasing use of automatic weapons remain unacceptable".

2.3.2 Maritime Terrorism

During recent years, maritime terrorism has drawn considerable attention in the maritime sector. Piracy is viewed as a crime solely for private gains, whereas terrorism has a political objective behind it (Michel, 2006; Sakhuja, 2007; Valencia, 2006). When looking into the maritime history, hijacking of the passenger liner Santa Maria in 1961 was an incident of maritime terrorism of modern time. Later, the seizure of Achille Lauro in 1985 led to the adoption of 'The Suppression of Unlawful Acts against the Safety of Maritime Navigation' (SUA) Convention in the year 1988 (Mensah, 2005; Raymond, 2005).

Maritime terrorism is not restricted to hijacking and seizure of ships. The attack on USS Cole in 2000 by suicide bombers, while refueling in the port city of Aden, Yemen is an example. A similar type of attack on an LNG tanker caused huge panic (Daly, 2008). According to Professor James Fay, Massachusetts Institute of Technology "Once ignited, as is very likely when the spill is initiated by a chemical explosion, the floating LNG pool will burn vigorously…Like the attack on the World Trade Center in New York City, there exists no relevant industrial experience with fires of this scale from which to project measures for securing public safety". (Hurst, 2008).

Utilizing a ship as a weapon against another ship or blocking vital choke points on the major sea routes, or attacking port facilities or vital installations on the coastlines,

as was done in the case of 9/11 attacks, is very much a possibility (Richardson, 2007). Reports indicate that terrorist organizations intend to disrupt the oil supply by blocking of choke points (Jones, 2006). In 2007 around 85 million bbl/d [16] oil was transported through shipping and 43 million bbl/d amounting to 50% of transshipment passes through the world oil transit chokepoints[17](US Government, 2008, p.1). Blocking of choke points will cause heavy financial losses as seen in the case of collision of the supply ship Lee with another ship, in the Southwest Pass entrance to the Port of New Orleans on February 21, 2004. The estimated loss to the Port of New Orleans was $3 million dollar every day (Howland, 2004b). Thus blocking of choke points can cause economic recession in many countries. Consequences of disruption of world choke points are found in Appendix C.

Incidents of maritime terrorism are very few as compared to piracy; however, it attracts more media attention due to involvement of greater loss of life, property and consequential economic losses. The psychology behind the motive of terrorism is not material or monetary gains, but to create panic in the society for more publicity, and to elicit fear and horror (Kanev, 2005). Table in Appendix D lists maritime terrorism incidents compiled from the various readings undertaken for the dissertation.

Valencia quotes Brian Jenkins[18], Captain P.K. Mukundan[19] and Admiral Thomas Fargo[20] having said that presently there is no authenticated report that establishes a link between piracy and terrorism (Valencia, 2006). However, Howland[21] (2004b) quoting, London-based security consultants Aegis Defence Service (ADS) in its October 2003 terrorism report warns against the threat posed by the partnership between maritime piracy and maritime terrorism. He further quotes a study carried

[16] Barrels per day.
[17] Chokepoints are narrow channels in the sea routes.
[18] A terrorist expert and senior advocate at RAND Corporation.
[19] Director IMB
[20] U.S. Commander-in-Chief of the Pacific fleet
[21] Editorial Assistant in The Jewish Institute for National Security Affairs (JINSA)

out by Chalk for RAND Corporation, which reveals that favorable environment for terrorists and pirates to operate is mainly due to little government regulation, absence of effective marine policing capabilities, and the necessary adherence of merchant vessels to established international sea-lanes (Howland, 2004a).

Howland (2004b) further reports, U.S. intelligence officials have identified between 12 and 300 ships possibly owned and/or operated by the al Qaeda terrorist group (Banlaoi, 2005; Richardson, 2004; Richardson, 2007). A recent study by the RAND Corporation indicates, "There have been persistent reports of political extremists boarding vessels in Southeast Asia in an apparent effort to learn how to pilot them for a rerun of 9/11 at sea," ("Piracy on the rise, but terrorism link not seen: Study", 2008). With the ongoing war on terrorism by the United States and its allies, the possibility of terrorist and pirates synergizing again security forces cannot be ruled out. How the two groups will associate with each other, time will testify (Ong-Webb, 2006a).

Since terrorism has a political motive linked to it, there has been no consensus on the definition of terrorism at the international level. According to Mejia (2003, p. 169), neither SUA 88 nor the twelve other international conventions and treaties focusing on terrorism give the definition of terrorism. The international conventions and treaties on terrorism are placed at Appendix E.

2.4 Legal Framework for Maritime Security

2.4.1 Present Instruments

Having seen aircraft being used as the weapon of mass destruction, the fear of a ship being transformed by terrorists, from a medium of transport to a weapon of mass destruction, in future, cannot be ruled out. While the industry was struggling to tackle piracy, 9/11 took it by surprise. Such an act was unthinkable by the world community. Uncertainty in mind led to intensive negotiations for fostering higher degree of security and the year 2002 resulted in the adoption of maritime security instruments at IMO, amendments to the International Convention for the Safety of

Life at Sea (SOLAS) 1974, and the concomitant International Ship and Port Facility Security (ISPS) Code. In addition to these, Articles 100-107 of the United Nations Convention on the law of the Sea (UNCLOS) 1982, and the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA) Convention, comprise the international legal umbrella for maritime security.

Mukherjee and Mejia (2004a, pp. 316-317) classify the international legal frame work for maritime security into criminal and regulatory Law (Figure 6). The criminal law basically defines the maritime crimes and regulatory law enumerates measures to be taken to prevent maritime security incidents. They categorize UNCLOS and SUA under criminal law and SOLAS and ISPS under the provisions of regulatory law.

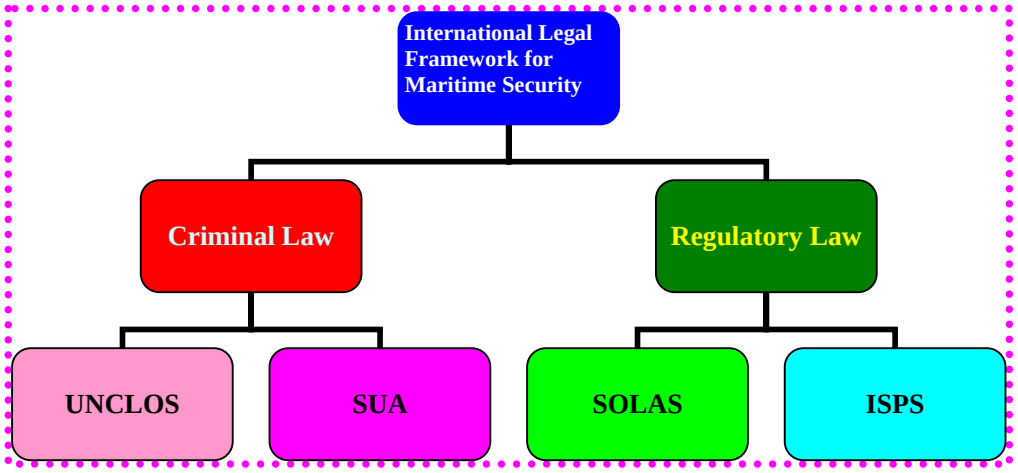


Figure 6: Criminal and Regulatory law in the international legal framework for maritime security.
Source: Mejia MQ Jr (2007). Law and ergonomics in maritime security. Published doctoral thesis. Lund: Department of Design Sciences, Lund University.

The respondents of survey are of the opinion that the existing provisions of present instruments are inadequate for combating maritime crime (Figure 7).

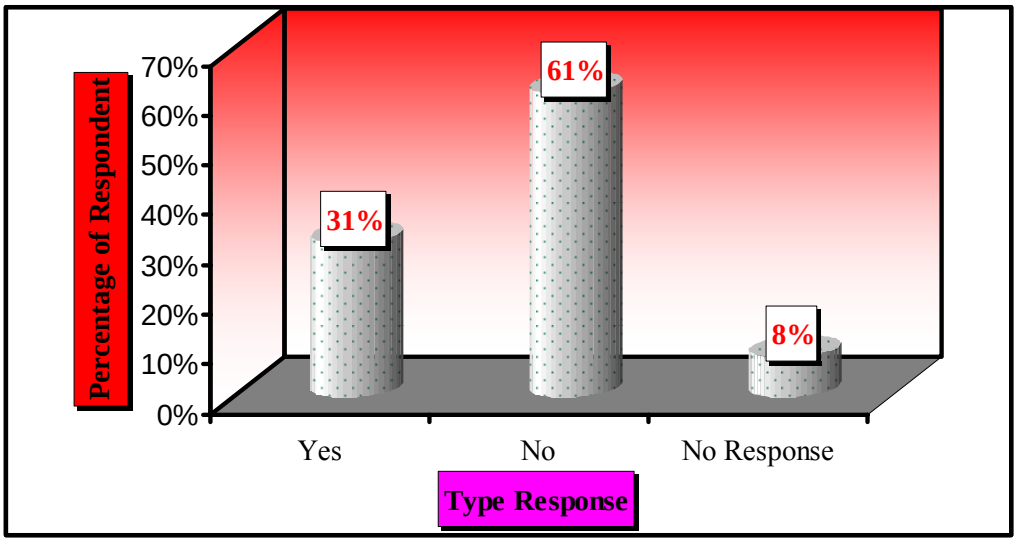


Figure 7: Adequacy of present instruments.
Source: Data compiled by author from the responses received from the questionnaire survey.

2.4.2 Future Developments

During recent years, the concept of maritime violence[22] has been gaining focus owing to the need to achieve both common international law and municipal law objectives with respect to piracy, terrorism, armed robbery against ships. Well chalked out laws would save the prosecutors from establishing critical legal intricacies, such as whether the act was on the high seas or in territorial waters, whether the motive was political or for material gains, and ensure successful conviction whenever such crimes are committed (Mejia, 2003).

The Comite Maritime International's (CMI) effort in drafting the Model National Law on Acts of Piracy and Maritime Violation is a way forward in resolving the legal technicalities. It purports to bring about consistency and uniformity in national laws for suppressing piracy and acts of maritime violence as well as in reporting and investigation of incidents (Comite Maritime International, 1997). The Comité

[22] The term "maritime violence" is used to designate those acts *generally* covered by the Rome Convention, as well as others, which might not support the sobriquet of "piracy".

Maritime International (CMI) has submitted a paper to the IMO Legal Committee at its 93rd session (Document LEG 93/12/1) containing proposed draft guidelines for national legislation on maritime criminal acts, including piracy (International Maritime Organization Legal Committee, 2007). According to Mukherjee and Mejia (2004b, p. 322) adoption of the Model National Law will fill the gap in the piracy provisions of UNCLOS and maritime offences in SUA. Its definitions of piracy and other acts of maritime violence overcome the limitations in UNCLOS and SUA.

It may be seen from the foregoing that piracy and terrorism pose a real threat to maritime security and result in severe consequences. Effective implementation of available instruments together with the spectrum of available technology is therefore inevitable. Towards this, IMO has adopted legal instruments mandating fitment of certain equipment for enhancing maritime security. Chapter 3 will look at the legal and technological developments that have taken place over the years in the field of maritime security.

CHAPTER 3

LEGAL AND TECHNOLOGICAL DEVELOPMENTS IN MARITIME SECURITY AND ITS IMPLEMENTATION

> "Where the old Maritime Strategy focused on sea control, the new one must recognize that the economic tide of all nations rises—not when the seas are controlled by one—but rather when they are made safe and free for all". - **Admiral Michael Mullen, Chief of Naval Operations,(Current Strategy Forum, Naval War College, 14 June 2006)**

The ramming of 'USS Cole' by an explosives laden boat in 2000, the 9/11 terrorist attack on twin tower in 2001 and the attack on the French tanker 'Limburg' off the coast of Yemen in October 2002 were the key events that triggered the IMO to consider a review of "measures and procedures to prevent acts of terrorism, which threaten the security of passengers and crews and the safety of ships" (Burmester). The international maritime community has recognized the vulnerability of the shipping industry to maritime terrorism and the need for adopting stringent security measures in order to protect the maritime assets (Nincic & Clark). This chapter reviews the various legal developments that took place in maritime security leading to adoption of new technology to enhance maritime security. Further, it looks into factors that are essential for effective implementation of these developments.

3.1 Developments at International Level for Enhancing Maritime Security

In the wake of the 9-11 incidents, it was not only the IMO that laid emphasis on maritime security but also the United Nations and other international agencies associated with the maritime sector too strengthen their security measures. Some of the major initiatives in legal and technological developments related to maritime security taken by these international bodies were as follows:

3.1.1 United Nations

United Nations [23] Security Council unanimously adopted resolution 1317 on December 17, 2001 (United Nations). The resolution obliges all the member states to "criminalize assistance for terrorist activities, deny financial support and safe haven to terrorists and share information about groups planning terrorist attacks". It also recommended setting up of 15-member Counter-Terrorism Committee (CTC) to monitor implementation of the resolution (United Nations, 2001). The Security Council adopted resolution 1535 and created the Counter-Terrorism Committee Executive Directorate (CTED) for facilitating expert advice to CTC under resolution 1373. Further, it provides technical assistance to countries, maintains closer cooperation and coordination within the UN organization and intergovernmental bodies (United Nations, 2004).

United Nations in a land mark decision[24] adopted a global counter-terrorism strategy on September 8, 2006. Kofi Annan, the former Secretary-General, proposed for a comprehensive counter-terrorism strategy that identified five key elements as basic elements namely "dissuading groups from resorting to terrorism; denying terrorists the means to carry out an attack; deterring states from supporting terrorist groups; developing state capacity to prevent terrorism; defending human rights in the context of terrorism and counter-terrorism" (United Nations, 2006).

UN Security Council Resolution 1816 (2008) authorized member states to suppress acts of Piracy and Armed Robbery off the coast of Somalia by all means and member state forces operating in the area to maintain vigil. Countries trading, or their ships

[23] United Nations name was coined by United States President Franklin D. Roosevelt, was first used in the "Declaration by United Nations" of 1 January 1942, during the Second World War for promoting international cooperation and to achieve peace and security in the world. The United Nations officially came into being on 24 October 1945(United Nations). Presently 192 countries are its members. International Maritime Organisation is a specialized agency of United Nation for coordinating matters related to shipping.

[24] It was the first time that all countries in the world agreed on a common approach to fight terrorism.

transiting through the waters close to Somalia can participate in coordination with Transitional Federal Government (TFG). Thus, foreign forces were permitted to enter into territorial waters for suppressing the act for a period of six months from the date of adoption of the resolution (United Nations, 2008, June 2). Such a step by a sovereign state to seek assistance of United Nations to combat maritime crime is a positive step of its commitment towards the world community and will be recognized by the world in years to come.

3.1.2 International Maritime Organisation

The International Maritime Consultative Organisation Convention was adopted in 1948 at an international conference in Geneva. The name was changed to International Maritime Organisation in the year 1982 ("History of IMO"). The primary objective was for enhancing safety in the shipping by framing international instruments and providing technical assistance to its members (Mitropoulos, 2005).

IMO is the international apex body coordinating maritime affairs and regulating the shipping industry. Its primary objective is to make travel and transportation by sea, as safe and secure as possible. IMO since its inception has adopted not less than 50 international conventions and protocols, covering different aspects of maritime safety, security, pollution prevention, liability and compensation, and facilitation of maritime traffic and salvage. The instruments are supported by codes, guidelines, and recommended practices. The literature covers ships from the drawing board to the scrap yard (International Maritime Organisation, 2008). Today, the IMO has 167 Member States.

In the course for enhancing maritime safety, IMO has adopted technology meeting the technical standards set by it. This approach of IMO can be credited for having paved the path for advancement in technology for the maritime sector, year after year. The equipment fitted on board in compliance with SOLAS Chapter V, basically adopted for safety of navigation, in the present day scenario can also play a vital role in enhancing maritime security. The author during the research found that some of

the features in this equipment are effective for alerting the operator to an incident that could also result in breach of maritime security. Furthermore, some of the equipment complements each other in terms of making the information more reliable or being a source of information when other equipment has technical limitations. The application of these features in enhancing maritime security will be critically analyzed in Chapter 4 of the dissertation.

The author did not find any measures that were promulgated by IMO prior to the 9/11 incidents, for preventing any maritime security incident. Only legal instruments were available for trial once the crime has been committed. The preventive measures that are available are fallout of the incident. In the wake of 9/11, IMO adopted new preventive instruments for enhancing maritime security. It developed standard operating procedures and also recommended fitment of latest technology for raising alert from sea. The motive was to alert the flag security agency for early response to any maritime security incident. IMO has since been working in close liaison with other international and regional bodies for strengthening maritime security. It has adopted new measures and standards for curbing maritime crime so as to make shipping safe and secure at all times. Leading initiatives in the maritime security field are enumerated in the succeeding paragraphs.

IMO through its Assembly Resolution A.924 (22) in November 2001 took numerous initiatives after having taken stock of the existing instruments for preventing and suppressing acts of terrorism against maritime asserts both afloat and ashore. Its objective was to:

- Mitigate the risk to passengers, crews and port personnel on board ships and in port areas,
- ensure security of vessels and their cargoes,
- enhance measures for ship and port security, and
- avert shipping falling prey to international terrorism.

Further, IMO boosted its technical cooperation programme by assisting the developing countries with funds amounting to GB £1.5 million so as to cope with the growing demand for maritime security in the wake of threats from terrorism (Hesse, 2003; Hesse & Charalambous, 2004). During the period under reference, approximately 4,390 people were trained in issues related to various aspects of maritime security through 41 country advisory missions and 27 regional and 55 national seminars, workshops and courses (Hesse, 2007). In addition, the IMO conducted, in December 2005 sub-regional workshops at Manila, Philippines for Southern and Eastern Asian countries and April 2006 for countries of the Indian subcontinent and parts of the Indian Ocean, in Mumbai, India (Blanco-Bazán, Jianxin, Hesse, & Charalambous).

Besides, seventeen courses on maritime security were launched worldwide under the 'Train-the-Trainer' campaign, a six-day course focused on developing instructors for imparting further training on maritime security. Till June 2006, around 577 persons were trained through this campaign (Hesse, 2007). Furthermore, it adopted amendments for the instruments, equipment and other measures for fostering maritime security are placed at Appendix F.

IMO also signed a Memorandum of Understanding (MoU) in July 2001 with the World Customs Organization (WCO) for closer co-operation and formulated a joint ILO/IMO Working Group that drafted comprehensive guidelines and a draft Code of Practice for the security of all port areas (Trelawny, 2003).

3.1.3 International Maritime Bureau and its Contributions to Maritime Security

The International Maritime Bureau (IMB) [25] is a non-profit making organization, established in 1981 to act as a focal point in the fight against all types of maritime

[25] It is a specialized division of the International Chamber Of Commerce (ICC).

crime and malpractice. The International Maritime Organization (IMO) in its resolution A 504 (XII) (5) and (9) adopted on 20 November 1981, had urged its member states and other organizations associated with shipping to cooperate and exchange information with each other and IMB with a view to maintaining and developing a coordinated action in combating maritime piracy. The IMB Piracy Reporting Centre, based in Kuala Lumpur, Malaysia, was started in 1992. The Centre maintains a round-the-clock watch on the world's shipping lanes, informing local law enforcement agencies regarding piratical attacks in their jurisdictions. IMB launched a new hotline in 2007 and according to IMB director Pottengal Mukundan "we will now cover the entire spectrum of maritime crime" ("IMB launches new hotline", 2007, August). IMB also maintains a databank of all piratical attacks reported to them and circulates them to the IMO and other interested organizations through monthly, quarterly and annual reports. The information circulated by IMB has been vital for mitigating this peril in some parts of the world and enhancing maritime security. The number of piracy incidents reported to IMB from 1991 till 30 June 2008 is shown in Figure 8.

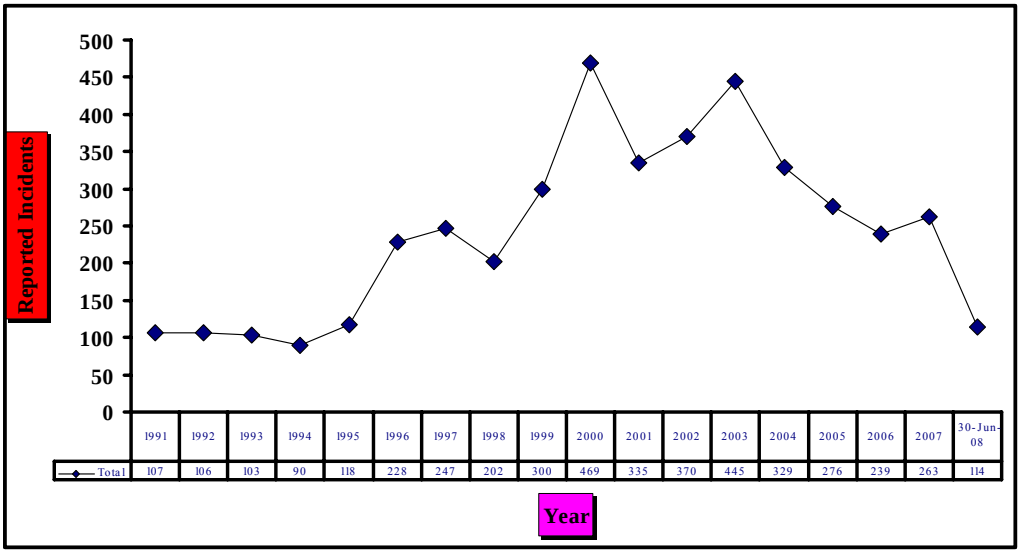


Figure 8: Piracy Incidents reported to IMB.
Source: Data compiled by author from IMB annual reports receive through e-mail from IMB Piracy Reporting Centre.

3.1.4 International Labour Organization (ILO)

The ILO is a specialized agency of United Nation created in 1919 on termination of World War I. The motive of its creation was to bring everlasting peace in the world through social justice. 182 countries are presently its members. It is the international meeting place for the world of work (International Labour Organization, 2008). ILO has been working in close liaison with IMO on various issues of seafarers such as minimum working hours and manning of ships (C180) Health Protection and Medical Care (Seafarers) (C164), and Seafarers' Welfare Convention (C163). Development of new seafarer's Identity Document (SID) C185 is the way forward in enhancing maritime security and will prevent illegal access to ships and port facilities.

3.1.5 World Customs Organization (WCO)

The WCO[26] adopts instruments related to Customs matters for regulating world trade. Its mission "is to enhance the protection of society and the national territory, and to secure and facilitate international trade…." It works in close liaison with IMO on various matters related to maritime trade and formulation of policies for improving the efficiency of customs organizations in the world. It developed a Framework of Standards to Secure and Facilitate Global Trade by its members (World Custom Organisation).

3.1.6 International Organization for Standardization (ISO)

It published ISO/PAS 28000:2005 standard ``Specification for security management systems for the supply chain". These new supply chain management standards will reduce risks of terrorism, piracy and fraud (Peleg-Gillai et al., 2006). Craig K. Harmon (2007, August 08), Chairman of joint the working group on supply chain applications of RFID, is of the view that the new ISO standard on the technology for

[26] The World Customs Organization (WCO) is an intergovernmental body established in 1952 for enhancing the effectiveness and efficiency of Customs administrations world wide. Today there are 173 members with approximately 98% of world trade.

tracking container movement has a potential to minimize handling costs, improve suppliers inventory due to tracking and updated information, which in turn will create a safe and secure international supply chain regime.

3.2 Regional Developments for fostering Maritime Security

3.2.1 Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia (ReCAAP)

It is the first multilateral government-to-government anti-piracy and armed robbery organization consisting of 16 countries[27] for combating Piracy and Armed Robbery against ships in Asia. The agreement came into force on September 4, 2006. The objective of the agreement is to share information facilitating operational cooperation and capacity building to combat piracy and armed robbery in the region. In order to achieve its objective an Information Sharing Centre (ISC) has been setup in Singapore for interacting with the focal point of the member countries (ReCAAP Agreement, 2006).

3.2.2 European Union (EU)

EU adopted regulation 725/2004 for enhancing ship and port facilities security. In pursuance of this regulation it promulgated directive 2005/65/EC on October 26, 2005 to further strengthen the security of port facilities (Blumel, Boeve, Recagno, & Schilk, 2008). It has formulated a comprehensive policy for its members entitled, 'towards a future Maritime Policy for the Union: A European Vision for the oceans and seas' (Eteris, 2008) and promulgated measures for maritime security for its member states(European Union, 2005, October 26). Project MarNIS[28], which is a Community Vessel Traffic Monitoring and Information System, aims to establish a

[27] People's Republic of Bangladesh, Brunei Darussalam, the Kingdom of Cambodia, the People's Republic of China, the Republic of India, the Republic of Indonesia, Japan, the Republic of Korea, the Lao People's Democratic Republic, Malaysia, the Union of Myanmar, the Republic of the Philippines, the Republic of Singapore, the Democratic Socialist Republic of Sri Lanka, the Kingdom of Thailand, and the Socialist Republic of Viet Nam.

[28] Maritime Navigation and Information Services, initiated by European Maritime Safety Agency (EMSA) on The European Parliament and the Council of the European Union, Directive 2002/59/EC.

platform integrating various maritime stakeholders of European member states[29] for maritime safety, improving port services, maritime security and environmental protection (EC Project MarNIS, 2007). In MarNIS the data of ship movements is provided automatically by Automatic Identification System (AIS) transponders through shore-based networks, and will be supplemented by data from Long Range Identification and Tracking (LRIT) ("MarNIS Concept"). The project is likely to be operational between 2012 and 2020 (MarNIS Information Centre, n.d.). From the maritime security point of view, the project will be a boon[30] since the most important requirement of security is a reliable databank of information on ships so that the security agencies can monitor and carry out analysis of the voyage of ships, a facility which is presently not available.

As per the survey results, the ships data from AIS, ship reporting system & Ship entering/leaving ports are not being effectively shared with the security agencies for analysis in most of the countries (Figure 9). Non availability of ships data for analysis is detrimental to maritime security and needs to be addressed between the maritime administration and the law enforcement agencies of the country.

[29] Namely, the National Authorities, Port Authorities, Vessel Traffic System, Vessel Owners, Captains, nautical services providers, etc.
[30] Advantage

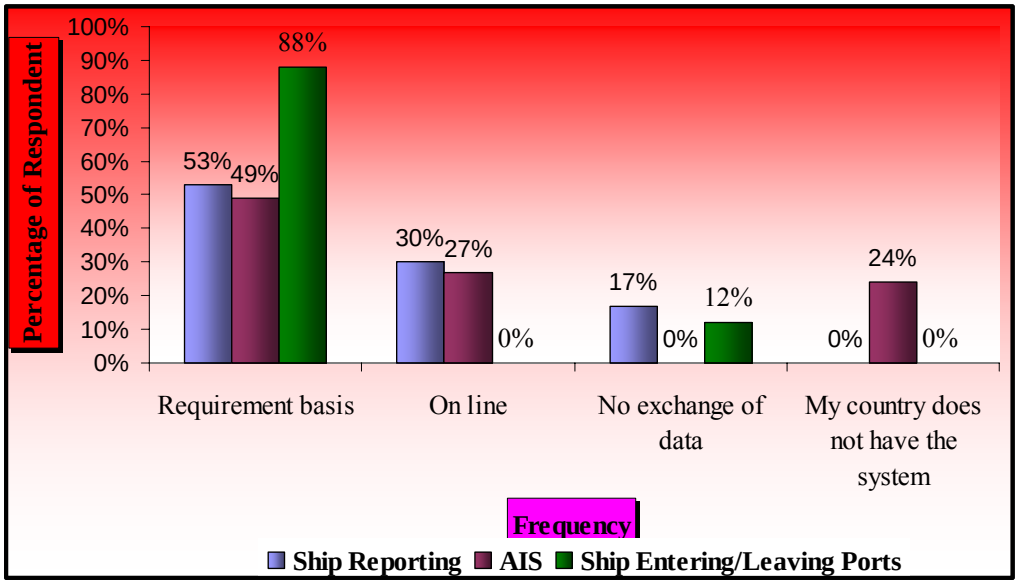


Figure 9: Sharing of data with Maritime Law Enforcement agency.
Source: Data compiled by author from the responses received from the questionnaire survey.

Furthermore, a series of other measures were also adopted to accelerate implementation of the WCO Framework, including the Authorized Economic Operator (AEO) program[31] as well as various initiatives that were taken by the World Trade Organization (WTO) to better facilitate World Trade (Peleg-Gillai et al., 2006, p. 7).

3.2.3 South Asian Regional Port Security Cooperation (SARPSCO)

SARPSCO comprising nine nations[32] of South Asia was initiated with the objective of combating maritime crime, especially piracy and terrorism("New Port Security for Asia", 2008, July).

[31] A strategy aimed at securing international commerce against terrorism while allowing trade to move faster and more reliably
[32] Namely Bangladesh, Comoros, India, Madagascar, Maldives, Mauritius, Oman, Pakistan and Sri Lanka

3.2.4 Asia Pacific Economic Cooperation (APEC)

APEC was started in 1989 and presently has 21 members[33]. It focuses on trade and investment liberalization, business facilitation and economic and technical cooperation between the members. At the Los Cabos, Mexico meeting in 2002, it adopted a counter-terrorism mechanism to secure Trade (Asia Pacific Economic Cooperation, 2002). Further, at its 2003 meeting in Bangkok, members took a pledge for initiating actions to dismantle terrorist organizations, eradicating the threat of weapons of mass destruction and confronting other security threats to international trade. Such an initiative by a large number of countries is a step forward for securing people, infrastructure and trade, which will also have positive impact on maritime security (Counter-Terrorism Task Force, 2003, August). Some of the other initiatives that will foster maritime security are the Association of Southeast Asian Nations (ASEAN), the ASEAN Regional Forum (ARF), the council for Security Cooperation in the Asian-Pacific (CSCAP) (Ong-Webb, 2006b) and North American Free Trade Agremment[34](NAFTA).

3.2.5 The Proliferation Security Initiative (PSI)

It is a global initiative for preventing of weapons of mass destruction (WMD), their delivery systems, and related materials being shipped in the world. The initiative is in line with the U.N. Security Council Resolution 1540. Eleven nations[35] participating in the Proliferation Security Initiative issued a statement of interdiction principles on September 4, 2003 ("The Proliferation Security Initiative", 2003; Richardson, 2007). "As of December 2007, 86 nations have formally committed to PSI participation" (Nikitin, 2008, February 4).

---

[33] Australia, Brunei Darussalam, Canada, Chile, People's Republic of China, Hong Kong, China, Indonesia, Japan, the Republic of Korea, Malaysia, Mexico, New Zealand, Papua New Guinea, Peru, Philippines, Russian Federation, Singapore, Chinese Taipei, Thailand, United States of America, and Viet Nam.

[34] Began on January 1, 1994 among the United States, Canada, and Mexico.

[35] Australia, France, Germany, Italy, Japan, the Netherlands, Poland, Portugal, Spain, the United Kingdom, and the United States

3.3 National Developments for enhancing Maritime Security

Maritime security became the focal point of the industry after the terrorist attack on the United States. Therefore, the US happens to be a major contributor in terms of initiatives for enhancing maritime security. Other countries have followed its lead. Some of the leading initiatives taken by the US for maritime security are enumerated in the subsequent paragraphs.

3.3.1 The Container Security Initiative (CSI)

CSI was started in January 2002 as a multinational program for protecting the containerized shipping from being exploited or disrupted by international terrorists. It has four core elements:

- Identifying high-risk containers.
- Pre-screening and evaluating containers before they are shipped.
- Using technology to pre-screen high-risk containers for rapid screening to prevent slowing down of trade.
- Using smarter containers[36] for easy identification if tampered in transit[37] (Brew, 2003).

CSI has been implemented at 44 ports in Europe, Asia, Africa, the Middle East and North, Central and South America till August 2006 (U.S. Customs and Border Protection, 2006a).

The WCO, the European Union and the G8 countries are supporting CSI expansion and have adopted resolutions to introduce and implement security measures and non-intrusive inspection standards similar to CSI at ports throughout the world (Bonner, 2003; U.S. Customs and Border Protection, 2006a).

---

[36] Equipping a container with a heavy-duty seal and installing an electronic container security device.
[37] After containers are security cleared in a foreign port, they will be sealed with tamper-proof seals with the intention that the containers will not be screened or inspected again on arrival in the US.

As recommended in the 9/11 Commission Act, 100 % scanning of U.S. bound containers is required by 2012. According to Albert Saphir[38] "One hundred percent scanning is far from being a reality…I do not believe it ever was or will be realistic" (US Government Accountability Office, 2008, June 17).

Further to complement the CSI, US Customs requires 24 hours in advance, through electronic transmission, detailed manifest information of a container's contents prior to loading (the '24-hour rule').

The author is of the view that present available technology presently cannot cope with the pace of container trade. Therefore, 100% scanning may not be feasible. However, the objective of introducing container scanning has shown positive results in different countries as it has lead to seizure of illegal items (Anthony, 2005). Narcotics Control Bureau (NCB), India seized about 200 kg of cocaine hidden inside a container at the Jawaharlal Nehru Port. According to NCB officials "16 `suspect containers,' which were scanned through X-ray machines, lead to the seizure of cocaine in one of them" ("Rs 500-cr cocaine seizure at JNPT ", 2004, June 5)[39].

In the opinion of the author, CSI is a positive initiative to ensure checks on the items being shipped through the containers. The volume of goods being shipped through containers has been growing at a fast pace and due to commercial pressures the requirement of scrutinizing the contents of the containers is being shadowed. The initiatives will bear fruits in the long run, which time will testify in the years to come. According to survey respondents, the best solution for scanning is through random scanning (Figure 10).

[38] President of international trade consultants ABS Consulting.
[39] Indian Rupee 500- corer ≈ 1.2 billion USD.

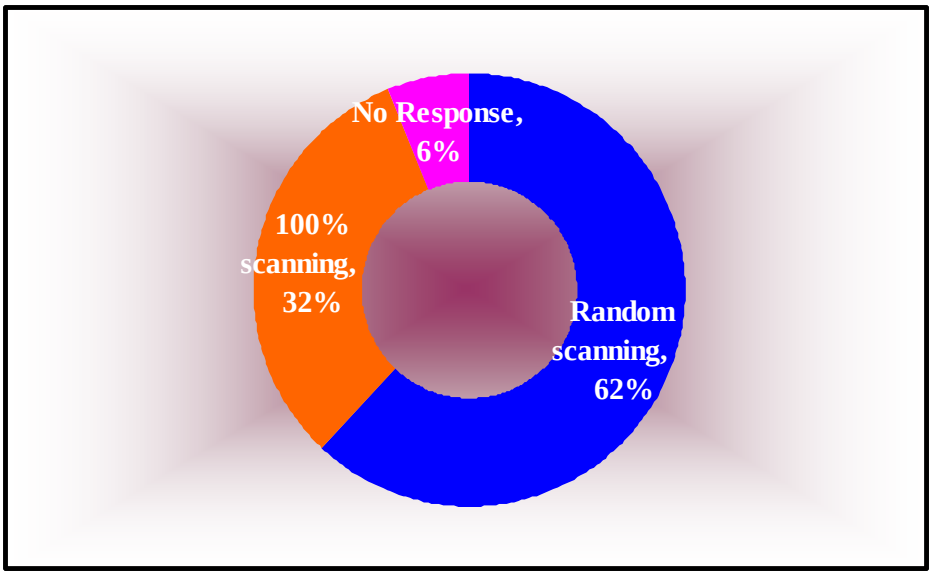


Figure10: Best option of container scanning for enhancing maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

3.3.2 The Customs-Trade Partnership against Terrorism (C-TPAT)

C-TPAT was launched in November 2001 with an objective to framing guiding principles for voluntary participation and developing security criteria, best practices and implementation procedures with other countries. Countries participating are required to set up mutually agreed security measures and Customs and Border Protection (CBP) "reduced inspections at the port of arrival, expedited processing at the border, and other significant benefits, such as 'front of line' inspections and penalty mitigation (U.S. Customs and Border Protection, 2006b, p iii). Survey results indicate that "More than half (56.8%) of the members indicated that C-TPAT benefits either outweighed the costs or were about the same" (Blumenthal, 2008; International Maritime Organization Legal Committee, 2007).

The applicability of CSI, C-TPAT and ISPS frameworks to the container logistic chain is illustrated in Figure 11.

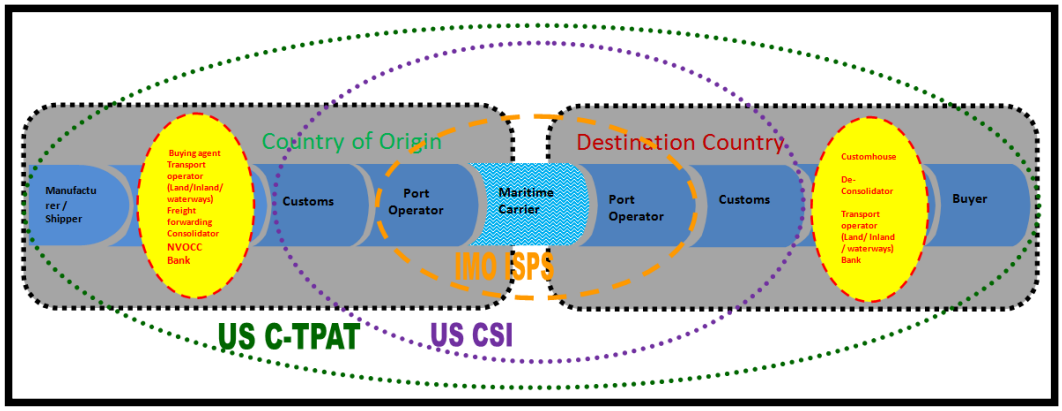


Figure11: Scope of Security Measures in the Container Logistics Chain.
Source: Port and Supply Chain Security 25th IAPH World Ports Conference, Houston2007, page 2.

3.3.3 The Advanced Manifest Rule (AMR)

The Advanced Manifest Rule (AMR) / Advance Cargo Information (ACI) is instituted by US-CBP for complementing CSI initiatives. AMR/ACI requires full cargo data for all modes of transportation to be submitted to US-CBP prior to its arrival. A container will be allowed into the US ports only if these details have been received by the Customs at least 24 hours prior to loading of container from a foreign port of origin. The information assists selecting containers for pre-screening / pre-inspection at ports of departure.

3.3.4 The Smart and Secure Trade-lanes (SST) program

It was initiated by the container shipping industry in October 2002 for ensuring the security of cargo carried in containers globally. Its objective was to develop infrastructure for providing real-time visibility, physical security through non-intrusive measures, automated inspection and detection alerts throughout the complete logistic chain, starting from origin till its final destination (Hudson, 2006).

3.4 Factors influencing Effective Implementation of Legal and Technological measures for fostering Maritime Security

Having seen the measures taken by the various agencies at different levels to enhance maritime security, success can only be achieved if these measures are implemented

in the true spirit. Other factors such as security assessment of port facilities and ships, implementation of security instruments, training and man-machine interface also play critical role in achieving maritime security are discussed in succeeding following paragraphs.

3.4.1 Security Assessment of Port Facilitates

A port facility is generally connected to road, rail and inland waterways networks. The cargo received is either in packaged form, in containers, or loose. The task is to ensure that the items that are being transported are not illegal. Passengers, workers, transporters gain access to port facilities when utilizing the services, when working and when transporting cargo respectively. While entering and leaving, they need to be screened for any illegal items and their credentials need to be checked to prevent unauthorized entry. Moreover, a vigil needs to be maintained in the port area to detect any intrusion by an unauthorized person, who may cause sabotage or engage in any other illegal act that may imperil maritime security.

The ISPS Code enumerates various measures that need to be taken to enhance maritime security. The survey results show that the technology that needs to be adopted at port facilities under the instruments is adequate (Figure 12).

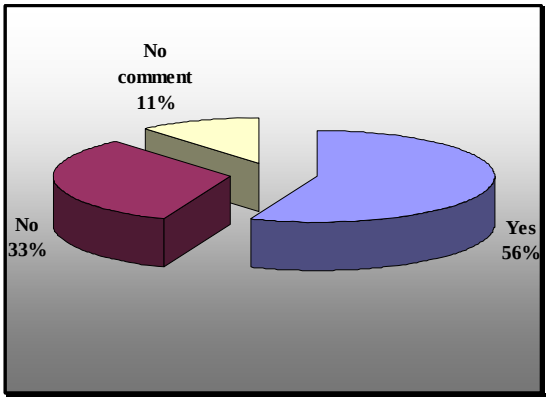


Figure12: Adequacy of technology for port security.
Source: Data compiled by author from the responses received from the questionnaire survey.

3.4.2 Security Assessment of Ships

Security threats to or from ships vary with location namely when in port, at anchorage and at sea. For ships in port, security cover from all types of threats, especially underwater attacks, is to be provided by the port authorities. Ships should complement the efforts of the port by taking measures which are within their scope and capability. For example, checking personal credentials of individuals prior allowing them access to the ship, maintaining a waterside lookout for approaching ships or boats. When the ship is at anchorage, the responsibility for maritime security will be more on the ship than on the port. The ship has to maintain vigil all around for boats. However, underwater protection needs to be provided by the port. At anchorage, the possibility of intruders embarking ships with the help of a boat or an underwater diver trying to sabotage will be easy as compared to when in port. When the ship is at sea then the sole responsibility for detecting a maritime security incident will rest with ship. While the ship is underway, the possibility of an underwater attack will be very low. There has been no incident or intelligence reported of any pirate or terrorist group having the capability of underwater targeting a moving ship. Underwater attacks on moving targets can be made by a torpedo[40] or sub-launched missiles[41] or by laying mines in the area. Only naval forces bear the capability required for launching an underwater attack on a moving ship, which is exercised in the event of war. This is being beyond the scope of the dissertation so it is not discussed any further. While the ship is moving, there is a high possibility of attack or, an intruder attempting to embark with the help of another ship or boat.

It needs to be emphasized here that technology is available for alerting or analyzing any situation that is likely to develop, or which may result in breach of maritime security. The possibility of an early detection will depend on the operator's

[40] It is a self-propelled explosive projectile weapon, launched above or below the water surface, propelled underwater toward a target, and designed to detonate on contact or in proximity to a target.
[41] Missile launched by a submarine underwater.

professional capability and his attentiveness in monitoring the emergent developments. Further, it will also depend on how reliable the technology is and the level of man-machine interface, i.e. how ergonomically[42] the equipment has been designed. The respondents of the survey are of the opinion that adequate technology exists on board to identify development of a situation which may compromise security of the ship (Figure 13).

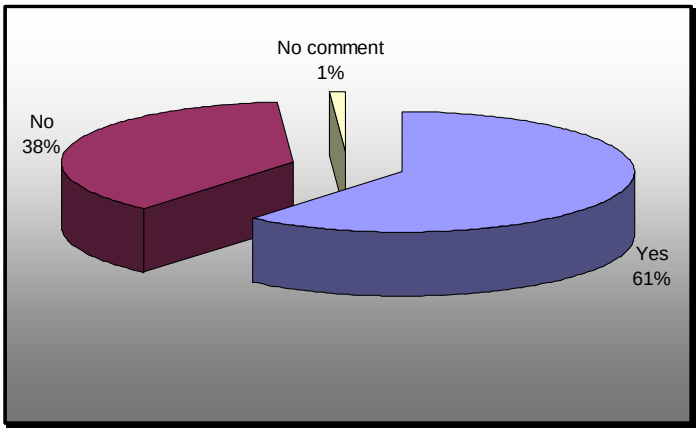


Figure13: Adequacy of technology for ship security.
Source: Data compiled by author from the responses received from the questionnaire survey.

3.4.3 Effective Implementation of Maritime security measures

IMO instruments that come into force are required to be incorporated by the member states in their national law for enforcement. The degree of enforcement varies from country to country. On adoption of an instrument, some countries incorporate it effectively on a priority basis while others may not implement it as effectively. The reasons could vary - from economic constraints to professional competency. Once an instrument gets incorporated in the national legal system, it needs to be implemented on ground i.e. in the maritime sector. The ISPS Code requires measures to be initiated by the contracting government, the companies and the ship. For ships, it is

[42] Ergonomics is the scientific discipline concerned with designing according to the human needs, and the profession that applies theory, principles, data and methods to design in order to optimize human well-being and overall system performance. The field is also called human engineering, and human factors engineering.

feasible to check the state of preparedness through port state control. However, no mechanism exists to ensure that measures adopted by the member state are adequate and will meet the objectives of the code. It is pertinent to mention that, to meet the objective of the code, the European Union has promulgated directives for conducting commission inspections for maritime security (European Union, 2005, June 10). This initiative will bring about standardization in measures adopted for maritime security among its member states. Further, the initiative of the IMO in introducing Voluntary IMO Member State Audit Scheme is the way forward in bringing standardization in the world and will foster maritime security ("Audit Scheme under way", 2007, February). The author is of the firm opinion that it is the 'will' and cooperation of the member states that can make shipping secure. The Port State Control drive by IMO member states for elimination of unsafe ships has produced substantial results. Thus, the need of the hour is to initiate a similar cooperation drive to eliminate ships indulging in illegal activities and jeopardizing maritime security.

It needs to be noted that in most countries across the world, the maritime administration is the maritime law enforcement agency in port while that at sea is another agency. Moreover, both are administered by different ministries. Thus, adequate interaction between the two agencies is important for effective implementation of maritime security. However, in practice, it does not so happen. The survey results also indicate that a law enforcement agency is different entity in their countries (Figure 14) and there is inadequate interaction between maritime administration and law enforcement agencies in their flag state (Figure 15), which needs to be addressed by the member states.

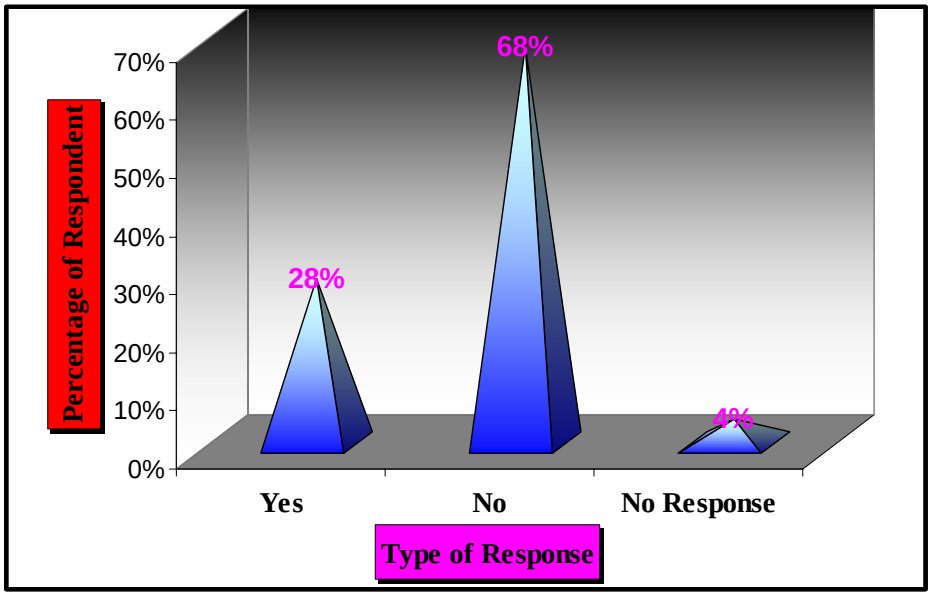


Figure14: Law enforcement agency at Port is same as that at Sea.
Source: Data compiled by author from the responses received from the questionnaire survey.

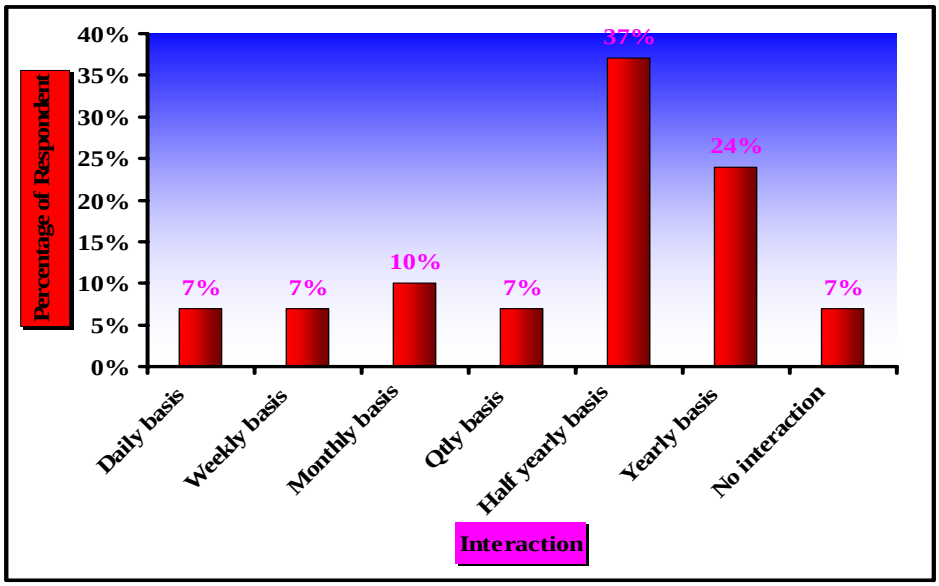


Figure15: Frequency of interaction between Maritime Administration and Law Enforcement Agency.
Source: Data compiled by author from the responses received from the questionnaire survey.

3.4.4 Importance of Training for Effective Utilization of Technology

It is evident that technology has ushered a revolution in day to day working in different fields all around the world. Technology not only has the capability to accomplish a task with precision, but to handle voluminous work which is beyond

human capability. In spite of the advantages and capability of technology, its effectiveness is dependent on the man behind the machine. The ultimate success and actual performance of a security system also depends on the people who operate this equipment. Therefore, it is vital that personnel manning the equipment are well trained (Ashmawy, 2005). The IMO has developed model courses for Ship/Port/Company Security Officer, in 2003. Personnel likely to be entrusted with the responsibility of SSO/PSO/CSO are required to undergo these courses (Anstey, 2005). However, Standards of Training, Certification and Watchkeeping for Seafarers (STCW) do not specify any competence standard for the training on maritime security for officers responsible for carrying out navigational watches at sea. They are the people who will encounter maritime security situations during their watches. The author is of the opinion that simulation training encompassing different situation that may be encountered at sea can be developed and the seafarers can be trained so that in real time, these situations can be handled more efficiently by them. Amendments endorsed by MSC 83 section for new regulation VI/6 and new section A-VI/ and B-VI/6 need to be implemented on priority.

3.4.5 Adequacy of man- machine interface

With rapidly changing technology it is important that there is adequate man-machine interface, as it is the man behind the machine that makes all the difference. According to Mejia, in a socio- technical subsystem, man-machine system is the major subsystem (Mejia, 2007, p. 27). The ship is a socio- technical system and wherever there is a human interacting with a system, there is a Human Element issue. Today, modern technology has revolutionized ship operations. However, adequate attention has not been paid to the man-machine interface in terms of the design, layout, and integration of systems (Mejia, 2007).

The study of ergonomics[43] is relatively new and sufficient expertise in not available in the industry (Mejia, 2007). It is commonly agreed in the shipping industry that close to 80% of accidents are rooted in human error (Fotland, 2004, April , p. 2; Hadfield, 2004; Schröder, 2006). The importance of man- machine interface is evident from the IMO safety standard setting regulations that basically address ship designs and the equipment fitted onboard. However, despite the best technological innovations, marine casualties and incidents continued to occur, provoking think tanks in the marine fraternity to broaden their horizon on maritime safety and consequently find human involvement in all aspects of marine endeavour, such as ship design, manufacturing, management, operations and maintenance (International Maritime Organisation, 2000).

Automation has qualitative consequences for human work and safety and does not simply replace human work with machine work. It changes the task it was meant to support. It creates new error pathways, shifts the consequence of error further into the future and may delay opportunities for error detection and recovery. It creates new kinds of knowledge demands (Blöchl, 2007) and tools for identifying human error that may result in compromising maritime security are still not known to the industry (Schröder, 2005).

Numerous studies are being carried out on the man-machine interface for improving safety at sea. Such studies need to be carried out for maritime security also. According to the UK P&I Club, human error costs the maritime industry $541m a year (Er & Celik, 2005; UK P & I Club, 2003, October, p. 3), for matters related to safety. However, its cost with respect to maritime security is yet to be known to the industry. The rapid growth of the industry in recent years, due to growing demand by

[43] The IMO definition of ergonomics is the study and design of working environments (e.g., workstation, cockpit, ship bridges) and their components, work practices, and work procedures for the benefit of the worker's productivity, health, comfort, and safety.

fast moving economies coupled with the rapid spread of international terrorism has lead to adoption of new legislative instruments in the industry, causing more workload on the people working in the industry. The situation becomes more complicated due to present maritime employment trends which concentrate on low crew costs, thus causing fatigue and frustration (Editor, 2004, July, p. 1). Further, marine accident reports are indicative that fatigue is the primary cause in most of the accidents, which in turn is caused by overwork or stress. Improper man-machine interface also leads to fatigue (Chakrabarti).

According to Anstey, fatigue impairs performance and diminished alertness irrespective of individual skills, knowledge or training, resulting in low assimilation of a situation which not only affects the ability to appreciate a developing maritime security scenario, but also will hamper normal day to day shipboard duties endangering safety of crew and ship (Anstey, 2005). Therefore, the existing regulations on safe manning need to be reviewed, so that there will always be a sufficient number of competent people on board every ship (Bowring, 2006, January, p. 3; "Increased manning could combat piracy", 2007, August; Sheen, 2007, January, p. 3).

The commercial interest of owners and administration focus on increasing the number of ships in their flag for more economic gains have led to a compromise in effective implementation of the IMO guidelines on manning of ships (Herbert-Burns, 2005). It has been observed that similar class of ships with similar trade pattern, registered under different flags have different manning plans (Othman & Halawa, 2005). The growing workload on people in the industry is a great concern for maritime security (Wheater, 2008, June). The respondent of the survey are also of the views that the present manning of ships is inadequate for the present security scenario (Figure 16).

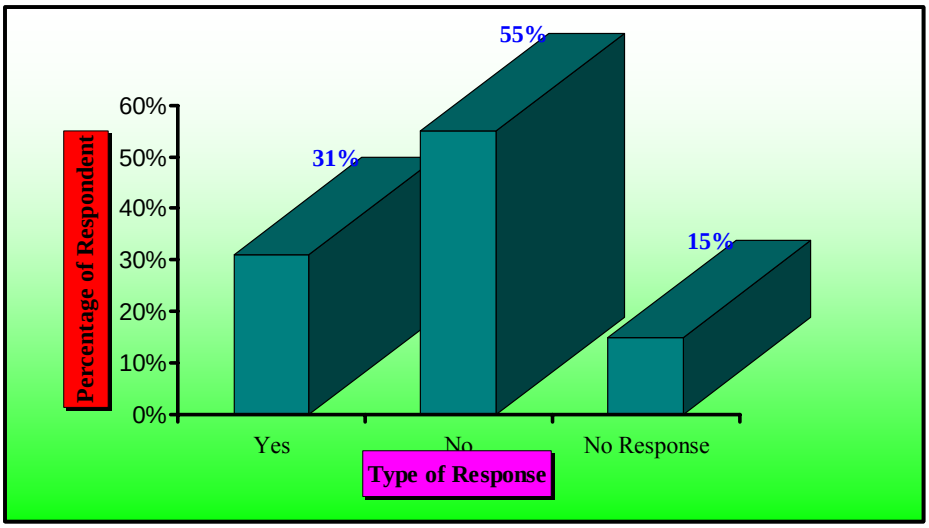


Figure16: Adequacy of present manning of ship.
Source: Data compiled by author from the responses received from the questionnaire survey.

Technology is the only source that can improve the efficiency of humans and make the drive a success (Bonner, 2005). The next chapter will look at how the technology can be optimally exploited for achieving the goal of maritime security.

CHAPTER 4

APPLICATION AND ADEQUACY OF TECHNOLOGY IN FOSTERING MARITIME SECURITY

"Security provides for insurance and liability reduction, offers contingency plans, conducts safety surveys and improves the company's image almost everywhere that it exists. Each of these functions has a substantial impact on profitability that should be noticed"- **Jones, R. F. Jr. (1994), Security as a Profit Center: Contributing to the Bottom Line in Security Journal, Vol. 5, No. 2.**

Effective and optimal utilization of maritime safety technology has enhanced maritime security manifold as seen in the case of the straits of Malacca and Singapore. Since it is an important shipping route linking the Indian Ocean to the South China Sea and the Pacific Ocean, a marine electronic highway (MEH) has been setup at the straits. The system utilizes the integrated data from ARPA, AIS, DGPS and ECDIS. The system has not only enhanced safety of ships transiting through the strait, but has also curbed the illegal acts of piracy due to its effective tracking and identification system (Boutilier, 2005).

In this chapter the main focus will be on the application of technology and its adequacy in meeting the requirements of maritime security. In order to carry out critical analysis the equipments is grouped into four categories as follows:

- Equipment inducted primarily for maritime security,
- Equipment adopted for purposes of safety, yet some features if optimally exploited can reinforce objectives of maritime security,
- Equipment adopted to meet local security requirements, and
- Equipment fitted in Systems setup for Safety of Navigation.

Further, the chapter will also look into technologies that are being used in other fields but may be utilized in the maritime sector for enhancing security. These technologies

will be discussed under the title future threat based technology for fostering maritime security.

4.1 Mandatory Equipment for Maritime Security

Ship Security Alert System

The purpose of a ship security system is to transmit a ship-to-shore security alert to a competent authority designated by the Administration. The alert will contain ship's identification, its position with a time tag[44]. The alert will indicate that the security of the ship is under threat or it has been compromised. This security alert will not be sent to any other ship and the transmission of the alert will not be known to the personnel onboard the ship. The alert once activated will keep transmitting until it is deactivated and/or reset. Moreover, it should be activated from the navigational bridge and from at least one more location[45] (Safety of life at Sea, 1974). The equipment utilizes the satellite system (Inmarsat or COSPAS[46]-SARSAT[47]) which is reliable and will deliver the alert subject to the equipment being functional. The respondents of the survey are of the view that SSAS will enhance maritime security (Figure 17).

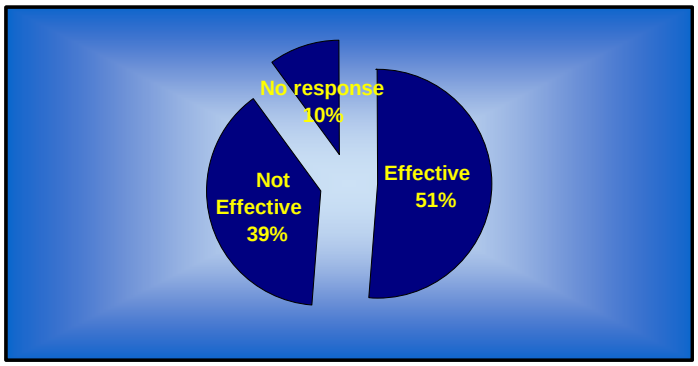


Figure17: Role of SSAS in promoting maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

[44] Date and time of the position.
[45] Chapter XI-2, Regulation 6 (2&3).
[46] Space System for the Search of Vessels in Distress.
[47] Search and Rescue Satellite-Aided Tracking.

While carrying out research it was analyzed that in the Global Maritime Distress and Safety System (GMDSS) adopted by IMO for Search and Rescue has similar provisions for sending a predermined alert (Distress Button) in case of distress at sea (Figure 18). Details sent in the predetermined distress alert are:

- Name of the vessel in distress
- MMSI[48]
- And its position with the time tag when the distress alert was sent.

The requirement of alerting in case of breach in maritime security could also have been achieved by providing an additional security alert button adjacent to the distress button in INMARSAT C terminal, with a predetermined security alert which could be clearly distinguished by the operator.

Figure18: Sailor Inmarsat 'C' Terminal.
Source: Retrieved on July 01, 2008 from the World Wide Web:
http://www.selexmarine.com/products/sailor/pdf/Sailor_H2095C.pdf

The author is of the view that in case of distress at sea, it is the life of the crew member and the ship that is jeopardized; however, in case of a terrorist attack on a

[48] It is 9-digit code. For ships first three digits indicate the country in which it is registered followed by the ship station identity.

ship, it may not only involve the ship and its crew but it may also jeopardize other people's life and property. Thus, the consequences of breach of maritime security can be graver compared to that of maritime safety. Under the GMDSS, IMO has adopted that ships should be able to transmit a ship-to-shore distress alert by at least two separate and independent means and each using different radio communication services. On the contrary, it is noted that there is no duplication of the SSAS equipment for sending a security alert; if SSAS malfunctions, the alert cannot be sent.

SSAS will meet the objective for which it has been adopted i.e. alert the concerned authority. However, how effective will the response be when a ship on the other side of the globe sends a security alert to the flag state in comparison to its being sent to the coastal state who is closer and in a position to provide immediate assistance but unfortunately not a recipient of the information at the very instance of the attack. The channel of communication will definitely delay the response. The Global Integrated Shipping Information System (GISIS)[49] on the IMO Webpage is the database where the contact details of the authority to be approached in case of maritime security assistance are listed. The latency of the data is a question in itself. Further, the GMDSS concept of alerting ships in the vicinity in addition to the authorities ashore (Brehaut, 2002), would have been more effective for maritime security. An additional security alert button can be provided for this purpose in the VHF Digital Selective Calling (DSC) equipment (Figure 19).

[49] http://gisis.imo.org/Public/

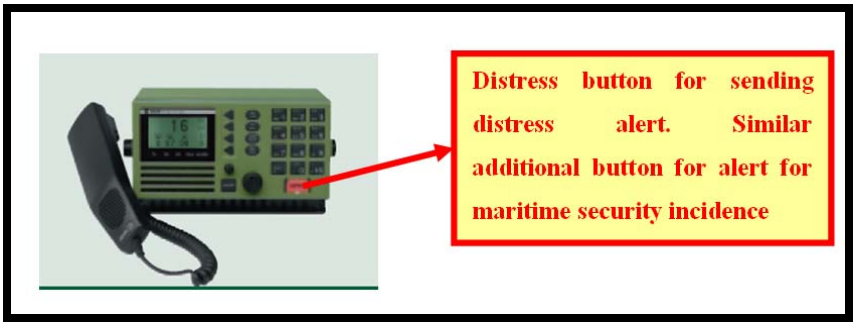


Figure19: Sailor VHF GMDSS equipment.
Source: Retrieved on July 01, 2008 from the World Wide Web:
http://www.selexmarine.com/products/sailor/pdf/Sailor_System_4000_GMDSS.pdf

Stewart in his report refers the requirement of IMO, which advices the captain to send alert in the event of an attack through SSAS rather than using the traditional radio mayday calls. This alert passes through at least three authorities in different parts of the world before action could be taken. He expresses concerns over the purpose of a ship security alert being sent only to a ship owner or Flag State who are thousands of miles away from the scene of the potential security threat, leaving everyone nearby completely unaware of the potential danger. Moreover, large numbers of ships are registered with Panama, Liberia and Bahamas. These countries are poorly equipped and may not be able to pass emergency information about a possible terrorist incident in time. With the traditional method of alerting, early response is feasible, which may deter terrorists from achieving their objective. He refers to the study carried out by Singapore's Rajaratnam School of International Studies that found "the system bordered on farcical and was utterly ineffective in stopping the use of merchant ships for acts of terrorism"(Stewart, 2008, June 23).

Michael Perry too is also of the view that "a ship mayday distress alert, which is globally monitored by maritime authorities, would generate a more rapid response to a terrorist attack". He further said "For ships positioned near highly populated areas, critical infrastructures or alongside large passenger ships, expediency is of the utmost importance if there is to be any hope of saving lives" (Perry, June 25, 2008).

In case a distress alert is transmitted on a radio frequency, shore authorities as well as ships in the area receive the alert. In case of a satellite transmission, alert goes only to the shore authority, who in turn broadcast the alert to ships in the area by radio or by Enhance Group Call[50] of Inmarsat (Brehaut, 2002, p. 121). These procedures can also be applied to security alerts. Assistance can be provided to the victim ship by ships in the area till the security forces come to the scene for carrying out the assault operation to apprehend the culprits. The advantages are twofold:

(a) The ships in the area will be alerted so that incident could be prevented on board their ships, and
(b) Ships in the area can shadow[51] the criminal so that they do not escape easily after the crime.

As per IMO performance standards for GMDSS, there shall be the provision for transmitting distress alert by pressing buttons for 5 seconds (IMO, November 23, 1995). The equipment automatically transmits a predetermine message containing the following information:

- Name of the vessel in distress
- Call sign
- MMSI[52] no

Distress button provision is there in both radio and satellite GMDSS equipment as shown in Figure 18 & 19. Similar buttons could have been provided for security alert. Such an arrangement would have met the requirement and also proved to be economical.

[50] EGC is used for transmitting Maritime Safety Information utilizing INMARSAT Satellites.
[51] Secretly follow.
[52] It is 9-digit code. For ships first three digits indicate the country in which it is registered followed by the ship station identity.

4.2 Technology adopted for navigational safety (Chapter V, SOLAS)

4.2.1 Automatic Radar Plotting Aid (ARPA)

ARPA[53] was introduced in the maritime sector in the year 1969, for 'Automatic Target Tracking' (ATT). All ships of 500 gross tonnage and upward are required to have, at least one radar fitted (Safety of Life at Sea (1974), p. 373). The radar transmits an electronic magnetic energy wave and it receives a fraction of this energy after reflection from the target in the direction of the transmitting antenna. The maximum distance a radar can detect a target will depend on the transmitting frequency, height of antenna, energy transmitted and the energy reflected by the target. The strength of reflected energy will depend on the material, size and angle of reflecting surface of the target. For example, a steel hull ship can be detected by radar at a very far distance; however, a rubber boat may not be detected even at close ranges (Bole, Dineley, & Wall, 2005, pp. 146-150).

ARPA has the facility for auto acquiring and tracking of targets within the range set by the operator. The operator can define the range around his ship, and it is called the guard ring[54] (Figure 20). If any ship likely to pass less than the set range, the operator will be alerted automatically by means of an audio-visual alarm generated by the system (Burch, 1999, p. 37). After identifying ships which may be a potential threat to security, he can communicate by other means with such ships and ascertain whether it is a friendly or a rogue ship.

[53] First ARPA was fitted on board cargo liner MV Taimyr in 1969.
[54] User defined range rings that can be used to set alarms to signal whenever a target enters the sector defined.

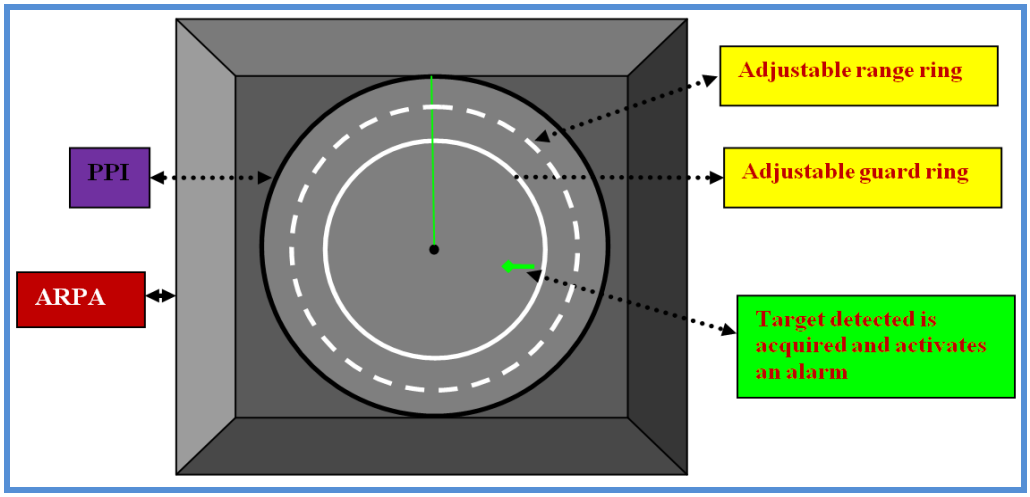


Figure20: ARPA ring guard.
Source: Radar and ARPA Manual (2005) 2nd edition by Alan Bole, Bill Dineley& Alan Wall, page 240

Some of the limitations of ARPA in detecting all targets, and hence its impediment to enhancing maritime security, are as follows:

- The performance of radar is severely affected in heavy rain and rough sea condition,
- When two acquired target pass close to each other, target swapping is very common. In ARPA this problem has been resolved to some extent as it continues tracking for some time, even if there is no response for some time (Bole et al., 2005, p. 224).
- Due to the position of radar antenna vis-a-vis the superstructure, the radar will not be able to acquire any contact in the sector obstructed by the superstructure. This sector will be the blind zone for the radar. Any target in this area or approaching from this sector will not be detected. Moreover, the radar will pickup targets that are in line of sight of the radar antenna and thus, targets behind a bend or behind any obstruction will not be detected.
- Since the radar detection depends on the reflected energy of the target, auto acquiring for rubber boats targets may not be effective.
- The radar may not be able to detect small boats or rafts.

Some of the above limitations can be overcome by effective design and correct location of the antenna. Detection of targets in bends and behind obstruction and target swapping can be supplemented by AIS. Further, detection of AIS targets are not affected by/in heavy rain and rough sea conditions. The problem of detecting small contacts and targets approaching through these sectors can be complemented by fitment of infrared cameras (Figure 21).

Figure21: Infrared cameras Nightnav Nv5000 Series Multiple Sensor Imaging Systems.
Source: Night Vision technology, Inc retrieved on July 17, 2008 from the World Wide Web: http://www.nightvisiontechnologies.com/images/5000SellSheeWT_11-07_1181678655_5927.pdf

Infrared cameras if fitted in such a position onboard as to have full all-around coverage, including in close proximity of the ship from where the likelihood of intrusion is highest, will facilitate a high degree of maritime security rather than sector coverage and will have advantage in different maritime security scenarios. It will be an effective tool for maintaining surveillance for small and unlit boats while the ship is in port, at anchorage, and when passing through dense traffic during all the hours of the day. Further, an infrared camera being radar and computer compatible, it is possible to track a radar target with it and also do video recording. Video recording will assist the law enforcement agencies to apprehend the culprits and bring them to book.

4.2.2 Automatic Identification System (AIS)

The basic function of AIS is to automatically and continuously transmit and receive a multitude of digital information without human interference (Hecht, Berking,

buttegenbach, Jonas, & Alexander, 2002). The functional requirement of ship borne AIS is to transmit the ship's own data, and receive data of other vessels and VTS stations, and display received data. AIS facilitates automatic calculation of Closest Point of Approach (CPA) and Time to Closest Point of Approach (TCPA) of a vessel transmitting its position information. The system operates on VHF band; therefore, it can monitor ships at a range of 20 to 30 nautical miles depending on antenna height. An operational equipment will automatically and continuously transmit and receive information without human interference (International Maritime Organization, 2002 January 25).

The information transmitted by ships AIS is as follows:

- Fixed or static information, which is entered at the time of initial installation. This is done by the service engineer of the manufacturing company and the operator has no control over the settings once it is programmed;
- Dynamic information is the ships navigational data and are automatically updated from the ship sensors linked to AIS; and
- Voyage related information, which is required to be manually entered by the ship and updated during the voyage.

The content of different types of information and the speed of exchange of information is in Appendix G.

Accuracy and reliability of information transmitted by AIS is vital from a security point of view. Therefore, IMO has laid down the security mechanism for detecting, disabling and preventing unauthorized alteration of input or transmitted data which is incorporated in the equipment (International Maritime Organization, 1998, May 12). Sandler, Gern and Zimmermann (2003, p. 78) are of the view that "AIS transponders offer new possibilities to enhance security and effectiveness of water borne transport". According to Reshetova, Direct Sales Administrator, Transas Limited, static information data which contains the ship identification is set by the service

engineer and is password protected and, therefore, the operator cannot tamper with this information. The operator has full control over the voyage related information which he can meddle with (Personal Communication, July 1, 2008). From the maritime security point of view, the operator will be able to segregate ships on innocent passage from rogue ships, since ships on innocent passage will continuously transmit and the data transmitted will be correct whereas a rogue ship either will switch off its AIS transmission or transmit misleading information to conceal its identity. Therefore, the operator can segregate ships and limit his auto tracking with ARPA to a limited number of ships. He will be able to appreciate security developments much better due to the limited number of ships being monitored. In view of the above, the author is of the opinion that switching off the AIS transmission will only complicate the situation and make it more difficult to identify of rouge ships.

In AIS the rate of updation is directly proportional to the ships speed – the higher the speed of a ship, the faster will be its rate of transmission of updates. For example, in a ship doing 0-14 knots [55] and changing course the data update will be every 4 seconds and if the ship is doing more than 23 knots and changing course then the data is updated every 2 seconds (International Maritime Organization, 2002, January 25) . Fast response is very important for early identification of ships that are not following the normal navigational routes in restricted waters. Therefore, AIS will prove advantageous when course and speed alterations of other ships are recognized, and the detection of small vessels that in radar systems are often unrecognizable in the sea or rain clutter or because of their size if they are displayed only at the last minute (Blöchl, 2007).

[55] It is the nautical unit of speed i.e. the distance travelled by a ship in an hour in sea.

AIS has the facility for identifying dangerous targets. If this facility is activated and the distance that another ship can safely pass (CPA)[56] is set in the equipment, then AIS will automatically calculate, for all the targets acquired, the closest distance that they will pass and the time that they will be at that position (TCPA[57]).

AIS overcomes the shortfalls of ARPA in tracking of targets and is free from problems such as dense traffic, target swap [58], heavy rain and sea clutter. AIS is capable of detecting other ships even if they are behind the bend in a channel or river or an island and detect a change in the heading almost instantaneously (Diestel, 2005; Pettersson, 2003). Survey respondents are of the views that the interfacing of radar with AIS will enhance operator efficiency for early detection of any maritime security incidence (Figure 22).

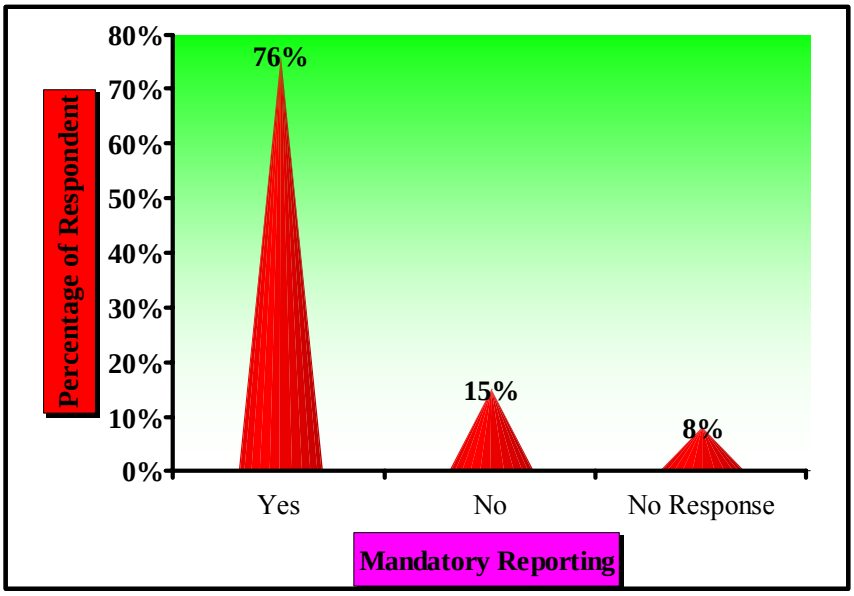


Figure22: Interfacing of Radar with AIS will enhance probability of detection of maritime security incident.
Source: Data compiled by author from the responses received from the questionnaire survey.

[56] Closest Point of Approach.
[57] Time to Closest Point of Approach.
[58] Target Swapping takes place when two targets respond within the tracking gate at the same time.

If any target is likely to pass at a distance less than that set by the operator, AIS will automatically alert the operator by giving an audio- visual alarm and the operator can assess the intention of the vessel and take necessary action. AIS gets a feed from various other sensors. If these sensors are malfunctioning, genuinely or intentionally, then AIS will transmit false information which can deceive the operator. Therefore, an operator with experience will be able to better appreciate the situation and utilize the equipment accordingly (International Maritime Organization, 2002, January 25).

Some countries have established shore based AIS network and others are in the process of doing so. Through this network a maritime security agency can analyze the pattern of shipping and track down ships that may be a potential threat (Junzhong, 2005, p. 28). The AIS was primarily inducted in the maritime industry for enhancing maritime safety, however, after 9/11 it was seen as an indispensable tool for enhancing maritime security as seen from IMO resolution A.917(22). "Target identification has always been a fundamental function of AIS equipment for security and vessel-management purposes" ("AIS - help or hindrance?" 2008, p. 5). However, the major security concerns comprise sharing of information among various stakeholders and the customers. Some AIS information providers are distributing the information through Internet, which is not a very secure means. Hacking of computers[59] and carrying out illegal money transaction has been witnessed in the past. Utilization of such expertise by terrorists for gaining access to the AIS on internet for planning an attack cannot be ruled out in future. IMO too had expressed its concerns over AIS information distribution through the internet (International Maritime Organisation, 2004, December). Survey results show that 62% are of the opinion that AIS fosters maritime security (Figure 23).

[59] It is the process by which individuals gain unauthorized access to computer systems for the purpose of stealing and corrupting data.

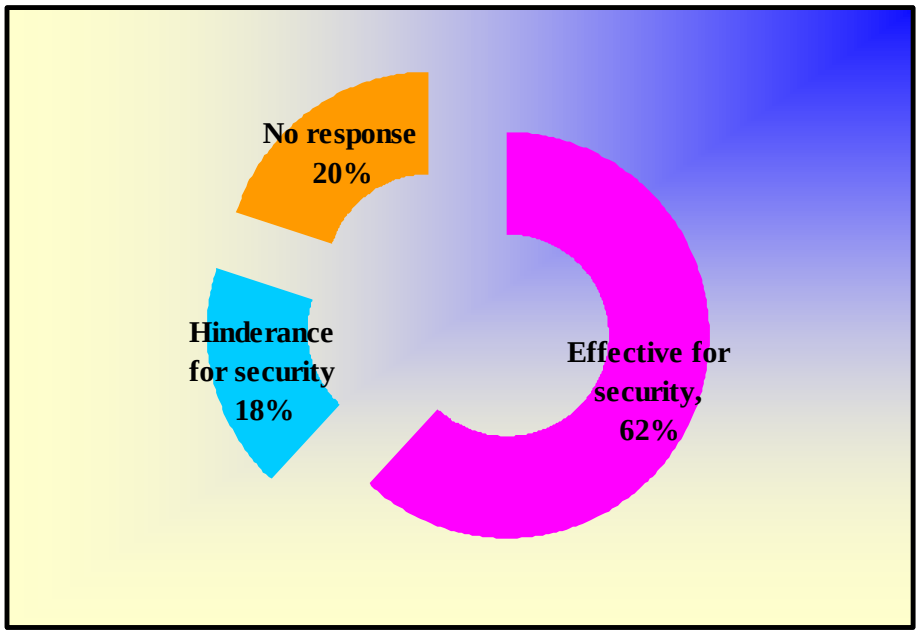


Figure23: AIS fosters maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

4.2.3 Integrated Bridge system or Integrated Navigation Systems

Present day technology has made it possible to interface Radar/ARPA, Electronic Chart System/Electronic Chart Display and Information System (ECS/ECDIS), and AIS. The vital advantage of this interface from a maritime security point of view is that if the target is found suspicious then the OOW or ship's captain can promptly initiate evasive action to prevent breach of security, keeping the ship in safe waters as all the information is available to him at a place with the help of the Integrated Bridge System. Further, the greatest advantage of integration is that all the information is available to the operator together and, in a situation where one of the systems has technological limitations another fills in, leaving no gaps in the information. For example, if a ship being tracked passes close to another ship while ARPA information may be incorrect due to target swapping, AIS will not be affected and, therefore, during that period the operator continues to get reliable information. According to Efthikios Mitropoulos, Secretary General, IMO "Not only do these technologies hold the promise of reducing navigational errors and accidents, they

also have the potential to deliver benefits in other ways. Search and Rescue, responding to pollution incidents, ship and port security….." (Mitropoulos, 2007, March, p. 7).

During the course of interviews with ship masters' it was brought out that they were required to maintain a large folio of paper charts onboard, which are required to be corrected regularly for Notices to Mariners. It is a herculean task because of the large number of folios being maintained. Due to shortage of time in ports, the chart correction is generally being carried out at sea while carrying out sea watches. Thus, the OOW will not be able to appreciate any developing maritime security incident as he is fully engrossed in the chart corrections (personnel Interviews with ship captains, 2008 July- August). Several studies have revealed that it takes between several hours to two and a half man day efforts to carry out chart correction on paper charts, leading to undue fatigue. With ECDIS, irrespective of the number of charts that the ship may hold, the entire process of updating takes just a few minutes producing the highest standards of updating, week after week (United Kingdom Hydrographic Office, 2008). Therefore, introduction of ECDIS will facilitate maintenance of better vigil by the OOW during his watch, enhancing both safety and security (Patraiko, 2007, March).

4.2.4 Long-range identification and tracking (LRIT)

LRIT was one of the outcomes of the Diplomatic Conference in the wake of 9/11 for enhancing maritime security. LRIT has been introduced as an amendment to SOLAS Chapter V regulation 19-1, and was adopted on 19 May 2006 by Resolution MSC.202 (81) and came into force from 01 January 2008. LRIT equipment is fitted on the following types of ships engaged on international voyages[60]:

- Passenger ships, including high-speed passenger craft;

[60] SOLAS 74 Regulation 19-1, section 2.1.

- Cargo ships, including high-speed craft, of 300 gross tonnage and upwards; and
- Mobile offshore drilling units.

LRIT equipment will automatically transmit every 6 hours or on receipt of polling command [61], the required information without the interference of the operator. The information that will be transmitted is the ship's identity, its position in latitude and longitude with date and time of the position. The regulation facilitates the provision of switching off the equipment in the shortest duration possible on the professional judgment of the master for protecting of ships navigational information if the situation warrants or there is likelihood of compromise on safety or security of the ship in the area. On doing so, he is required to inform the flag state and make an appropriate entry (Safety of Life at Sea (1974)).

The member states will be able to receive long-range identification and tracking information for their flag ships, ships that intend to use their port facility and ships transiting at a distance up to 1,000 nautical miles from its coast subjected to if the ship transiting is not in the territorial waters of the member state, whose flag the ship is flying. The regulation emphasizes the need to protect long-range identification and tracking information for commercial confidentiality and sensitivity and prevent unauthorized access (Tsamenyi & Palam, 2007). The broad difference between AIS and LRIT is on the range, AIS is for short range as it uses Very High Frequency and LRIT is long range and therefore uses satellite channels; second AIS is a broadcast system, where anyone with the equipment can receive, whereas LRIT information is on 'need to know basis', and lastly information transmitted for LRIT is ship's identity position with a time tag, whereas in AIS in addition to this, more information

[61] Polling is sequential interrogation of devices and is done for various purposes, such as, determining operational status or determining the readiness of the device to send or receive data or initiating device to transmit a pre defined data.

is transmitted. LRIT will assist in tracing ships which indulge in illegal trade and other illegal activities.

According to Martin Tsamenyi (2007, pp. 43-46) some of the member states and other stakeholders have expressed concerns that tracking ships all around the globe will compromise and be detrimental to maritime security. However, he is of the view that timely implementation of the LRIT system will complement the ISPS objectives and essentially ensure maritime safety and security. Identification and tracking rogue ships is very vital to ensure maritime security. Further, it is essential that the information regarding such ships needs to be shared for continually tracking until arrival at a port. Dissertation survey results show that 77% are of the opinion that LRIT fosters maritime security (Figure 24).

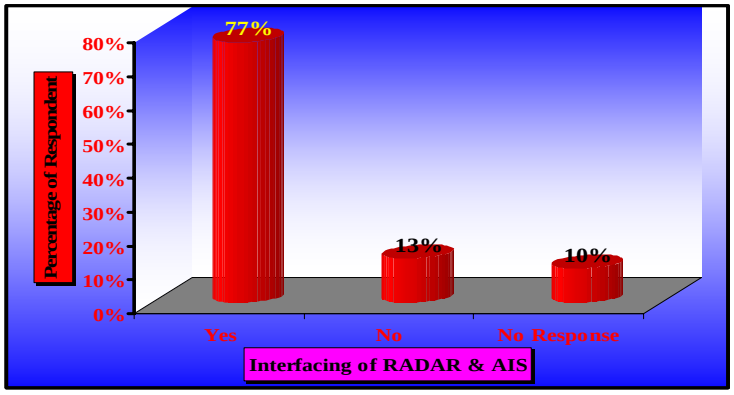


Figure24: LRIT fosters maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

It needs to be noted that most of the IMO member states have activated ship reporting system for search and rescue. The reporting into the system being voluntary, not many ships are reporting and the system is underutilized. The author is of the view that if reporting of ships when passing through the Search and Rescue Region (SRR)[62] of a nation be made mandatory so as to meet dual purpose for both maritime

[62] The SRR of a nation is the limits to which it is capable of delivering assistance. This limit if falling in the other nation's maritime zones then a mutual agreement has been made prior to its promulgation.

SAR and maritime security, it would be economical as most of the countries already have the system in place. The plot of ships in the ship reporting system can be provided to the maritime law enforcement agencies for maintaining vigil.

4.3 Threat perception based technology

The ISPS Code came into force on 1st July 2004, and the objective of this code was to "establish an international framework involving cooperation between contracting governments, government agencies, local administrations and the shipping and port industries to detect / assess security threats and take preventive measures against security affecting ships or port facilities used in international trade" (International Ship and Port Security (ISPS) Code, 2002, p. iii).

The Code delineated comprehensive measures for enhancing ships and port facilities' security based on risk management. It requires risk analysis to be carried out and implementation of necessary measures for preventing or mitigating consequences in the event of breach of maritime security. In order to meet the requirement of the Code different technologies have been adopted to enhance maritime security. The capabilities of these technologies are discussed below.

4.3.1 Container scanning

Container scanning was part of the initiatives taken by the U.S. Customs and Border Protection Agency to enhance maritime security. The initiative requires steps to be taken for ensuring that all cargo containers at ports outside the country are scanned before they are shipped to the United States. The policy is that a container should be transshipped only if it has been scanned 'Sail only if scanned' (SOS). Scanning of 100% baggage is already part of the aviation industry due to its fragility. According to Chalk (2008a, p. 10) "Today, 80 % of all global freight is transshipped by sea; 12 million to 15 million containers are estimated to be on the world's oceans at any one time". Out of it only 2% of them are checked for its contents (Banomyong, 2005; Blumel et al., 2008; Frittelli, 2003; Kanev, 2005). The container traffic is growing year after year, as it is the most suitable way to ship cargo because of easy and fast

handling (Figure 25). This has been only possible due to the advanced technology adopted by ports.

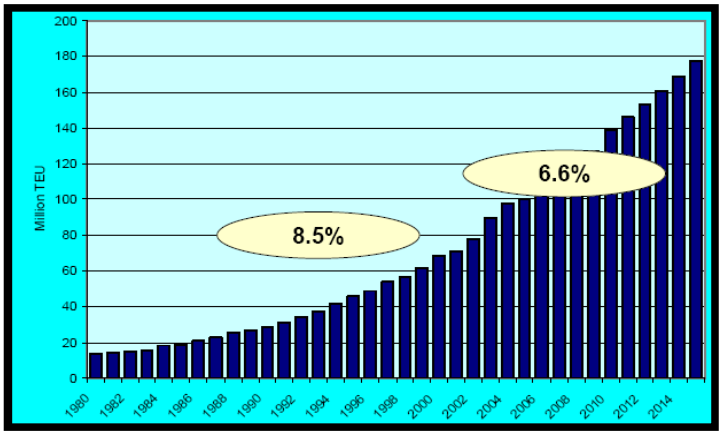


Figure25: Past growth and forecast of global container volumes (1980-2015).
Source: United Nation Report on Regional Shipping and Port Development Strategies, 2005, page 28, retrieved on July 28, 2008 from the World Wide Web:
http://www.unescap.org/ttdw/publications/tfs_pubs/pub_2398/pub_2398_fulltext.pdf

The maritime sector has welcomed the initiative of container scanning, but has raised its concern regarding feasibility of 100% scanning. The scanning technology available today cannot cope with the volume of container traffic and 100% scanning will severely impinge the trade. The container trade has been steadily growing and is likely to maintain the pace of growth in future also.

The volume of cargo that is shipped through containers, together with need for rapid movement and complex transport mechanisms, poses a great challenge to the security systems. The fast moving container supply chain has created a huge potential for terrorist groups and other perpetrators to use containers as modern day Trojan Horses for smuggling weapons of mass destruction (WMD) and mobilizing terrorists (Richardson, 2007). Therefore, scanning of containers has become inevitable in the wake of growing international terrorism and the consequent maritime security demands. Today, the scanning technology has not developed so that it can maintain the pace with the volume of cargo and the speed of its handling.

The dissertation survey also recommends that in order to protect the commercial trade, 100% scanning is not feasible for enhancing maritime security (see Figure 10).

The author is of the opinion that efforts should be made to develop technology that can be applied for scanning of container so that the pace of the container movement in the logistic chain is not affected. Presently, scanners employed require the container to pass at a slow speed at the time of scanning. A viable solution could be if the containers can be scanned in the loading/unloading process. This will save time and not hamper trade. According to John Alioto, CEO of VeriTainer Corporation "By using a combination of nuclear detection techniques with sophisticated software, we think that adequate security can be achieved without sacrificing global economic efficiency" (Jeffery, 2006, October, pp. 22-23). The Crane mounted scanner while loading/ unloading can scan the containers (Figure 26). If this technology is proved, then it will bring a revolution into the maritime industry and the tussle between security and economic efficiency will ease, breaking the deadlock between the two. This technology will be the way forward for maritime security in achieving its objective of making shipping secure.

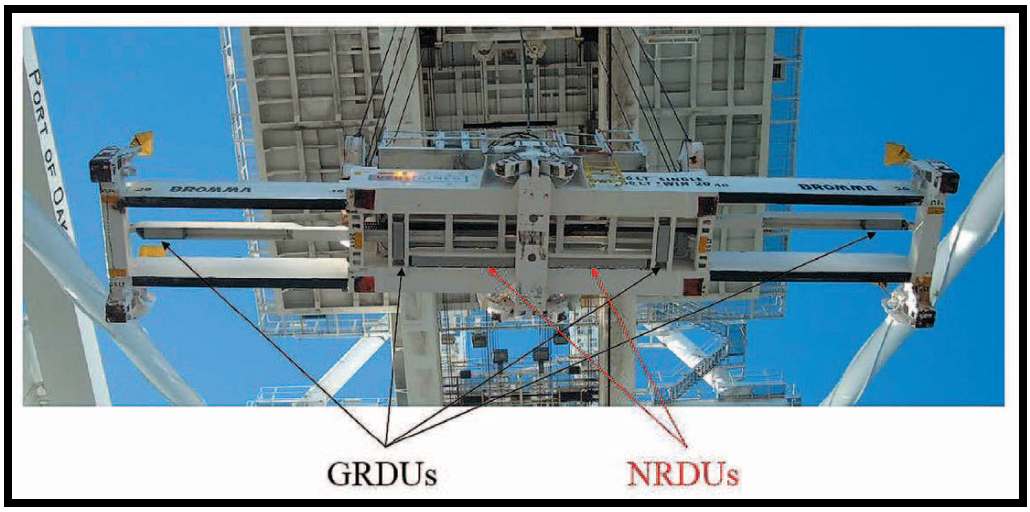


Figure26: The crane is fitted with gamma ray detection units (GRDUs) and neutron ray detector units (NRDUs) which scan the container while it is being moved.
Source: Digital Ship magazine October 2007, page retrieved on March 9, 2008 from the World Wide Web: http://www.thedigitalship.com/DSmagazine/DigitalShipOct06.pdf

4.3.2 Container Tracking

Container tracking is also one of the initiatives of the U.S. Customs and Border Protection Agency. As was brought out in Chapter 3, the World Customs Organization, the European Union and the G8 have welcomed the initiative and have expressed their support in CSI expansion. The containers, after they are sealed by the customs department of the departure country, travel through different modes of transportation, sometimes awaiting transshipment at intermediate ports before finally reaching the destination port. In this long multi-modal chain, it is seen that the containers are tampered with, goods stolen or replaced with illegal ones. Thus, the containers movements need to be monitored and containers carrying illegal weapons of mass destruction, or other illegal goods identified and confiscation. This complicated and herculean task can only be accomplished with the help of suitable technology. A provision for tracking the container will be critical to fostering maritime security manifold.

There are private companies providing a solution to the shippers to track their consignment from start point to the end point and even receive information on seal being tampered with. The Advanced Container Security Device (ACSD) from L-3 Communications[63] is one such solution that can track the cargo containers on their journey from the moment they are sealed until their arrival and delivery at destination port. The device will automatically identify tampering at any point in the container passage. ACSD will detect any breaches and unauthorized access and alert authorities to potential threats. Through ACSD, a container's condition can be monitored while in the supply chain through its real time communications network (L-3 Communications, 2006, October, p. 24).

[63] L-3 Communications is Defense Company in the United States and undertakes defense contracts in Intelligence, Surveillance and Reconnaissance (ISR), secure communications, government services, training and simulation and aircraft modernization and maintenance.

Looking from the security point of view, tracking of containers is important. It will foster maritime security only if there is an intelligence input indicating the container carrying illegal goods. However, containers that get maneuvered without coming under the intelligence scanner will be able to make to their destination because the other security measure, i.e. container scanning, is still not in place. Therefore, the author is of the view that suitable technology that can also give some indication of the presence of biological/ chemical materials, explosives, ammunition or other dangerous goods that can be used for destruction will be the way forward for achieving the maritime security objectives.

4.3.3 NANO Technology 'a way forward in Container Security'

Nanotechnology [64] has proved to be a revolution in the field of Science and Technology and has helped in development of devices, such as sensors, that are on a NANO scale[65]. Nanotechnology today harnesses developments in a wide spectrum of fields namely, chemistry, physics, materials science, and biotechnology for creating novel materials. Some of these inventions have been transformed into consumer products, such as sun screens and stain-resistant paints. Research is on at various levels for finding solutions to humanity's greatest problems, such as diseases, clean energy, and clean water. In future, nanotechnology products will pave the path for more revolutionary application to that of today ("Applications of Nanotechnology").

According to Dr. Morton L. Wallach, President of PEL Associates, NANO technology can be vital for container security such as container tracking and tampering detection. Utilizing the technology, Micro-sensors (~2-3mm spheres) can be designed with surface material reactive to chemicals and biological environment(Patel-Predd, 2008). On reaction, the sensors can be programmed to emit

[64] Nanotechnology refers to a field of applied science and technology whose theme is the control of matter on the atomic and molecular scale, generally 100 nanometers or smaller, and the fabrication of devices or materials that lie within that size range.
[65] One nanometer is one billionth, or 10-9 of a meter.

an agent specific color or infrared signal to its control system. In case of a dirty bomb or WMD, the sensor scan is designed with a conductive coating. When such a material is present that emits energetic particles, the air present in the container will get ionized. This ionized air, when it comes in contact with the sensors emits in a characteristic manner which is picked up by its control systems. Since the sensors have been designed utilizing NANO technology, their size is so small that they can be impregnated on to the surface of a thin plastic film, which in turn can be adhered to the wall. The cost of the sensor is estimated about 3-5 cents per sensor or five dollars per container. He further said that Nanotechnology could also be used to tag containers for tracking their movement along the supply chain with their updated position. Seals impregnated with NANO sensors could be fitted on the container door systems maintaining an electronic 'guard' on the doors. If the container is opened in an unauthorized manner, the sensor would transmit an alert (DiRenzo & Doane, 2007, March). The International Container Standards Organization (ICSO) on working for developing international security standards for ocean-going cargo containers. The author is of the view that ICSO needs to incorporate fitment of such sensors in the containers and the custom authorities before sealing the containers should certify proper functioning of these sensors. Such an arrangement will assist in mitigating the threats posed by containerization and will enhance maritime security.

4.3.4 Screening and identification of personnel

With exponential growth of the maritime sector the human interaction with facilities and ships has also significantly increased (World Travel & Tourism Council, International Hotel & Restaurant Association, International Federation of Tour Operators, International Council of Cruise Lines, & United Nations Environment Programme, 2002). Furthermore, shipping is the most affordable and luxury means of transportation with more than 12 million passengers cruising each year (Cruise Lines International Association, 2008). Therefore, it is important to have access control and scrutinize the credentials of the personnel. The Transportation Worker Identification Credential (TWIC) ID card scheme initiated by the US government is a positive step forward in maritime security. The identification card includes biometric

data, such as fingerprints, of the individual (Bryant, 2006, September; "US ID card scheme begins", 2007, April, p. 20). International Labour Organization (ILO) also adopted the revised Seafarers' Identity Documents (SID) Convention (Convention No. 185) in June 2003 for preventing acts of terrorism that threaten the security of passengers and crews and the safety of ships. The SID also incorporates biometric technology [66] (International Labour Organization, 2004). Biometric-based authentication is being extensively used for sensitive and important matters. Its utility can be seen in applications such as workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction security and Web security. It has also been effectively utilized in secure electronic banking, law enforcement, passport programs, driver licenses, and financial transactions ("Biometrics"). TWIC ID-card and SID initiatives will prove to be a great deterrent to criminals intending to intrude taking advantage of the large scale movement of the personnel and will be a vital identity for proving the credentials of genuine people associated with industry.

Since shipping is the most economical and comfortable means of transportation, the passengers utilizing these facilities are continuously growing, as can be seen from the data collected from shipping companies (Figure 27). Passengers travelling by cruise and passenger liners are being screened 100% since the numbers are small in comparison to ferries. Owing to the nature of ferry operations there have been difficulties as they mobilize mass populations in a short time for quick turnaround, which poses a great threat to maritime security.

[66] Biometrics is the automated method of recognizing a person based on a physiological or behavioral characteristic.

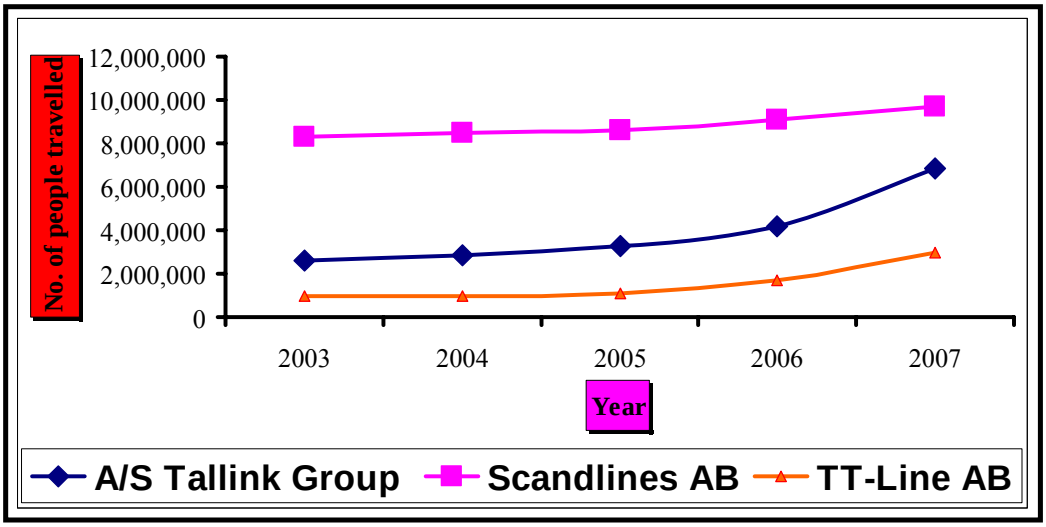


Figure27: Passenger traffic shipping 2003-2007.
Source: Data received from the shipping companies through E-mail.

4.3.5 SPO-20 – people screening security system

The X-ray and metal detectors are the common control security system which is seen at places such as airports. These systems are very useful when the number of people to be screened is limited or controlled. However, in high density places such as ferry terminals, it will take a long time for scanning each and every person. SPO-20 is capable of screening at places, where large volumes of people need to be screened (Figure 28). There is no emission as in the case of the traditional scanners. It uses the passive millimetre wave technology and is capable of detecting threats in high traffic areas at distances of up to 20 metres. It can detect a range of potential threats, including liquids and improvised explosive device (IED). Being a portable unit, it does not require any infrastructure ("SPO-20 is the only real-time people screening of its kind in the world"). Fitting a suitable number of SPO 20 will enhance the security of ferry services. The author is of the opinion that induction of such technologies in the maritime sector will complement other technologies adopted for enhancing maritime security.

Figure28: SPO-20, people screening security system.
Source: Retrieved on March 7, 2008 from the World Wide Web:
http://www.qinetiq.com/home/products/spo_20.html

4.4 Services for Safety of Navigation (Chapter V, SOLAS) fostering maritime security

Vessel Traffic Services

Charles W. Koburger Jr. (1986, p. 9) defines VTS as an "assortment of personnel, operational procedures equipment and regulations assembled for the purpose of marine traffic management…..it carries out surveillance and can be effectively utilized for enhancing maritime security in the area of operation". VTS is set up in an area of high traffic density, narrow channels and restricted waterways, traffic carrying hazardous cargoes, difficult hydrographical, hydrological and meteorological conditions, at port configuration. Such areas are considered a high risk for casualty. Therefore, traffic in such areas needs to be monitored continually so that it is regulated.

The infrastructure and other paraphernalia required for meeting its objectives are computers with suitable software for generating the surface picture of the traffic in the area, navigational sensors such as DGPS, AIS, and Metrological data. VTS has surveillance capabilities since "it is generally fitted with radars / ARPA, low light level TV, infrared (IR) cameras, radio direction finder, communication sets, patrol boats and long range patrol aircraft" (Koburger, 1986, pp. 10-11), which are vital

tools for maritime security. According to the dissertation survey, VTS is an active measure for mitigating security threats (Figure 29).

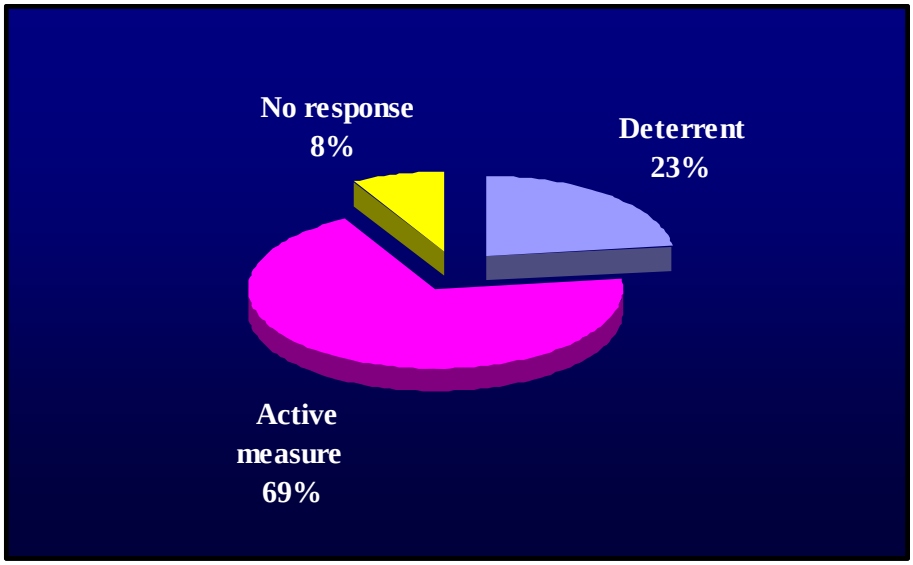


Figure29: VTS is a measure for mitigating security threat.
Source: Data compiled by author from the responses received from the questionnaire survey.

IMO identifies the purpose of vessel traffic services[67] as enhancing safety and efficiency of navigation, protection of the marine environment and adjacent shore areas. VTS plays a vital role in identification and monitoring of vessels for strategic planning of vessel movements, facilitating metrological and navigational information, and rendering assistance in emergencies. The efficiency of a VTS depends on reliable and secure communications. VTS also maintains a database of the participating vessels and this data can be easily retrieved for carrying out an analysis in case of a marine accident (International Maritime Organisation, 1997). However, all VTS will not be equally effective since reporting has not been made mandatory,

[67] IMO defines Vessel traffic service (VTS) as "a service implemented by a competent authority, designed to improve the safety and efficiency of vessel traffic and to protect the environment. The service should have the capability to interact with the traffic and to respond to traffic situations developing in the VTS area".

for example Malmö VTS. The survey results indicate that mandatory reporting will enhance overall security in the area (Figure 30).

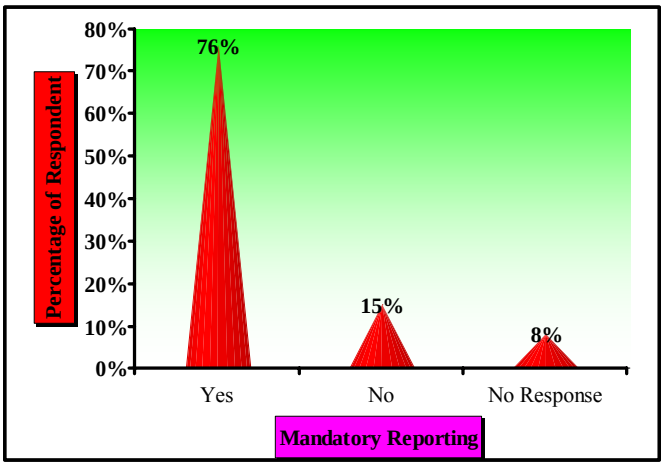


Figure30: Mandatory reporting to VTS will enhance maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

A VTS centre is required to continually monitor the movements of all shipping and other vessels for safety. In order to achieve safety it uses a traffic image of its operational area, developed by computers and continuously updated by the radars and other sensors configured with it. The system generates an alert if any potentially dangerous situation is developing. The operator advises the ship to take necessary measures or informs the authorities concerned to take necessary action to prevent any disaster (Richard, 2004; Valencia, 2006). "The basic function of VTS is data collection, data evaluation, information services, supporting allied services…." (Marcoyannis, 1988, p. 21). These are also the vital elements of security. VTS fosters maritime security since "movement reporting and surveillance together also helps identifying 'rogue' ships….."(Koburger, 1986, pp. 132-133).

In an assessment report submitted by the Philippine Port Authority, it has been brought out that the Vessel Traffic Management System (VTMS) is a valuable tool that can be used for tracking pirates. They could resolve four piracy cases namely Bay Bridge, Salvage Challenger, Barge Tenyu and Mercury, in Manila and bay area

("VTMS can track pirates", 2008, p. 11).The survey analysis also indicates that VTS fosters maritime security (Figure31).

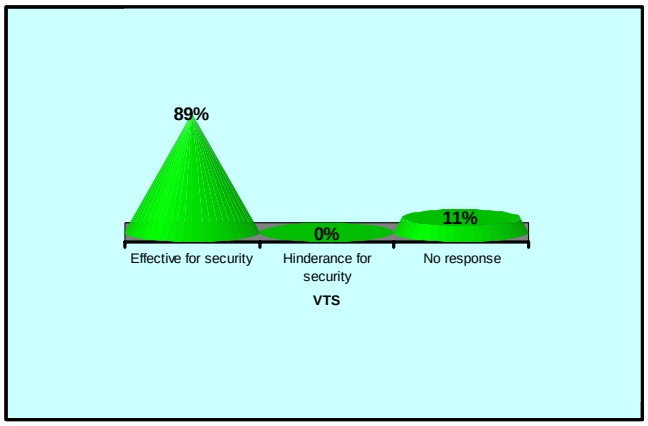


Figure31: Role of VTS in maritime security.
Source: Data compiled by author from the responses received from the questionnaire survey.

The author is of the view that the VTS staff if trained for maritime security, their services will be boon[68] to the maritime industry in fostering maritime security. Alternately, if the data and VTS plot is made available online to the maritime security agency this will also enhance maritime security.

4.5 Future Threat based technology for fostering maritime security

4.5.1 Cerberus360 Anti-Terrorist Diver Detection System

Incidents in the past have also revealed the vulnerability of maritime targets from small boats and divers (Richardson, 2004). The sinking of Sri Lankan Naval vessel by suicide divers of Tamil Tigers in 1995, the attack on an Israeli beach front by Hamas frogmen in March 2004, the targeting of Iraqi oil rigs with small boats laden with explosives in April 2004, the attack on USS Cole and oil rigs off the Iraqi coast targeted by small boats are some of the incidences drawing the attention of the existing threats. Detection of small boats or terrorist divers and swimmers armed with explosives will be the future challenge of security agencies (Dunham, 2004).

[68] Advantage

Cerberus 360 sonar is capable of providing diver detection at 800 metres radius. In order to provide full coverage of a port and channel a number of units in a cordon can be attached to the seabed (Figure 32). The advantage of cordon attachment is it enhances the coverage area to 1000 metres and beyond (Hardy, 2004). Usage of such equipment in future to protect high profile targets off shore and in ports for enhancing maritime security is not very far.

Figure32: Cerberus 360 anti terrorist diver detection system.
Source: retrieved on March 7, 2008 from the World Wide Web:
http://www.qinetiq.com/home/products/cerberus.Par.37768.Image.ImagePopup.html

4.5.2 Remote Operated Vehicle (ROV) System

Figure33: Remote Operated Vehicle System.
Source: Retrieved on March 7, 2008 from the World Wide Web: http://www.seaeye.com/

ROVs (Figure 33) have been in use for under water surveillance; mine counter measures as well as for commercial activities, such as salvage and diver support tasks as well as to coastal and inshore operators for observation, inspection, and environmental work, deep tunnel penetration and survey operations ("Saab Underwater Systems "). Adoption of this technology for providing underwater surveillance for high profile strategic targets will be effective in fostering maritime security.

4.5.3 High-Altitude Long-Endurance Unmanned Aerial Vehicle (UAV)

Figure34: High Altitude Long Endurance UAV.
Source: Retrieved on March 7, 2008 from the World Wide Web:
http://www.qinetiq.com/home/products/zephyr.Par.23364.Image.ImagePopup.html

UAV has been effectively utilized for carrying out surveillance by military forces for gathering information on strategic targets of enemy and Exclusive Economic Zones (EEZ) vigilance (Ball, 2004). However, this technology has not been utilized in the maritime sector for commercial shipping. Zephyr is an ultra-lightweight carbon-fiber aircraft capable of flying on the solar power which is generated by amorphous silicon arrays fitted in the aircraft wings (Figure 34). The thickness of silicon array is not thicker than sheets of paper which makes it ultra light. It can be launched by hand and weighs 30 kgs with a wingspan of up to 18 metres. It is also provided with rechargeable lithium-sulphur batteries that can be recharged during the day using solar power. The aircraft uses United Solar Ovonic solar arrays, a full flight-set of Solar Power batteries, as well as a novel solar-charger and bespoke autopilot. Zephyr has attained the world record for the longest duration unmanned flight. The aircraft achieved a 54-hour flight, reaching an altitude of 58,355 feet in September 2007 ("High-Altitude Long-Endurance Unmanned Aerial Vehicle ", 2008).

According to Home Affairs Minister Bob Debus, Australia "UAVs are quiet, virtually undetectable and can maintain extended surveillance of a target area or vessel for many hours at a time." Video, photographs, live radar and vessel information will be transmitted from the aircraft ("UAV tested for patrols over northern waters", 2008, May 23). UAVs can be effectively utilized for enhancing maritime security for commercial shipping with the growing threat from piracy and armed robbery and maritime terrorism.

4.5.4 Port and Channel surveillance

The attacks on USS Cole in the port city of Aden, Yemen and French VLCC Limburg in the Persian Gulf, off Yemen were described earlier. In the previous chapters, it has also been brought out that the threat to shipping in narrow channels and in port areas is high. Therefore, it is important to maintain port and channel surveillance. In most of the cases surveillance is generally carried out by radars. Further, as radar technology has limitation of acquiring / tracking small targets in port and channel areas, the possibility of an attack by small rubberized high speed boats is high. Therefore, to complement and overcome the technological deficiency, port and channel surveillance by Infrared thermal cameras (Figure 35) will enhance maritime security many folds.

Figure35: Thermalvision camera for port and channel security.
Source: Retrieved on 16 July 2008 http://www.gs.flir.com/docs/gs/Documents/Sentinel.pdf

4.5.5 Patrolling sensitive areas with Unmanned Surface Vessel

Harbors, anchorages and channels are strategic marine assets that are susceptible to a terrorist attack. Therefore, it is important to maintain a high degree of surveillance in these areas. In most countries, harbour, anchorage and channel patrol is being carried out by manned boats. It is difficult to carry out long hours of patrol by these boats because of fatigue, need to change and exposure to some degree of risk. Unmanned surface vessels (Figure 36) which can be remotely operated can be utilized for hours of surveillance and anti-piracy patrol, with no threat to human life. The vessel can be operated through a satellite system or with microwave guidance or cellular technology depending on the requirement of the security agencies.

Figure36: Patrolling by remotely controlled Unmanned Vessel.
Source: Retrieved on July 23, 2008 from the World Wide Web: http://www.5gmarine.com/

4.5.6 Secure Ships with electric fencing

It can be seen from the piracy incidents that ships with low superstructure are vulnerable to attacks as they are easy to board. Secure-Ship (Figure 37) is the most recent and effective innovation to fight against piracy. It is a non-lethal, electrifying fence surrounding the whole ship, which has been specially adapted for maritime use. The fence uses a 9,000-volt pulse to deter boarding attempts. An intruder coming in contact with the fence will receive an unpleasant non-lethal shock that will result in the intruder abandoning the attempted boarding. At the same time an alarm will go off, activating floodlights and a very loud siren. IMB also strongly recommends that

this arrangement will deter the pirates from getting access to the ships while moving and will assist in mitigating piratical attacks ("Secure-Ship ").

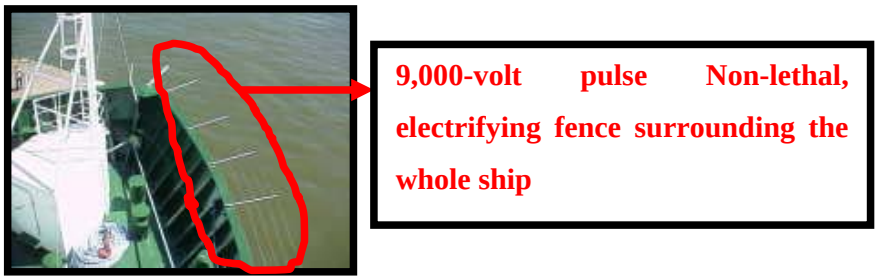


Figure37: Non- lethal electrical fencing around ship.
Source: Retrieved on July 17, 2008 from the World Wide Web: http://www.secure-marine.com/ship/ship3.htm

CHAPTER 5
CONCLUSIONS AND RECOMMENDATIONS

"Terrorism strikes at the very heart of everything the United Nations stands for. It presents a global threat to democracy, the rule of law, human rights and stability. Globalization brings home to us the importance of a truly concerted international effort to combat terrorism in all its forms and manifestations" **- Kofi Annan, Secretary-General, United Nations, Message to Tashkent Ceremony, June 17, 2004**

5.1 Conclusions

In this dissertation an attempt has been made to take the reader through the versatility of the maritime industry and vulnerability of its security. Economic boom especially in developing countries has lead to manifold increase in international trade. Ships have become more sophisticated with induction of new technology for improving efficiency and precision. The industry was focused on safety and environmental protection; maritime security took a back seat. The research reflects that the industry is vulnerable to piracy and armed robbery, and maritime terrorism. Piracy which started off as maritime muggings has become bloodier as it has transformed from the usage of swords to automatic weapons in committing heinous crimes against innocent seafarers.

On the other hand maritime terrorism incidents are less; however, maritime terrorism remains high on the risk agenda due to unprecedented growth of terrorism globally. A few incidents do not reduce the threat perception of such attacks.

IMO has adopted legal instruments such as the UNCLOS, SUA, SOLAS and ISPS, which form the legal umbrella for maritime security for combating these perils. It has been observed that these instruments have several shortfalls such as lack of uniformity in the adoption and application of the legal system to combat these

menace. However, it is beyond the scope of the dissertation and, therefore, not discussed.

The dissertation has attempted to find solutions to prevent industry falling prey to the piracy and armed robbery, and maritime terrorism by effective and optimal utilization of technology. To enable detailed analysis for its application and adequacy of the technology adopted in the maritime sector, the dissertation segregated it into four categories. These are identified technology primarily for maritime security, safety based, threat perception based, and systems setup for safe navigation.

SSAS which is inducted for alerting the shore authority is the only channel recommended by IMO. While carrying out analysis it was observed that the system sometime transmits false alerts due to its malfunctioning or accidental activation. Equipment provides no alarm on board when the alert is activated; hence no one on board will be aware of its activation and would not be able to cancel the alert. In case of distress and safety (GMDSS), IMO has ensured that the ship should be able to alert shore authorities by at least two separate and independent means and each using different radio communications services. There can be grave consequences of a maritime security incident and there will always be danger to life. Thus, relying on one technology and one mode of transmission in case of security threat needs to be addressed.

Moreover, present regulations restrict the transmission of the security alert to the flag administration or the nominated authority only and not to coastal states or other ships in the area[69]. The author is of the opinion that if the security alert is also transmitted to other ships in the area, in addition to providing assistance if possible, the ships will at least be vigilant and alert while passing through the area. Additionally, a coastal

[69] SOLAS 74, Chapter XI-2, Regulation 6.2.2

state is in a better position to provide early assistance to the affected ship avoiding delays which may occur under the current adopted procedures. IMO needs to further review the SSAS alert procedures to ensure a foolproof system with enhanced reliability, response time and improving safety.

The dissertation has brought out that the technology adopted to meet safety requirements can also be used as a secondary tool for enhancing security. Whilst using the equipment, its technological limitation needs to be considered which if used in tandem with other equipment may complement each other. For example, radar performance is limited in bad weather, but combined use of Radar and AIS under such environmental conditions will produce better results and thus enhance safety and security as well. The dissertation also analyzed the important of identifying small unlit boats for safety and security point of view. Thus recommends for feasible study for fitting infrared cameras on board.

The usage of optional or non mandatory technology is based on the threat perception and cost analysis by a country or region. According to the author, the ISPS Code is a risk management system. In order to comply with the provisions of the code some countries have taken steps forward and initiated additional measures such as scanning and tracking of the containers, and screening of personnel to mitigate the risk involved.

Readers may agree that the threat to maritime security is maritime mobile units and its infrastructure being used as mode of transportation for transporting illegal arms and ammunition including WMD. Since the volume of goods shipped by sea is very large there always exists a risk of illegal cargoes being shipped along with legitimate cargo. Segregating such cargoes is a challenge and a voluminous task beyond the capability of humans. Therefore, measures have been initiated for utilizing technology to identify and track such shipments.

Today the container traffic has grown to the extent that about 12 million to 15 million containers and 80% of the cargo is shipped through containers. The US initiative for screening of containers is a positive step for enhancing maritime security. However, due to the large number of containers involved, it may not be practical to carry out 100% scanning with the present technology in use.

Whilst carrying out the research, the author reviewed paper by the NANO technology Inc which suggests that the usage of NANO sensor for detection of radioactive materials, chemical and biological agents can be used. Currently, this technology is being applied in other areas and the concept involved creating novel materials optimizing their unique properties as their structures can be determined utilizing the nanometer scale[70]. The sensors developed will be 2-3mm in size and are also economical (costing approximate3-5 cents).

Under current conditions proper identification of shipment is of paramount importance and NANO technology provides a solution which needs to be further assessed and developed for industry specific use[71]. The author strongly feels that adopting such innovative technologies in the maritime sector is the need of the hour in the context of the current security perspective.

TWIC[72] ID and SID[73] require biometric data of individuals, which is a positive step to prevent unauthorized access. Biometric data is a reliable and well tested system used in identifying the credentials of an individual and has been adopted by vital sectors such as Immigration control, and banking. A research study undertaken by

---

[70] One nanometer is one billionth or 10^{-9} of a meter.
[71] NANO sensors can be designed with metallic reactive to chemical and biological environment, with conductive coating for detecting dirty bombs or WMD or can also be used in the seals for detecting any unauthorized access after the container has been sealed and till it reaches its detonation.
[72] Transportation Worker Identification Credential.
[73] Seafarers' Identity Documents.

National security research division of RAND cooperation reveals in future bio & NANO technology will play a dominant and significant role.

Navigational safety system such as VTS, whose prime function encompasses safety enhancement, is also an effective tool for fostering maritime security. Today, VTS has been set up in almost every vital junction on the sea route, thus ensuring smooth flow of traffic and assisting ships in safe navigation. The technology provided by the system enables the VTS operators to monitor the area effectively, thus enabling good assessment about the developing traffic situations. This will also facilitate the security agencies to monitor ships navigating in the area and identify rogue ships, if any. Therefore, VTS information will enhance maritime security and needs to be shared with the security agencies. However, research indicates that VTS data and also data from other sources such as AIS, ship entering/ leaving information are not been shared effectively, which needs to be addressed by the individual member states.

LRIT will be fully functional by 31 December 2008, which will be boon[74] to the maritime security as the movement of all the ships in its water can be monitored by member state. However having a secure data bank of ships with their company's details will assist in tracking down the culprits and bring them to book when indulging in illegal activities. Moreover, exchange of information between port authorities regarding movement of ships from one port to another, will compliment LRIT objectives and further boosting maritime security.

Further, the dissertation highlights that even the best technology available will not be able give to the desired results if it is not properly and optimally exploited. Having seen the capability of various technologies, the dissertation has brought out certain other important issues that need consideration for enhancing maritime security.

[74] Advantage

These are the issues of training, ergonomics and effective implementation of instruments. Training is an inevitable part and it not only improves professionalism but also better appreciation of a situation under given conditions. Training of seafarers on simulators for different security scenarios will psychologically prepare them to handle dangerous situations of terrorism till arrival of shore support of a national security agency.

Ergonomics also plays an important role in maritime security, as human interface is must for scanning and monitoring of large volume of containers and cargo. Hence, technology needs to focus on ergonomic issues too.

Last but not the least, the most crucial is the role of member states in ensuring effective implementation of maritime security instruments to which they are signatory. Currently, there is no mechanism for IMO to ensure that the measures taken by the administration are adequate enough to meet the objective of the instrument. Introduction of a voluntary IMO member audit scheme is a step in the right direction enabling and assisting member states to work towards the goal of Safe, Secure and Efficient Shipping on Cleaner Oceans.

The dissertation has also identified the importance of the human aspect involved in ensuring the effectiveness of the technology used as it is always the man behind the machine that makes the difference. Today the shipping industry works on cost cutting measures for making more profits and for some flag administrations the sole objective remains to register more ships without any regard to the quality of tonnage involved. The survey results are also indicative of this fact and recommends that IMO take more active measures in manning (Figure38).

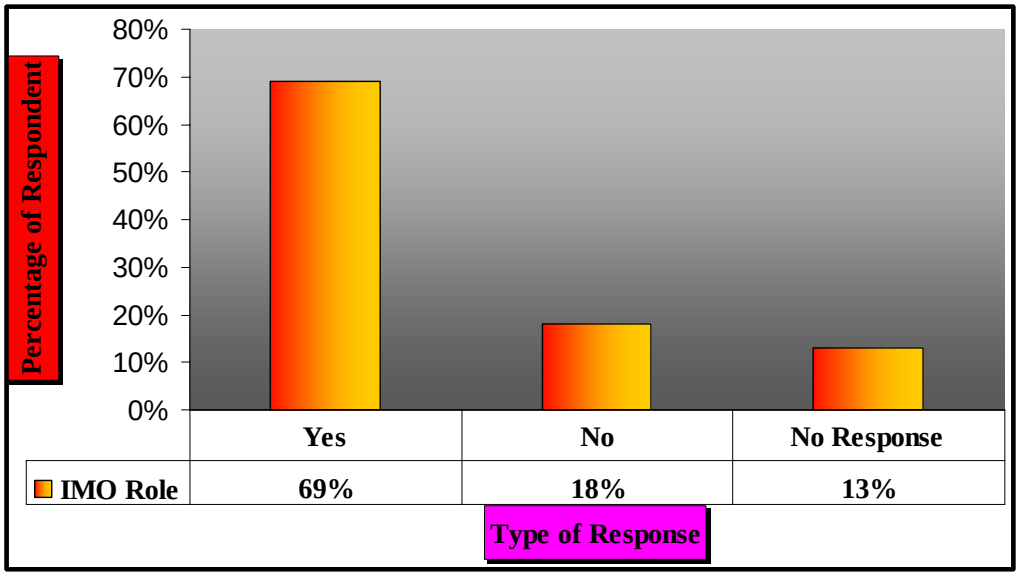


Figure 38: IMO needs to have more active role in present manning process.
Source: Data compiled by author from the responses received from the questionnaire survey.

The author summarizes the requirement of maritime security as enumerated in the dissertation in a top-down and bottom-up design (Figure 39). The maritime environment is gigantic and complex. Securing it from being attacked or from being used in an attack, or in support of an attack, is a global challenge. The author feels that the recommendations in the succeeding paragraphs if adopted may pave the path for success and enhance maritime security.

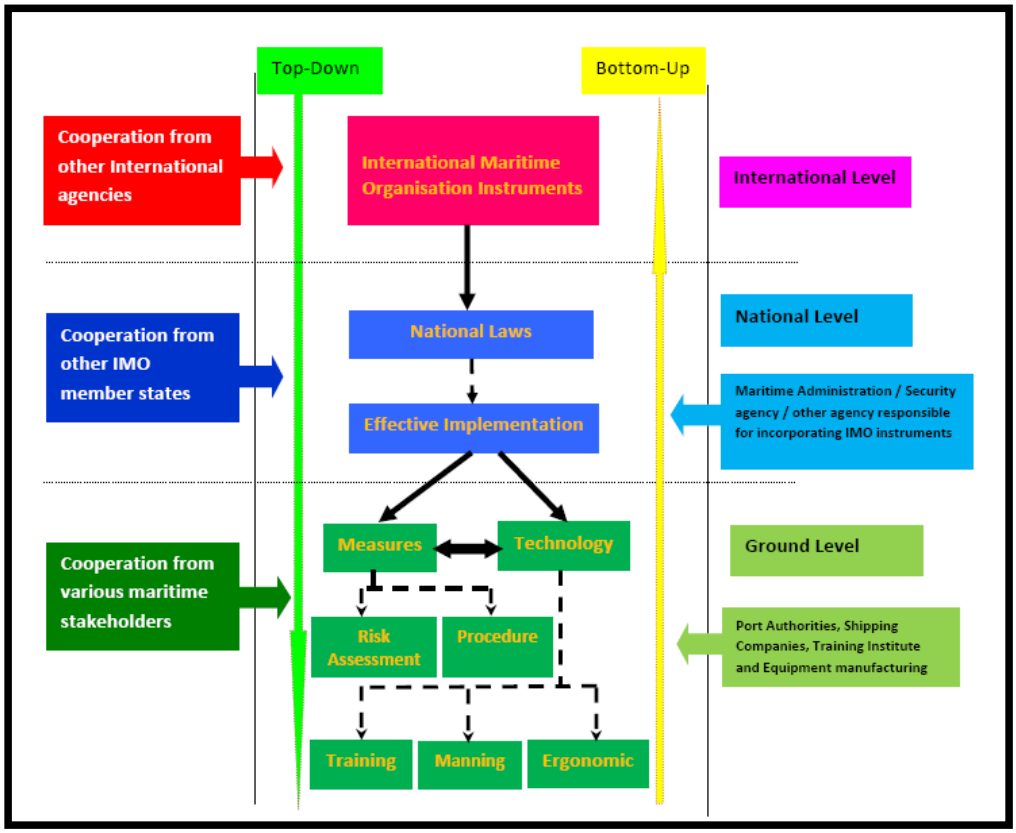


Figure 39: Top-Down and Bottom-Up concept for fostering Maritime Security.
Source: Author 2008

5.2 Recommendations

(a) Review of alerting procedures for maritime security incidents and seeking and developing alternate means of communication on lines of GMDSS. A feasibility study for making similar provision in Inmarsat-C and VHF DSC for transmitting security alerts.

(b) Fitting of 9,000 volt fence in areas with low free board to prevent intruders gaining access to the ship while it is moving. Fitting all around the ship will be more preferred as it will prevent intrusion at anchorages and in ports.

(c) Feasible study for fitting of infrared cameras for maintaining all round surveillance while ship is at port, anchorage or at sea, against non conspicuous radar targets and vessels not complying with AIS requirements.

(d) Adoption and development of new technologies such as NANO technology for its application in monitoring movement of containers and be able to identify the cargoes in the container in an effective, efficient and economical solution.

(e) From the security perspective, it is important that the agencies responsible for maritime law enforcement should be provided with the information and data that is available for carrying out proper analysis. MarNIS[75] is an ideal platform created by the European community, where all the stake holders including law enforcement agencies have access to the information. This will facilitate a holistic view and complete the surface picture of vessel movements, making monitoring more effective and enabling proactive preventive measures rather than reactive measures for boosting maritime security. MRCC are linked to such databanks. Therefore, housing maritime law enforcement agency with MRCC by member state will foster maritime security (Figure 40)

[75] Community Vessel Traffic Monitoring and Information System.

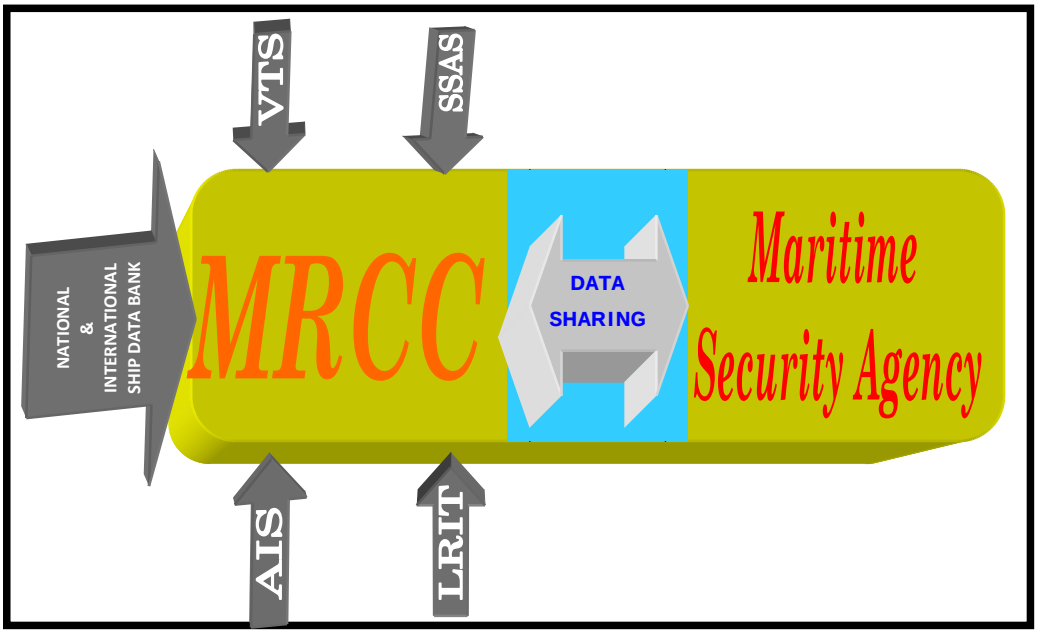


Figure 40: Collocating MRCC and Maritime Security agency in a member state for effective data sharing.
Source: Author 2008

(f) Developing of a secure data bank consisting of ship's name, call sign, MMSI number, IMO number, and Flag administration name and contact details including telephone, fax and E-mail address, of ships operating in the international trade. This will facilitate security agencies to correlate the data with the AIS data being transmitted by the ship and the IMO number engraved on the vessel. This correlation will assist in identifying phantom ships. Discrepancies in ship's data in databank with the actual documents should be treated as deficiency under port state control. It will ensure that genuine ships operate for the industry and owners can be tracked when required, making flag administration accountable for their flag ships. Correlation of ships data from the databank with visual details will help in identifying 'Phantom Ships' by maritime security forces during patrol.

(g) Establishing a 'Port Fixed Telephone Network (PFTN)' link between various ports serving international shipping for exchange of information

regarding ships departure and next port of call. Similar practice is being followed among various airports in the world. LRIT data in conjunction with this information will help maritime security agency to monitor any deviation from the intended plan and will prevent ships indulging in illegal activities.

(h) Numerous studies have been carried out for man-machine interface for improving maritime safety at sea, since maritime security elements also contain both technology and the human element. Therefore, similar studies need to be carried in order to develop and improve its ergonomics which eventually will improve security.

(i) Review of manning requirements to meet the growing demand of maritime security and other instruments.

The tussle will remain between the idealists and pragmatists doing the Cost Benefit Analysis, where the idealist will argue that no price can be placed on human life while the pragmatist will say that sadly such assessments are a daily occurrence, ask anyone working in P&I(Alderton, 2002). In the end, the author would like to conclude by submitting that the technology has immense potential for monitoring, detection, scrutinizing and alerting. Correct technology needs to be developed and adopted in the maritime sector, which will produce the desired result. However, the objectives of maritime security in the fragile political scenario still remain a distance dream. There is a need to develop an environment of trust to overcome the perilous situation evolved by terrorism and piracy. Nothing is impossible to achieve, it is just sincere consistent selfless iterative efforts and verve required on part of the Flag States, Ports States, Coastal States, maritime transport providers, and the users, to use their best endeavor to fight the peril. ‘Good will’ will prevail, synergizing the efforts, overcoming the difficult mission, and making shipping safe and secure for all.

REFERENCES

Abhyankar, J. (2005). Maritime crime. In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 201-243). Malmö, Sweden: WMU Publications

Abhyankar, J. (2007). Piracy and armed robbery at sea: an overview. In M. Q. Mejia & J. Xu (Eds.), *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea* (pp. 97-119). Malmö: WMU Publications

Abhyankar, J. (Ed.). (2006). *Piracy, Armed Robbery and Terrorism at Sea: A Global and Regional Outlook*. Singapore: Institute of Southeast Asian Studies, 30 Heng Mui Keng Terrace, Pasir panjang, Singapore 119614.

AIS - help or hindrance? [Electronic (2008). Version]. *Signals NewsLetter*, 12. Retrieved July 1, 2008 from The World Wide Web: http://www.nepia.com/risk/publications/newsletters/pdf/signals_70.pdf.

ALDERTON, P. M. (2002). The maritime economics of security. *Maritime Policy & Management: An International Journal of Shipping and Port Research, 2*(29), 105 — 106.

Amirell, S. E. (Ed.). (2006). *Political Piracy and Maritime Terrorism : A Comparison between the Straits of Malacca and the Southern Philippines*. Singapore: Institute of Southeast Asian Studies, 30 Heng Mui Keng Terrace, Pasir panjang, Singapore 119614.

Anstey, F. Maritime Security Regulations: Who Really Pays? [Electronic Version]. *International Association of Maritime Universities*. Retrieved April 1, 2008 from the World Wide Web. http://www.iamu-edu.org/generalassembly/aga7/projectsession/35_MaritimeSecurityRegulations.pdf.

Anstey, F. (Ed.). (2005). *The fast track to ISPS code and national security regulation implementation and the implications for maritime educators*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Anthony, D. (2005). Scanning the world for the best security solution. *Bimco Review*, 179-181.

Applications of Nanotechnology. Retrieved July 22, 2008, from the World Wide Web: http://www.foresight.org/nano/applications.html

Ashmawy, M. E. D. M. E. (Ed.). (2005). *Including ISPS requirements in the MET scheme of the Arab Academy for Science, Technology and Maritime Transport through its Regional Maritime Security Institute*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Asia Pacific Economic Cooperation. (2008). Key APEC Milestones. Retrieved August 7, 2008, from The World Wide Web: http://www.apec.org/apec/about_apec/history.html

Audit Scheme under way. (2007, February). *Safety at Sea International,* 40-41.

Ball, D. (2004). Intelligence collection operations and EEZs: the implications of new technology [Electronic Version]. *Marine Policy*, 67–82. Retrieved July 22, 2008 from the World Wide Web: http://www.sciencedirect.com/science?_ob=MImg&_imagekey=B6VCD-4B3JSS9-1-1&_cdi=5952&_user=6990453&_orig=search&_coverDate=01%2F31%2F2004&_sk=999719998&view=c&wchp=dGLbVtb-zSkzk&md5=e2e6440a5bc6929ee2f4bc8f1ece51b9&ie=/sdarticle.pdf.

Banlaoi, R. C. (Ed.). (2005). *Maritime Security Outlook for Southeast Asia*. Singapore: Institute of Defence and Strategic Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798.

Banomyong, R. (2005). The impact of port and trade security initiatives on maritime supply-chain management *Maritime Policy & Management, 32*(1), 3-13.

Biometrics. (September 3, 2007). Retrieved March 3, 2008, from the World Wide Web: http://www.globalsecurity.org/security/systems/biometrics.htm

Blanco-Bazán, P. A., Hesse, H. G., Jianxin, Z., & Charalambous, N. L. Work Undertaken by the International Maritime Organization: In an Effort to Prevent and Combat Terrorism. London: International Maritime Organisation, 4 Albert Embankment, London SE1 7SR, United Kingdom.

Blanco-Bazán, P. A., Jianxin, Z., Hesse, H. G., & Charalambous, N. L. Work Undertaken by the International Maritime Organization in an Effort to Prevent and Combat Terrorism [Electronic Version]. *IMO Papers*, 10. Retrieved July 25, 2008 from the World Wide Web: http://www.imo.org/.

Blöchl, D. (2007). EMPA News. *European Maritime Pilots Associations(EMPA), , 43*(August), 7-9.

Blumel, E., Boeve, W., Recagno, V., & Schilk, G. (2008). Ship, Port and Supply Chain Security Concepts Interlinking Maritime with Hinterland Transport Chains. *WMU Journal of Maritime Affairs, 7*(1), 205-225.

Blumenthal, D. (2008). C-TPAT strengthens ability to manage supply chain: survey [Electronic Version]. *Frontline*, 49. Retrieved July 23, 2008 from the World Wide Web: http://www.cbp.gov/linkhandler/cgov/newsroom/publications/frontline_magazine/frontline.ctt/frontline.pdf.

Bole, A., Dineley, B., & Wall, A. (2005). *Radar and ARPA Manual* (Second ed.). UK: Elsevier Butterworth-Heinemann, Linacre House. Jordan Hill, Oxford OX2 8DP, 30 Corporate Drive, Burlington, MA 01803.

Bonner, R. C. (2003). Keeping world trade safe, secure and efficient. *Bimco Review*, 112-115.

Bonner, R. C. (2005). From Cold War to war on terror: security and facilitation in the post-9/11 era. *Bimco Review*, 174-177.

Boutilier, J. (Ed.). (2005). *The Best of Times, the Worst of Times: The Global Maritime Outlook 2004*. Singapore: Institute of Defence and Strategic Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798.

Bowring, A. (2006, January). Safe Manning [Electronic Version]. *Alert*, 8. Retrieved March 9, 2008 from the World Wide Web: http://www.he-alert.org/user/download.asp.

Brehaut, D. (2002). *GMDSS: A User's Handbook* (Second ed.). London: Adlard Coles Nautical, 37 Soho Square, London W1D 3QZ.

Brew, N. (2003). Ripples from 9/11: the US Container Security Initiative and its Implications for Australia. Retrieved July 21, 2008, from the World Wide Web: http://195.178.246.26/maritime/03cib27.pdf

Bryant, D. (2006,September). TWIC: A Bridge Too Far? [Electronic Version]. *Maritime Repoter and Engineering News*, 22-24. Retrieved March 28, 2008 from the World Wide Web: http://www.marinelink.com/magazines/archive.aspx?m2=mr.

Burch, D. (1999). *Starpath Radar Trainer: User's Guide*. Retrieved June30, 2008, from the World Wide Web: http://www.webwerff.nl/hobby/ezs/sp/radar.pdf.

Burmester, C. International Ship and Port Facility Security (ISPS) Code – perceptions and reality of shorebased and sea-going staff [Electronic Version]. *International Association of Maritime Universities*. Retrieved April 1, 2008 from the World Wide Web: http://www.iamu-edu.org/generalassembly/aga6/pdf/s2-burmester.pdf.

Chakrabarti, D. Ergonomics/ Human factors : Human aspect of technology [Electronic Version], 7. Retrieved July 31, 2008 from the World Wide Web: http://www.iitk.ac.in/directions/march2005/13_DebKC.pdf.

Chalk, P. (2008a). *The Maritime Dimension of International Security*. Retrieved July 30, 2008, from the World Wide Web: http://www.rand.org/pubs/monographs/2008/RAND_MG697.pdf.

Chalk, P. (2008b). *The Maritime Dimension of International Security: terrorism, piracy, and challenges for the United States*. Santa Monica: RAND Corporation 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138.

Chamberlain, G. (2008). Pirate attacks around the world rise by 20pc. Retrieved May 24,, 2008, from the World Wide Web http://www.telegraph.co.uk/news/2021510/Pirate-attacks-around-the-world-rise-by-20pc.html

Chellaram, S. L. (2004). Globalisation and the shipping business- a shipowner's perspective. *BIMCO Review*, 28-31.

Comite Maritime International. (1997). Report of the joint International working group. Retrieved June 08, 2008, from the World Wide Web: http://www.comitemaritime.org/singapore/piracy/piracy_report.html

Council, N. P. (2007). *Facing the Hard Truths about Energy: A comprehensive view to 2030 of global oil and natural gas*. Washington D.C.: National Petroleum Council.

Counter-Terrorism Task Force. (2003, August). The Need to Build Capacity to Fight Terrorism [Electronic Version]. Retrieved August 7, 2008 from the World Wide Web: http://www.apec.org/apec/documents_reports/counter_terrorism_task_force/2003.html.

Cruise Lines International Association. (2008). Personal Safety And Security Retrieved April 24, 2008, from http://www.cruising.org/industry/personal_safety_security.cfm

Daly, J. (2008). Terrorism and Piracy: The Dual Threat to Maritime Shipping. *Terrorism Monitor, VI* (16), 4-7.

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

Diestel, H.-H. (2005). *Compendium on Seamanship & Sea Accidents*. Hamburg Seehafen Verlag GmbH, Postfach 10 16 09, Nordkanalstrabe 36, D-20097 Hamburg.

DiRenzo, J., & Doane, C. (2007, March). Nanotechnology: The Next Frontier? [Electronic Version]. *Maritime Repoter and Engineering News*, 40-41. Retrieved March 28, 2008 from the World Wide Web: http://www.marinelink.com/magazines/archive.aspx?m2=mr.

Dunham, S. (2004). Defending the Fleet in Harbor -Stevens Tech Studies Navy Antiterrorism and Force Protection Measures [Electronic Version]. *Journal of Homelands Security*. Retrieved May 5, 2008 from the World Wide web: http://www.homelandsecurity.org/newjournal/Articles/displayArticle2.asp?article=112.

EC Project MARNIS. (2007). *The MARNIS Concept*: [Brochure]. EC Project MARNIS: Author

Editor, T. (2004, July). Garbage In, Garbage Out..... [Electronic Version]. *Alert*, 8. Retrieved March 9, 2008 from the World Wide Web: http://www.he-alert.org/user/download.asp.

Eklöf, S. (2005). Piracy in Southeast Asia: Real Menace or Red Herring? [Electronic Version]. *Japan Focus an Asian Pacific e- journal*. Retrieved February 20, 2008 from the World Wide Web. http://www.japanfocus.org/products/details/2370.

Enhanced Focus on Maritime Security in IMO Secretariat [Electronic (2007, August). Version]. *International Federation of Shipmaster's AssociationsNewsletter no 52*. Retrieved March 28, 2008 from the World Wide Web: http://www.ifsma.org/.

Er, Z., & Celik, M. (Eds.). (2005). *Definitions of human factor analysis for the maritime safety management process*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Eteris, E. (2008). Maritime policy for the European Union: a new Commission's initiative [Electronic Version]. *The Baltic Course*. Retrieved July 21, 2008

from the World Wide Web: http://www.baltic-course.com/eng/eu_baltics/?doc=3214.

European Union. (2005, June 10). *Procedures for conducting Commission inspections in the field of maritime security,COMMISSION REGULATION (EC) No 884/2005 of June 10, 2005*. Retrieved. from the World Wide Web: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_148/l_14820050611en00250029.pdf.

European Union. (2005, October 26). *Measures on Enhancing Port Security, Directive 2005/65/EC of the European Parliament and of the Council October 26, 2005*. Retrieved. from the World Wide Web: http://europa.eu.int/eur-lex/lex/LexUriServ/site/en/oj/2005/l_310/l_31020051125en00280039.pdf.

Fotland, H. (2004, April). Humen Element-A Fragile Chain of Contributing Elements [Electronic Version]. *Alert*, , 8. Retrieved March 9, 2008 from the World Wide Web: http://www.he-alert.org/user/download.asp.

Franson, J. (2005). Formulating the ISPS Code: a general background. In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 9-15). Malmö: WMU Publications

Frecon, E. (Ed.). (2006). *Piracy and Armed Robbery at Sea along the Malacca Strait: Initial Impressions from the Riau Islands*. Singapore: Institute of Southeast Asian Studies, 30 Heng Mui Keng Terrace, Pasir panjang, Singapore 119614.

Frittelli, J. F. (Ed.). (2003). *Maritime Security: Overview of Issues*. New York: Nova Science Publishers, Inc., 400 Oser Ave, Suite 1600 Hauppauge, New York 11788-3619.

Gill, M., Burns-Howell, T., Keats, G., & Taylor, E. (2007). *Demonstrating the value of security*. Retrieved July 9, 2008, from the World Wide Web: http://www.perpetuityresearch.com/publications.html#valueofsecurity.

Glass, C. (2003, December 18). The New Piracy [Electronic Version]. *London Review of Books*. Retrieved August 8, 2008 from the World Wide Web: http://www.lrb.co.uk/v25/n24/glas01_.html.

Hadfield, L. (2004). Are drugs and alcohol rocking your boats. *Bimco Review*, 164-166.

The Halifax Explosion. Retrieved July 06, 2008, from the World Wide Web: http://www.halifaxexplosion.org/intro.html

Hardy, G. (2004). Anti-terrorist diver detection system to be evaluated by US Navy. Retrieved March 7, 2008, from the World Wide Web: http://www.qinetiq.com/home/newsroom/news_releases_homepage/2004/2nd_quarter/anti-terrorist_diver.html

Harmon, C. K. (2007, August 08). ISO offers systematic approach to container security tracking. Retrieved July 24, 2008, from the World Wide Web. http://www.iso.org/iso/pressrelease.htm?refid=Ref1067

Hecht, H., Berking, B., buttegenbach, G., Jonas, M., & Alexander, L. (2002). *The Electronic Chart*. Netherland: GITC bv, Lemmer, The Netherlands.

Herbert-Burns, R. (Ed.). (2005). *Terrorism in the Early 21st Century Maritime Domain*. Singapore: Institute of Defence and Strategic Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798.

Hesse, H. (2003). Ship and port security - the IMO's response. *Bimco Review*, 118-120.

Hesse, H. (2007). A briefing on maritime/coastal security. In M. Q. Mejia & J. Xu (Eds.), *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea* (pp. 189-197). Malmö: WMU Publications

Hesse, H., & Charalambous, N. L. (2004). New Security Measures for the International Shipping Community. *WMU Journal of Maritime Affairs, 3*(2), 123-138.

High-Altitude Long-Endurance Unmanned Aerial Vehicle (2008). Retrieved March 7, 2008, from the World Wide Web: http://www.qinetiq.com/home/products/zephyr.html

History of IMO. Retrieved July 10, 2008, from the World Wide Web: http://www.imo.org/

Howland, J. (2004a). Countering Maritime Terror, U.S. Thwarts Attacks, Builds Up Foreign Navies: Resistance Encountered in Critical Malacca Straits Region Foreign Crews to Be Investigated for Terror Ties Retrieved July 01, 2008, from the World Wide Web: http://www.jinsa.org/articles/articles.html/function/view/categoryid/1701/documentid/2567/history/3,2360,655,1701,2567?error=Session+Expired

Howland, J. (2004b). Hazardous Seas: Maritime Sector Vulnerable to Devastating Terrorist Attacks. Retrieved July 01, 2008, from the World Wide

Web:http://www.jinsa.org/articles/index.html/function/view/categoryid/1701/documentid/2426/history/3,2360,655,1701,2426

Hudson, S. (2006). Smart and Secure Tradelanes [Electronic Version]. *Supply Chain Resource Consortium*. Retrieved July 30, 2008 from the World Wide Web: http://scm.ncsu.edu/public/security/sec060221.html.

Hurst, C. (2008). Terrorist Threats to Liquefied Natural Gas: Fact or Fiction? [Electronic Version]. *The Cutting Edge*. Retrieved June 21, 2008 from the World Wide Web: http://www.thecuttingedgenews.com/index.php?article=529.

IMB launches new hotline. (2007, August). *Safety at Sea International,* 10.

IMO. (November 23, 1995). *Performance Standards for a Ship Borne Integrated Radio Communication System (IRCS) when used in the GMDSS, Resolution A.811 (19)*. London: International Maritime Organisation.

Increased manning could combat piracy. (2007, August). *Safety at Sea International,* 10.

Insall, C. (2003). Recent developments in communications and safety requirements for ship operators via satellite. *Bimco Review*, 215-219.

International Labour Organization. (2004). *Seafarers' Identity Documents Convention (Revised), 2003 (No. 185) ILO Seafarers' Identity Documents Biometric Testing Campaign Report Part I Geneva, 2004*. Retrieved July 22, 2008, from the World Wide Web: http://www.ilo.org/public/english/dialogue/sector/papers/maritime/sid-test-report1.pdf.

International Labour Organization. (2008). The ILO at a glance. Retrieved August 3, 2008, from the World Wide Web: http://www.ilo.org/global/About_the_ILO/lang--en/index.htm

International Maritime Organisation. (1997). *Resolution A.857(20): Guidelines for Vessel Traffic Services*. London: International Maritime Organisation.

International Maritime Organisation. (2000). *Amendment to the code for the investigation of marine casualties and incidents[Resolution A.849(20)]*. London: International Maritime Organisation.

International Maritime Organisation. (2002, December 9). *Opening Address by the Secretary-General of The International Maritime Organization Mr. William A. O.Neil SOLAS/CONF.5/INF.4*

International Maritime Organisation. (2004,December). Goal-based standards under development at IMO's Maritime Safety Committee. Retrieved July 21, 2008, from the World Wide Web: http://www.imo.org/newsroom/mainframe.asp?topic_id=848&doc_id=4574#security

International Maritime Organisation. (2008). *IMO: 50 years, 50 treaties on 20 April 2008*. Retrieved April 30, 2008, from the World Wide Web: http://www.imo.org/home.asp.

International Maritime Organization. IMO Convention adopted 60 years ago, IMO news briefing 04, 06 March 2008. Retrieved 20 April, 2008, from http://www.imo.org/home.asp

International Maritime Organization. (2002, December 5). *Summary of Decision*. Retrieved June 10, 2008, from the World Wide Web: http://docs.imo.org/Category.aspx?cid=38&session=89.

International Maritime Organization (1998 May 12). *Adoption of New and Amended Performance Standards*. London: Author.

International Maritime Organization (2002 January 25). *Guidelines for the Onboard Operational Use of Ship borne Automatic Identification Systems (AIS), Resolution A.917 (22)*. Retrieved July 10, 2008, from the World Wide Web: http://www.imo.org/includes/blastDataOnly.asp/data_id%3D6031/222.pdf.

International Maritime Organization (2002 January 25). *Guidelines for the Onboard Operational Use of Ship borne Automatic Identification Systems (AIS)*. London: Author.

International Maritime Organization Legal Committee. (2007). *Draft report of the legal committee on the work of its ninety-third session*. London.

International Ship and Port Security(ISPS) Code. (2002). (2003 ed.): International Maritime Organization,London.

Jane's Terrorism and Insurgency Intelligence Centre. (2007). JTIC briefing: LNG tanker terrorism [Electronic Version]. Retrieved July 6, 2008 from the World Wide Web: http://www.janes.com/news/security/terrorism/jtic/jtic070803_1_n.shtml.

Jeffery, K. (2006, October). Container scanning from a crane [Electronic Version]. *Digital Ship*, , 28. Retrieved March 9, 2008 from the World Wide Web: http://www.thedigitalship.com/DSmagazine/DigitalShipOct06.pdf.

Jones, S. M. (2006). *Maritme Security: A Pratical Guide*. London: The Nautical Institute, 202 Lambeth Road, London, SE1 7LQ, England.

Junzhong, B. (2005). Potential Application of AIS on Safety Environment Protection. *European Journal of Navigation, 3*(3), 28-31.

Kanev, D. (Ed.). (2005). *Seaborne trade effects of international terrorism and effectiveness of the anti-terrorist policy*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Kasperson, J. X., Kasperson, R. E., Pidgeon, N., & Slovic, P. (2003). *The Social amplification of risk: assessing fifteen years of research and theory*. Retrieved July 6, 2008, from the World Wide Web: http://books.google.com/books?hl=en&lr=&id=4Ry6ar929bMC&oi=fnd&pg=PR10&dq=social+amplification+of+risk+framework&ots=witOP9mDtr&sig=FmnZfRU62lVdLKoqs5tQLTq0cX8#PPP1,M1.

Koburger, C. W. (1986). *Vessel Traffic System* (First ed.). Maryland: Cornell Maritime press,1400 E. Clement Street Baltimore, MD 21230.

L-3 Communications. (2006, October). L-3 Communications to provide US security system [Electronic Version]. *Digital Ship*, , 28. Retrieved March 9, 2008 from the World Wide Web: http://www.thedigitalship.com/DSmagazine/DigitalShipOct06.pdf.

LNG tanker terrorism [Electronic (2007). Version]. *Jane's Terrorism & Security*. Retrieved July 6, 2008 from the World Wide Web: http://www.janes.com/news/security/terrorism/jtic/jtic070803_1_n.shtml.

Marcoyannis, G. (1988). Vessel Traffic Services(VTS) and its contribution to risk reduction. *Shipping*.

MarNIS Concept. Retrieved June 24, 2008, from the World Wide Web: http://www.marnis.org/?page=18

MarNIS Information Centre. (n.d.). Innovatory European Maritime Navigation Services (MarNIS): Concept to be Unveiled [Electronic Version]. Retrieved July 10, 2008 from the World Wide Web: http://www.marnis.org/filecontent/downloads/MarNIS%20explained.doc.

Mbiah, K. (2007). Unlawful acts in West African waters. In M. Q. Mejia & J. Xu (Eds.), *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea* (pp. 125-135). Malmö: WMU Publications

McNicholas, M. (2008). *Maritime Security: An Introduction*. Burlington: Butterworth-Heinemann, 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA.

Mejia, M. Q. (2003). Defining maritime violence and maritime security. In P. K. Mukherjee, M. Q.Mejia & G. M. Gauci (Eds.), *Proceedings of the International symposium for Maritime Violence and other Security issues at Sea* (pp. 27-38). Malmö, Sweden: WMU Publications

Mejia, M. Q. (2003). Maritime Gerrymandering: Dilemmas in Defining Piracy, Terrorism and other Acts of Maritime Violence. *International Commertial Law, 2*(2), 153-175.

Mejia, M. Q. (2007). *Law and Ergonomics in Maritime Security, PhD Thesis*: Department of Design Science, Lund University, 221 00 Lund, Sweden.

Mensah, T. A. (2005). The ISPS Code and the international regime to protect maritime security. In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 1-8). Malmö: WMU Publications

Michel, K. (2006). War, piracy and terror: thr high seas in the 21st century. *The Journal of International Maritime Law, 12*, 313-324.

Mitropoulos, E. (2007, March). E-navigation: a global resource. *Seaways*, 7-8.

Mitropoulos, E. E. (2005). IMO-moving with the times. *Bimco Review*, 170-173.

Mitsatsos, D. C. (2005). An industry perspective on ISPS Code implementation. In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 265-275). Malmö, Sweden: WMU Publications

Mortensen, N. B., & Rasmussen, P. L. (2003). Substandard shipping - the curse of modern shipping. *Bimco Review*, 198-203.

Mukherjee, P. K., & Mejia, M. (2004a). Selected Issues of Law and Ergonomics in Maritime Security. *The Journal of International Maritime Law, 10*(4), 316-326.

Mukherjee, P. K., & Mejia, M. (2004b). Selected issues of law and ergonomics in maritime security. *Journal of International Maritime Law, 10*(4).

Mukherjee, P. K., & Mejia, M. Q. (2005). The ISPS Code: legal and ergonomic considerations. In M. Q. Mejia (Ed.), *Proceedings of the International*

symposium for Contemporary Issues in Maritime Security (pp. 33-51). Malmö: WMU Publications

New Port Security for Asia. (2008, July). *Safety at Sea International,* 13.

Nikitin, M. B. (2008, February 4). *CSR Report for US Congress: Proliferation Security Initiative (PSI).*

Nincic, D. J. (2005, October 24-26). *Maritime terrorism and developing case study for teaching and analysis: an interim report.* Paper presented at the 6th Annual General Assembly and Conference of International Association of Maritime Universities(IAMU), World Maritime University, Malmö, Sweden.

Nincic, D. J., & Clark, B. The Utility of Risk Assessment Tools in Maritime Security Analysis [Electronic Version]. *International Association of Maritime Universities*. Retrieved April 1, 2008 from the World Wide Web. http://www.iamu-edu.org/generalassembly/aga7/projectsession/28_TheUtilityofRisk.pdf.

Ong-Webb, G. G. (2006a). *Piracy, Maritime Terrorism and Securing the Malacca Straits*. Singapore: Institute of Southeast Asian studies, 30 Heng Mui Keng Terrace, Pasir Panjang.

Ong-Webb, G. G. (2007). Piracy in Maritime Asia: Current Trends. In P. Lehr (Ed.), *Violence at Sea: Piracy in the age of Global Terrorism* (pp. 37-93). New York: Taylor & Francis Group, 270 Madison Avenue, NY 10016.

Ong-Webb, G. G. (Ed.). (2006b). *Southeast Asian Piracy: Research and developments*. Singapore: Institute of Southeast Asian Studies, 30 Heng Mui Keng Terrace, Pasir panjang, Singapore 119614.

Osler, D. (Monday, June 2, 2008). Pirates' payday. *Lloyd's List*.

Othman, E., & Halawa, A. (Eds.). (2005). *Towards effective implementation of the ISPS Code onboard ships*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Özçayir, Z. O. (2003). War, piracy and terror: thr high seas in the 21st century. *The Journal of International Maritime Law, 9*(6), 578-582.

Patel-Predd, P. (2008). Smarter, Faster Nano Sensor: A tiny detector can quickly sniff out dangerous gases [Electronic Version]. *Technology Review*. Retrieved August 6, 2008 from thw World Wide Web: http://www.technologyreview.com/Nanotech/20976/page1/.

Patraiko, D. (2007, March). Introducing the e-navigation revolution. *Seaways,* 5-8.

Peleg-Gillai, B., Bhat, G., & Sept, L. (2006). Innovators in Supply Chain Security: Better Security Drives Business Value: The Manufacturing Institute, 1331 Pennsylvania Avenue, NW • Washington, DC 20004-1790.

Perry, M. (June 25, 2008). Ship terrorism alert system seen flawed*. International Herald Tribune*.

Pettersson, B. (2003). The Implementation of AIS-Automatic Identification System. *European Journal of Navigation, 1*(2), 49-53.

Piracy on the rise, but terrorism link not seen: Study. (2008, June 4). *The Economic Times*.

Prakash, J. (2008, January 10). Somali pirates are tied to Dubai. *Fairplay, 362,* 10.

Proliferation Security Initiative. (2003). Retrieved August 13, 2008, from the World Wide Web: http://usinfo.state.gov/products/pubs/proliferation/

Raymond, C. Z. (Ed.). (2005). *Maritime Terrorism, A Risk Assesment: The Australian Example*. Singapore: Institute of Defence and Strategic Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798.

ReCAAP Agreement. (2006). *Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia*. Retrieved July 7, 2008, from the Worls Wide Web: http://www.recaap.org/about/pdf/ReCAAP%20Agreement.pdf.

Richard, R. (2004, June28, 2004). *VTS: an Aid To Navigation.* Paper presented at the 17th Congress of International Maritime Pilots' Association Istanbul.

Richardson, M. (2004). *A Time Bomb for Global Trade*. Singapore: Institute of Southeast Asian Studies, 30 Heng Terrace, Pasir Panjang.

Richardson, M. (2007). The terrorist threat to shipping. In M. Q. Mejia & J. Xu (Eds.), *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea* (pp. 51-59). Malmö: WMU Publications

Rs 500-cr cocaine seizure at JNPT (2004, June 5). Retrieved July 26, 2008, from the World Wide Web: http://www.thehindubusinessline.com/2006/06/05/stories/2006060502320500.htm

S.M.Jones. (2006). *Maritime Security: A Practical Guide*. London: The Nautical Institute, 202 Lambeth Road, London, SEI 7LQ, England.

Safety of life at Sea. (2004 ed.). London: International Maritime Organisation 1974.

Safety of Life at Sea (1974). London: International Maritime Organisation, 1974.

Safety of Life at Sea (1974). (2004 ed.): IMO(1974).

Sakhuja, V. (2007). Sea Piracy in South Asia. In P. Lehr (Ed.), *Violence at Sea: Piracy in the age of Global Terrorism* (pp. 23-36). New York: Taylor & Francis Group, 270 Madison Avenue, NY 10016.

Sandler, M., Gern, T., & Zimmermann, R. (2003). Integration of Inland ECDIS, RADAR and AIS. *European Journal of Navigation, 1*(2), 78-82.

Schröder, J.-U. (2005). An Introduction to Shipboard Security Risk Assessment, . In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 101-116). Malmö, Sweden: WMU Publications

Schröder, J.-U. (2006). Seminar on Maritime Casualty investigations: World Maritime University, Malmö.

Secure-Ship Retrieved July 17, 2008, from the World Wide Web: http://www.icc-ccs.org/prc/piracyreport.php

Sheen, R. (2007, January). Fatigue and an alternative watch system [Electronic Version]. *Alert*, 8. Retrieved March 9, 2008 from the World Wide Web: http://www.he-alert.org/user/download.asp.

Shipping and World Trade : Key facts. Retrieved April 19, 2008, from World Wide Web http://www.marisec.org/shippingfacts//worldtrade/index.php?SID=7b13f84c271e024c372544c682f31831

Sklet, S. (2006). Safety barriers: Definition, classification, and performance *Journal of Loss Prevention in the Process Industries Volume 19*(Issue 5), Pages 494-506.

Somali pirates are tied to Dubai. (2008, January 3). *Fairplay, 362*, 12.

SPO-20 is the only real-time people screening of its kind in the world. Retrieved March 7, 2008, from the World Wide Web: http://www.qinetiq.com/home/products/spo_20.html

Stewart, C. (2008, June 23). Terror warning system 'useless'. *The Australian*.

Thucydides (Ed.). (2006). *The History of the Peloponnesian war*. New York: Barrnes & Noble books, 122 Fifth Avenue, new York, NY 10011.

Timlen, T. (2002). Security - not just an owner's problem. *Bimco Review*, 244-247.

Timlen, T. (2005). The broadening the scope of maritime security. *Bimco Review*, 182-183.

Tomberlin, R. L. (2008). Terrorism's Effect on Maritime Shipping [Electronic Version], 1-16. Retrieved July 3, 2008 from the World Wide Web: http://www.maritimeterrorism.com/wp-content/uploads/2008/07/terrorisms-effect-on-maritime-shipping.pdf.

Trelawny, C. Containerised cargo security - a case for "joined-up" government [Electronic Version], 5. Retrieved July 28, 2008 from the World Wide Web: http://www.imo.org/includes/blastDataOnly.asp/data_id%3D17982/Containerised.pdf.

Trelawny, C. (2003). *IMO Activities to Enhance Maritime Security.* Paper presented at the Expert Meeting on the Development of Multimodal Transport and Logistics Services, Geneva, 24-26 September 2003.

Trelawny, C. (2005). *Maritime Security: Implementation of the ISPS Code.* Paper presented at the 3rd Intermodal Africa 2005 Tanzania Exhibition and Conference, 3 to 4 February 2005, Dar es Salaam.

Tsamenyi, M., & Palam, M. A. (2007). Legal considerations in the implementation of long-range identification and tracking systems for vessels. *Journal on International Maritime Law, 13*, 42-55.

U.S. Customs and Border Protection. (2006a). *Container Security Initiative, 2006–2011 Strategic Plan*. Retrieved July 11, 2008. from thw World wide Web: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_strategic_plan.ctt/csi_strategic_plan.pdf.

U.S. Customs and Border Protection. (2006b). *Supply Chain Security Best Practices Catalog*. Retrieved July 23, 2008, from the World Wide Web: http://www.customs.gov/linkhandler/cgov/trade/cargo_security/ctpat/ctpat_members/ctpat_best_practices.ctt/ctpat_best_practices.pdf.

UAV tested for patrols over northern waters. (2008, May 23). *The Australian News* Retrieved May 21, 2008, from The World wide web: http://www.theaustralian.news.com.au/story/0,25197,23745612-2702,00.html

UK P & I Club. (2003,October). Just Waiting to Happen ...The work of the UK P&I Club [Electronic Version]. *Alert*, , 8. Retrieved March 9, 2008 from the World Wide Web: http://www.he-alert.org/user/download.asp.

UNCTAD. (2007). *Review of Maritime Transport 2007*.

United Kingdom Hydrographic Office. (2008). The Human Face of ECDIC: Updating the Admiralty Way [Electronic Version]. *Admiralty World*, 11. Retrieved July 14, 1008 from the World Wide Web: http://www.admiraltyworld.co.uk/.

United Nations. History of United Nation. Retrieved July 05, 2008, from the World Wide Web: http://www.un.org/aboutun/unhistory/

United Nations. Security Council discusses Terrorism. Retrieved February 10, 2008, from the World Wide Web: http://www.un.org/sc/ctc/

United Nations. (2001). Security Council Resolution 1373 adopted on September 28, 2001. Retrieved February 10, 2008, from the World Wide Web: http://daccessdds.un.org/doc/UNDOC/GEN/N01/557/43/PDF/N0155743.pdf?OpenElement

United Nations. (2004). Security Council Resolution 1535 adopted on March 26, 2004. Retrieved February 10, 2008, from the World Wide Web: http://daccessdds.un.org/doc/UNDOC/GEN/N04/286/41/PDF/N0428641.pdf?OpenElement

United Nations. (2006). Adopting a Global Counter-Terrorism Strategy. Retrieved February 10, 2008, from the World Wide Web: http://www.un.org/terrorism/framework.shtml

United Nations. (2008, June 2). *Security Council Condemns Acts of Piracy, Armed Robbery off Somalia's Coast, Authorizes for Six Months 'All Necessary Means' To Repress Such Acts.* Retrieved June 25, 2008, from the World Wide Web: http://daccessdds.un.org/doc/UNDOC/GEN/N08/361/77/PDF/N0836177.pdf?OpenElement.

United Nations Conference on Trade and Development. (2008). Version]. *UNCTAD Transport Newsletter*, 28. Retrieved August 14, 2008 from the World Wide Web: http://www.unctad.org/en/docs/sdtetlbmisc20081_en.pdf.

US Government. (January 2008). World Oil Transit Chokepoints. Retrieved June 28, 2008, from the World Wide Web: http://www.eia.doe.gov/cabs/World_Oil_Transit_Chokepoints/pdf.pdf

US Government Accountability Office. (2008, June 17). Port Security: Government Accountability Office(GAO) cites challenges for 100 percent scanning of U.S.-bound cargo containers. Retrieved July 1, 2008, from the World Wide web: http://www.logisticsmgmt.com/article/CA6570296.html?industryid=48468

US ID card scheme begins [Electronic (2007, April). Version]. *Digital Ship*, , 28. Retrieved March 9, 2008 from the World Wide Web: http://www.thedigitalship.com/DSmagazine/dsapr07rr.pdf.

Valencia, M. J. (Ed.). (2006). *The Politics of Anti-Piracy and Anti-Terrorism Responses in Southeast Asia*. Singapore: Institute of Southeast Asian Studies, 30 Heng Mui Keng Terrace, Pasir panjang, Singapore 119614.

VTMS can track pirates. (2008). *Safety at Sea International*.

Warrick, J. (2003, August 14). On North Korean Freighter, a Hidden Missile Factory. *Washington Post*

Weeks, S. B. (Ed.). (2005). *New Initiatives for Maritime Cooperation*. Singapore: Institute of Defence and Strategic Studies, Nanyang Technological University, Block S4, Level B4, Nanyang Avenue, Singapore 639798.

Wheater, P. (2008, June). Sitting targets. *Safety at Sea International, 42,* 52-53.

White, P. (2003, March 25-26). *Improving Maritime and Port Security.* Paper presented at the International Conference : Passenger Ship Safety, London, UK.

Wilson, N. (2008, January 11). US LNG tankers vulnerable to attack. *The Australian Business*.

World Custom Organisation. Profile. Retrieved July 14,, 2008, from the World Wide Web: http://www.wcoomd.org/home_about_us_our_profile.htm

World Travel & Tourism Council, International Hotel & Restaurant Association, International Federation of Tour Operators, International Council of Cruise Lines, & United Nations Environment Programme. (2002). *Industry as a partner for sustainable development: Tourism*: United Nations Environment Programme,Division of Technology, Industry and Economics,39-43 Quai André Citroën, 75739 Paris Cedex 15,France.

Yilmazel, M., & Asyali, E. (Eds.). (2005). *An analysis of port state control inspections related to the ISPS Code*. UK: WIT Press, Ashurst Lodge, Ashurst, Southampton, SO40 7AA.

Appendix A

Questionnaire

Personal Declaration

Sir/Madam,

I am studying for a master's degree in maritime affairs at the World Maritime University in Malmö, Sweden, affiliated to the International Maritime Organization and writing a dissertation entitled, "*The role of technology in fostering maritime security: a survey of its development, application, and adequacy*".

In recent years, maritime security issues have been the top priority in the working at IMO. However, there is lot which needs to be done so that we can make the maritime sector secure. The maritime industry has introduced the state of art equipment for enhancing maritime security. However, still breach in security has been taking place. The dissertation is an effort to determine how technology in the maritime industry can be efficiently and effectively utilized to foster maritime security.

I will be much obliged if you could complete the questionnaire below to the best of your belief and knowledge. The filled-in questionnaire will be treated with the strictest confidentiality and used purely for academic purposes.

Thank you.

Yours sincerely,

Bhim Singh Kothari
Student no. s08075
MSEA Specialization
World Maritime University, Malmö, Sweden

Note: - You are kindly requested to answer the questions with your own opinion on basis of your personal experience gained while working in the maritime field. The questionnaire has been framed for three groups, namely

Maritime Administration officials who are responsible for overall administration and legal aspects of the maritime sector within a Flag Administration,

The second group of people is responsible for enforcing National Maritime Legislation in their maritime zones such as Coast Guard, Navy, Maritime Security Agency (MSA) and Marine Police, and

The third group of people is Ships Masters, Shipping Companies, Organizations working for the Maritime Sector and Shipping Associations.

MARITIME ADMINISTRATION

Country in which you are working
Q1. Is your country signatory to? (a) UNCLOS ☐ Yes ☐ No (b) SOLAS ☐ Yes ☐ No (c) SUA ☐ Yes ☐ No (d) STCW ☐ Yes ☐ No (e) ILO Convention No. 185 [Seafarers Identity Document (SID)] ☐ Yes ☐ No
Q2. Do you feel, in the present day scenario there is a need to enhance maritime security? ☐ Yes ☐ No ☐ No response
Q3. In your opinion, which crime poses the greatest threat to the maritime sector? ☐ Piracy and Armed robbery against ships. ☐ Maritime Terrorism ☐ Drug Trafficking ☐ Illegal migration ☐ Stowaways ☐ Human Trafficking ☐ Container crimes ☐ Others
Q4. In your opinion, are the instruments adopted by IMO adequate to combat the above maritime crimes? ☐ Yes ☐ No ☐ No response
Q5. In your Flag Administration is the same agency responsible for providing maritime security in ports, anchorage area, and ships outside port jurisdiction? ☐ Yes ☐ No ☐ No response
Q6. How frequently does the maritime administration interact for maritime security issues with Law enforcement agencies? Tick your answer(only one)

☐ Daily basis ☐ Weekly basis ☐ Monthly basis ☐ Quarterly basis ☐ Half yearly basis ☐ Yearly basis ☐ No interaction
Q7. How are the data listed below being shared between the Flag Administration and maritime law enforcement agency? Requirement basis ☐ Ship Reporting ☐ AIS ☐ Ship entering/leaving ports Online ☐ Ship Reporting ☐ AIS ☐ Ship entering/leaving ports No exchange of data ☐ Ship Reporting ☐ AIS ☐ Ship entering/leaving ports My country does not have the system ☐ Ship Reporting ☐ AIS ☐ Ship entering/leaving ports
Q8. Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? Ports ☐ Yes ☐ No ☐ No Comment Ships ☐ Yes ☐ No ☐ No Comment Other installations ☐ Yes ☐ No ☐ No Comment
Q9. How does your organization motivate its staff to comply with security guidelines? ☐ Financial incentive, such as, reward money / out of turn promotion ☐ Recognition in public, by giving certificate or insignia ☐ Other incentives or than above ☐ mentioned ☐ No response
Q10. Are the present manning levels onboard your flagships adequate to comply with security regulations? ☐ Yes ☐ No ☐ No response
Q10. Present trend shows that certain flag state administration issue safe manning certificates without giving due attention to vessels trading, administrative work onboard and security requirements. Keeping in mind the present security scenario in the world, do you feel IMO should play more active role with regard to safe manning of ships? ☐ Yes ☐ No ☐ No response
Q11. How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security? ☐ Effective ☐ Not Effective ☐ No response
Q12. Have you dealt with a security incident in your place of work? ☐ Yes ☐ No ☐ No response
Q13. How would you rate the response of Maritime Administration / Maritime Law Enforcement agencies in the above incident(s)? ☐ Effective ☐ Inadequate ☐ No response
Q14. Is Vessel Traffic System (VTS) fostering security or is it a hindrance?

☐ Effective for security ☐ Hindrance for security ☐ No response
Q15. Is VTS a deterrent or an active measure for mitigating security threat? ☐ Deterrent ☐ Active measure ☐ No response
Q16. Will interfacing of radar with AIS enhance the operator efficiency in early identification and prevention security incident from occurring? ☐ Yes ☐ No ☐ No response
Q17. Will long-range identification and tracking of ships (LRIT) foster the objective of secure shipping or will be a hindrance? ☐ Foster maritime security ☐ Will be a hindrance ☐ No response
Q18. Do you have any experience in security scanning of containers? ☐ Yes ☐ No ☐ No response
Q19. Taking into consideration the security risk and commercial commitment of ship owners, what in your opinion would be the best solution for enhancing maritime security will be? ☐ Random scanning ☐ 100% scanning ☐ No response
Q20. There are different ship reporting systems worldwide, such as Automated Mutual-Assistance Vessel Rescue system (AMVER), Japanese Ship Reporting System (JASREP), Indian (Maritime) Search and Rescue Computerized Ship Reporting System (INDSAR) etc. In your opinion, reporting into any one of these systems facilitate rendering of early assistance to ships threatened by a maritime security incident? ☐ Yes ☐ No ☐ No response
Q21. In your opinion should reporting to any one of the world wide ship reporting systems be made mandatory for all ships on international voyages? ☐ Yes ☐ No ☐ No response
Q22. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to training? ☐ Yes ☐ No ☐ No response
Q23. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to analysis? ☐ Yes ☐ No ☐ No response
Q24. Would you like to add any comments regarding your experience with maritime security that has not been covered in this questionnaire? Comments:

Maritime Law Enforcement Agencies

Country in which you are working							
Q1. Do you feel, in the present day scenario there is a need to enhance maritime security? ☐ Yes ☐ No ☐ No response							
Q2. In your opinion, which crime poses the greatest threat to the maritime sector?							
☐ Piracy and	☐ Maritime	☐ Drug	☐ Illegal	☐ Stowaways	☐ Human	☐ Container	☐ Others

Armed robbery Terrorism Trafficking migration Trafficking crimes against ships.
Q3. In your opinion, are the instruments adopted by IMO adequate to combat the above maritime crimes? Yes No No response
Q4. How frequently does the maritime administration interact for maritime security issues with Law enforcement agencies? Tick your answer(only one) Daily basis Weekly basis Monthly basis Quarterly basis Half yearly basis Yearly basis No interaction
Q5. How are the data listed below being shared between the Flag Administration and maritime law enforcement agency? Requirement basis Ship Reporting AIS Ship entering/leaving ports Online Ship Reporting AIS Ship entering/leaving ports No exchange of data Ship Reporting AIS Ship entering/leaving ports My country does not have the system Ship Reporting AIS Ship entering/leaving ports
Q6. Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? Ports Yes No No Comment Ships Yes No No Comment Other installations Yes No No Comment
Q7. As a maritime law enforcement agency, do you have access to the data bank for the ships registered in your country? Yes No No response Q8. How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security? Effective Not Effective No response
Q9. Have you dealt with a security incident in your place of work? Yes No No response
Q10. How would you rate the response of Maritime Administration / Maritime Law Enforcement agencies in the above incident(s)? Effective Inadequate No response
Q11. Is Automatic Identification System (AIS) fostering security or is it a hindrance? Effective for security Hindrance for security No response
Q12. Is Vessel Traffic System (VTS) fostering security or is it a hindrance?

☐ Effective for security ☐ Hindrance for security ☐ No response
Q13. Is VTS a deterrent or an active measure for mitigating security threat? ☐ Deterrent ☐ Active measure ☐ No response
Q14. Will mandatory reporting to Vessel Traffic System (VTS) enhance overall security in the area? ☐ Yes ☐ No ☐ No response
Q15. Will interfacing of radar with AIS enhance the operator efficiency in early identification and prevention security incident from occurring? ☐ Yes ☐ No ☐ No response
Q16. Will long-range identification and tracking of ships (LRIT) foster the objective of secure shipping or will be a hindrance? ☐ Foster maritime security ☐ Will be a hindrance ☐ No response
Q17. Do you have any experience in security scanning of containers? ☐ Yes ☐ No ☐ No response
Q18. Taking into consideration the security risk and commercial commitment of ship owners, what in your opinion would be the best solution for enhancing maritime security will be? ☐ Random scanning ☐ 100% scanning ☐ No response
Q19. There are different ship reporting systems worldwide, such as Automated Mutual-Assistance Vessel Rescue system (AMVER), Japanese Ship Reporting System (JASREP), Indian (Maritime) Search and Rescue Computerized Ship Reporting System (INDSAR) etc. In your opinion, reporting into any one of these systems facilitate rendering of early assistance to ships threatened by a maritime security incident? ☐ Yes ☐ No ☐ No response
Q20. In your opinion should reporting to any one of the world wide ship reporting systems be made mandatory for all ships on international voyages? ☐ Yes ☐ No ☐ No response
Q21. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to training? ☐ Yes ☐ No ☐ No response
Q22. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to analysis? ☐ Yes ☐ No ☐ No response
Q23. Would you like to add any comments regarding your experience with maritime security that has not been covered in this questionnaire? Comments:

SHIPS MASTERS / SHIPPING COMPANIES / SHIPPING ASSOCIATIONS

Country in which you are working
Q1. Do you feel, in the present day scenario there is a need to enhance maritime security? ☐ Yes ☐ No ☐ No response
Q2. In your opinion, which crime poses the greatest threat to the maritime sector?

☐ Piracy and Armed robbery against ships. ☐ Maritime Terrorism ☐ Drug Trafficking ☐ Illegal migration ☐ Stowaways ☐ Human Trafficking ☐ Container crimes ☐ Others
Q3. In your opinion, are the instruments adopted by IMO adequate to combat the above maritime crimes? ☐ Yes ☐ No ☐ No response
Q4. Is the technology required under different IMO instruments effective in fostering maritime security in the area of the maritime sector listed below? Ports ☐ Yes ☐ No ☐ No Comment Ships ☐ Yes ☐ No ☐ No Comment Other installations ☐ Yes ☐ No ☐ No Comment
Q5. How does your organization motivate its staff to comply with security guidelines? ☐ Financial incentive, such as, reward money/ out of turn promotion ☐ Recognition in public, by giving certificate or insignia ☐ Other incentives or than above ☐ mentioned No response
Q6. Are the present manning levels onboard your flagships adequate to comply with security regulations? ☐ Yes ☐ No ☐ No response
Q7. Present trend shows that certain flag state administration issue safe manning certificates without giving due attention to vessels trading, administrative work onboard and security requirements. Keeping in mind the present security scenario in the world, do you feel IMO should play more active role with regard to safe manning of ships? ☐ Yes ☐ No ☐ No response
Q8. How effective do you think the role of Ship Security Alarm System (SSAS) is in promoting maritime security? ☐ Effective ☐ Not Effective ☐ No response
Q9. Have you dealt with a security incident in your place of work? ☐ Yes ☐ No ☐ No response
Q10. How would you rate the response of Maritime Administration / Maritime Law Enforcement agencies in the above incident(s)? ☐ Effective ☐ Inadequate ☐ No response
Q11. Is Automatic Identification System (AIS) fostering security or is it a hindrance? ☐ Effective for security ☐ Hindrance for security ☐ No response
Q12. Is Vessel Traffic System (VTS) fostering security or is it a hindrance? ☐ Effective for security ☐ Hindrance for security ☐ No response
Q13. Is VTS a deterrent or an active measure for mitigating security threat?

☐ Deterrent ☐ Active measure ☐ No response
Q13. Will mandatory reporting to Vessel Traffic System (VTS) enhance overall security in the area? ☐ Yes ☐ No ☐ No response
Q14. Will interfacing of radar with AIS enhance the operator efficiency in early identification and prevention security incident from occurring? ☐ Yes ☐ No ☐ No response
Q15. Will long-range identification and tracking of ships (LRIT) foster the objective of secure shipping or will be a hindrance? ☐ Foster maritime security ☐ Will be a hindrance ☐ No response
Q16. Do you have any experience in security scanning of containers? ☐ Yes ☐ No ☐ No response
Q17. Taking into consideration the security risk and commercial commitment of ship owners, what in your opinion would be the best solution for enhancing maritime security will be? ☐ Random scanning ☐ 100% scanning ☐ No response
Q18. There are different ship reporting systems worldwide, such as Automated Mutual-Assistance Vessel Rescue system (AMVER), Japanese Ship Reporting System (JASREP), Indian (Maritime) Search and Rescue Computerized Ship Reporting System (INDSAR) etc. In your opinion, reporting into any one of these systems facilitate rendering of early assistance to ships threatened by a maritime security incident? ☐ Yes ☐ No ☐ No response
Q19. In the present security scenario, will you prefer that your ship's position be monitored by law enforcement agencies? ☐ Yes ☐ No ☐ No response
Q20. In your opinion should reporting to any one of the world wide ship reporting systems be made mandatory for all ships on international voyages? ☐ Yes ☐ No ☐ No response
Q21. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to training? ☐ Yes ☐ No ☐ No response
Q22. Does the Vessel Data Recorder (VDR) add value to maritime security with regard to analysis? ☐ Yes ☐ No ☐ No response
Q23. Would you like to add any comments regarding your experience with maritime security that has not been covered in this questionnaire? Comments:

APPENDIX B

CRONOLOGICAL ORDER OF SELECTED MARITIME CRIME

1. Seizure of Santa Maria on January 24, 1961
2. Cambodian seizure of Mayaguez on May 12, 1975
3. Episode of Achille Lauro incident on, October 7, 1985
4. Hijacking of City of Poros on July 11, 1988.
5. Hijacking of MV Petro Ranger by pirates in the South China Sea carrying $2.3 million worth cargo of diesel oil and jet fuel on April 17, 1998.
6. Hijacking of MV Cheung Son on November 19, 1998.
7. Confiscation of assembly line for ballistic missiles from North Korean freighter Kuwolsan by Indian customs on June 30, 1999.
8. Capturing of Hijacked pirated ship MV Alondra Rainbow, by Indian Coast Guard on November 16, 1999.
9. Attacks on U.S. Navy guided missile destroyer USS Cole October 12, 2000.
10. Bombing of Our Lady of Mediatrix on December 8, 2000.
11. Apprehension of Al Murtada by Indian Coast Guard, July 3, 2002.
12. Suicide attack on Limburg in October 6, 2002.
13. Hijacking of Oil Tanker Penrider in August 2003.
14. Sabotage of Super Ferry 146 by Abu Sayyaf group February 2004.
15. Explosion at port Ashdod in Israel by suicide bombers in March 14, 2004.
16. Terrorist acts at Umm Qasr8 near Basra in Apr 2004.
17. Bomb blast onboard Philippines ferry Dona Ramona August 30, 2005.

Sources:

(a) Jayant Abhyankar(2005) Maritime crime, In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (pp. 201-243). Malmö: WMU Publications.

(ii) Mejia, M. Q. (2003). Defining maritime violence and maritime security. In P. K. Mukherjee, M. Q.Mejia & G. M. Gauci (Eds.), *Proceedings of the International symposium for Maritime Violence and other Security issues at Sea* (pp. 27-38). Malmö, Sweden: WMU Publications

(iii) Mejia, M. Q. (2007). *Law and Ergonomics in Maritime Security, PhD Thesis*: Department of Design Science, Lund University, 221 00 Lund, Sweden.

(iv) S.M.Jones. (2006). *Maritime Security: A Practical Guide*. London: The Nautical Institute, 202 Lambeth Road, London, SEI 7LQ, England.

APPENDIX C

CONSEQUENCES OF DISRUPTING WORLD OIL TRANSIT CHOKEPOINTS

Important World Oil Transit Chokepoints						
Name	2006 E Oil Flow (bbl/dl)	Width at Narrowest Point	Oil Source Origin	Primary Destination	Past Disturbances	Alternative Routes
The Straits of Hormuz	16.5 – 17 million	21 miles	Persian Gulf Nation including Saudi Arabia, Iran and UAE	Japan, The United States, Western Europe, other Asian Countries	Sea mines were installed during Iran-Iraq War 1980s. Terrorist threat post September 11,2001	745 mile long East-West pipeline throughout Saudi Arabia to the Red Sea
The Strait of Malacca	15 million	1.7 miles	Persian Gulf Nations, West Africa	All Asia/Pacific consumers including Japan and China	Descriptions from pirates are a constant threat, including a terrorist attack in 2003. Collision and oil spills are also a problem. Poor visibility from smoke haze	Reroute through the Lombok or Sunda Strait in Indonesia. Possible pipeline construction between Malaysia and Thailand.
The Suez canal/ Sumed Pipeline	4.5 million	1000 feet	Persian Gulf Nations, especially Saudi Arabia, and Asia	Europe and The United States	Suez Canal was closed for eight years after the Six-Day War in 1967. Two large oil tankers ran aground in 2007 suspending traffic	Reroute around the southern tip of Africa (the Cape of Good Hope); additional 6000 miles
Bab El Mandab	3.3 million	18 miles	The Persian Gulf	Europe and The United States	USS Cole attack in 2000, French oil tanker in 2002, both attacks off the coast of	Northbound traffic can use the East-West oil pipeline through Saudi Arabia; Reroute around

					Aden, Yemen	the southern tip of Africa (the Cape of Good Hope); additional 6000 miles
The Turkish Straits	2.4 million	0.5 mile	Caspian Sea Region	Western and Southern Europe	Numerous past shipping accidents due to the straits sinuous geography. Some terrorist threats were made after September 11, 2001.	No clear alternative; potential pipelines discussed including a 173-mile pipeline between Russia; Bulgaria, and Greece.
The Panama Canal	0.5 million	110 feet	The United States	The United States, and other Central American countries	Suspected terrorist target	Reroute around Straights of Magellan, Cape Horn and Drake passage; additional 8,000 miles

Source: Data from Energy Information Administration: Official Energy statistics from the US Government. Retrieved on 28 June 2008 from http://www.eia.doe.gov/cabs/World_Oil_Transit_Chokepoints/pdf.pdf

APPENDIX D

MARITIME TERRORISM INCIDENTS

Ships			
Year	**Vessels Name**	**Nature of attack**	**Fatalities / Nature of loss or Damage**
1961	Santa Maria	Hijacking	1 killed
1974	Vory	Hijacking	--------
1979	Haleha Baru Adal	Hijacking	03 killed
1985	Achille Lauro	Hijacking	1 killed
1985	Rainbow Warrior	Explosion by 02 Limpet mines	1 killed and Ship Sank
1988	City of Poros	Direct shipboard attack	9 killed and 98 wounded
1995	Irish Mona	Hijacking	Nil
2000	Our Lady of Mediatrix	Bombing	40 killed and 50 wounded
2000	USS Cole	Suicide boat attack	17 Killed and 39 injured
2001	Silk Pride	Suicide boat attack	10 killed
2002	Limburg	Suicide boat attack	1killedand 90,000 barrels oil spilled
2004	Superferry 14	Bombing	118 killed
2005	one barge and two other ships(INDIA)	detonated several improvised explosive devices (IEDs)	All three ships damaged
2005	Ferry Dona Ramona	Explosion onboard	30 Killed
Port Facilities			
2004	Port of Ashdod, Israeli	Bomb Explosion	10 killed and 16 wounded
2007	Port Harcourt, Nigeria	20 armed assailants in speedboats	9 killed, approximately $31,000 US cash stolen
Off Shore Installations			
2004	Basra oil terminal (ABOT)& Khawr Al'Amaya (KAAOT) oil terminals in the	Suicide boat attack	3 killed

	Persian Gulf in the Persian Gulf		
2008	Royal Dutch Shell's Bonga platform in the Gulf of Guinea,	Firing automatic weapons from speedboats.	Temporarily shut down of Production.

Sources:

(b) Chalk, P. (2008). *The Maritime Dimension of International Security: terrorism, piracy, and challenges for the United States*. Santa Monica: RAND Corporation 1776 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138.

(ii) Daly, J. (2008). Terrorism and Piracy: The Dual Threat to Maritime Shipping. *Terrorism Monitor, VI* (16), 4-7.

(iii) Mejia(2005) Contemporary Issues in Maritime Security. In M. Q. Mejia (Ed.), *Proceedings of the International symposium for Contemporary Issues in Maritime Security* (p. ix,). Malmö: WMU Publications.

(iv) Mejia, M. Q. (2007). *Law and Ergonomics in Maritime Security, PhD Thesis*: Department of Design Science, Lund University, 221 00 Lund, Sweden.

(v) Menefee(2007) Terrorism and the slave trade: an analogy, In M. Q. Mejia & J. Xu (Eds.), *Proceedings of the International symposium for Coastal Zone Piracy and Other Unlawful Acts at Sea* pp61-78, Malmö: WMU Publications.

APPENDIX E

INTERNATIONAL CONVENTIONS AND PROTOCOLS ON TERRORISM

Convention	Signed at	Entered into Force	Number of Signatories
Convention on Offences and Certain Other Acts Committed On Board Aircraft	Tokyo on 14 September 1963	4 December 1969	182 Parties
Convention for the Suppression of Unlawful Seizure of Aircraft	The Hague on 16 December 1970	14 October 1971	185 Parties
Convention for the Suppression of Unlawful Acts Against the Safety of Civil Aviation	Montreal on 23 September 1971	26 January 1973	185 Parties
Convention on the Prevention and Punishment of Crimes against Internationally Protected Persons, including Diplomatic Agents	New York on 14 December 1973	20 February 1977	166 Parties
International Convention Against the Taking of Hostages	New York on 17 December 1979	3 June 1983	168 Parties
Convention on the Physical Protection of Nuclear Material	Vienna on 26 October 1979	8 February 1987	130 Parties
Amendments to the Convention on the Physical Protection of Nuclear Material	Vienna on 8 July 2005	Subject to ratification	
Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, done at Montreal on 23 September 1971	24 February 1988	6 August 1989	161 Parties
Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation	10 March 1988	1 March 1992	146 Parties
Protocol to the Convention for the Suppression of Unlawful	Adopted at London on 14		

Acts Against the Safety of Maritime Navigation	October 2005		
Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf	10 March 1988	1 March 1992	135 Parties
Protocol to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf	Adopted at London on 14 October 2005		
Convention on the Marking of Plastic Explosives for the Purpose of Detection	1 March 1991	21 June 1998	136 Parties
International Convention for the Suppression of Terrorist Bombings	New York on 15 December 1997	23 May 2001	153 Parties
International Convention for the Suppression of the Financing of Terrorism	9 December 1999	10 April 2002	160 Parties
International Convention for the Suppression of Acts of Nuclear Terrorism	New York on 13 April 2005	7 July 2007	29 Parties

(Information on status current as of 12 December 2007)

Source: Retrieved on 10 February 2008 from the World Wide Web: http://www.un.org/sc/ctc/law.shtml

APPENDIX F

AMENDMENTS FOR THE INSTRUMENTS, EQUIPMENT AND OTHER MEASURES

(a) Amending SOLAS Chapter XI to incorporating a new chapter XI-2 and the ISPS Code,

(b) Fitting of ship-borne Automatic Identification Systems (AIS) onboard ships of 500 gross tonnage and above, on international voyages by amending Regulation 19 of SOLAS Chapter V,

(c) Amending SUA Convention and adoption of new protocol,

(d) Fitting of ship security alert system (SSAS) for alerting authorities ashore of maritime security incident from sea,

(e) Developing performance standards and procedures for the above mentioned new fitment,

(f) Promulgating guidelines on SSAS through MSC/Circ.1072 on ‘Guidance on provision of ship security alert systems’ and MSC/Circ.1073 on ‘Directives for maritime rescue co-ordination centres (MRCCs) on acts of violence against ships’,

(g) Accelerating the process for implementation of long-range ships' identification and tracking system,

(h) Working on issues related to human element, manning of ships and shore leave for seafarers,

(i) Developing training guidelines and model courses for ship security officers, company security officers, port facility security officers and company, ship and port security personnel(Blanco-Bazán, Hesse, Jianxin, & Charalambous; Trelawny, 2005),

(j) Establishing a new sub-division in Maritime Safety Division at IMO for focusing on security matters. ("Enhanced Focus on Maritime Security in IMO Secretariat", 2007, August, p.23),

(k) Requiring permanent marking of IMO ships identification number on hull of the ship, and

(l) Requiring maintenance of a Continuous Synopsis Record onboard (Özçayir, 2003).

APPENDIX G

AIS INFORMATION SENT BY SHIPS

Information item	Information generation, type and quality of information
Static	
MMSI (Maritime Mobile Service Identity)	Set on installation. Note that this might need amending if the ship changes ownership.
Call sign and name	Set on installation. Note that this might need amending if the ship changes ownership.
IMO Number	Set on installation
Length and beam	Set on installation or if changed
Type of ship	Select from pre-installed list
Location of position-fixing antenna	Set on installation or may be changed for bi-directional vessels or those fitted with multiple antenna.
Dynamic	
Ship's position with accuracy indication and integrity status	Automatically updated from the position sensor connected to AIS. The accuracy indication is for better or worse than 10 m.
Position Time stamp in UTC	Automatically updated from ship's main position sensor connected to AIS.
Course Over Ground (COG)	Automatically updated from ship's main position sensor connected to AIS, if that sensor calculates COG. This information might not be available.
Speed Over Ground (SOG)	Automatically updated from the position sensor connected to AIS. This information might not be available.
Heading	Automatically updated from the ship's heading sensor connected to AIS.
Navigational status	Navigational status information has to be manually entered by the OOW and changed as necessary, for example: - underway by engines - at anchor - not under command (NUC) - restricted in ability to manoeuvre (RIATM) - constrained by draught - aground - engaged in fishing - underway by sail In practice, since all these relate to the COLREGs,

	any change that is needed could be undertaken at the same time that the lights or shapes were changed.
Rate of turn (ROT)	Automatically updated from the ship's ROT sensor or derived from the gyro. This information might not be available
Voyage-related	
Ship's draught	To be manually entered at the start of the voyage using the maximum draft for the voyage and amended as required (e.g. – result of de-ballasting prior to port entry)
Hazardous cargo (type)	To be manually entered at the start of the voyage confirming whether or not hazardous cargo is being carried, namely: DG (Dangerous goods) HS (Harmful substances) MP (Marine pollutants) Indications of quantities are not required
Destination and ETA	To be manually entered at the start of the voyage and kept up to date as necessary.
Route plan (waypoints)	To be manually entered at the start of the voyage, at the discretion of the master, and updated when required
To be manually entered at the start of the voyage, at the discretion of the master, and updated when required	Free format short text messages would be manually entered, addressed either a specific addressee or broadcast to all ships and shore stations

Source: Guidelines for the Onboard Operational Use of Ship borne Automatic Identification Systems (AIS), IMO Resolution A.917 (22), January 25, 2002.

Report rate of dynamic information

Type of ship	General reporting interval
Ship at anchor	3 min
Ship 0-14 knots	12 sec
Ship 0-14 knots and changing course	4 sec
Ship 14-23 knots	6 sec
Ship >23 knots	3 sec
Ship >23 knots and changing course	2 sec

Source: Guidelines for the Onboard Operational Use of Ship borne Automatic Identification Systems (AIS), IMO Resolution A.917 (22), January 25, 2002.