THE ISPS CODE AND MARITIME TERRORISM

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΝΑΓΟΠΟΥΛΟΥ ΜΑΡΙΑ

ΣΠΟΥΔΑΣΤΗΣ: ΓΚΑΡΑΣ ΒΑΣΙΛΕΙΟΣ

ΑΕΝ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΠΛΟΙΑΡΧΩΝ

ΑΚΑΔΗΜΑΪΚΟ ΕΤΟΣ 2021-2022

ΑΚΑΔΗΜΙΑ ΕΜΠΟΡΙΚΟΥ ΝΑΥΤΙΚΟΥ ΜΑΚΕΔΟΝΙΑΣ

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

ΕΠΙΒΛΕΠΩΝ ΚΑΘΗΓΗΤΗΣ: ΠΑΝΑΓΟΠΟΥΛΟΥ ΜΑΡΙΑ

ΘΕΜΑ:

THE ISPS CODE AND MARITIME TERRORISM

ΤΟΥ ΣΠΟΥΔΑΣΤΗ: ΓΚΑΡΑ ΒΑΣΙΛΕΙΟΥ
Α.Γ.Μ: 4509

Ημερομηνία ανάληψης της εργασίας:

Ημερομηνία παράδοσης της εργασίας:

Α/Α	*Ονοματεπώνυμο*	*Ειδικότης*	*Αξιολόγηση*	*Υπογραφή*
1	ΤΣΟΥΛΗΣ ΝΙΚΟΛΑΟΣ	ΔΙΕΥΘΥΝΤΗΣ ΣΧΟΛΗΣ ΠΛΟΙΑΡΧΟΣ Α'		
2	ΠΑΝΑΓΟΠΟΥΛΟΥ ΜΑΡΙΑ	ΚΑΘΗΓΗΤΡΙΑ ΑΓΓΛΙΚΩΝ		
3				
ΤΕΛΙΚΗ ΑΞΙΟΛΟΓΗΣΗ				

Ο ΔΙΕΥΘΥΝΤΗΣ ΣΧΟΛΗΣ : ΤΣΟΥΛΗΣ ΝΙΚΟΛΑΟΣ

CONTENTS

ABSTRACT

In the present work, the framework of the International Ship & Port Facility Security Code (ISPS Code) is outlined in conjunction with the phenomenon of Maritime Terrorism. The procedures that preceded the adoption of the ISPS Code by the International Maritime Organization (IMO) as well as the circumstances that made its conception and worldwide implementation a necessary act of Maritime Law, shall be mention thoroughly. The core, purpose and applicable clauses of the Code will be extensively documented, in a comprehensive way for the reader, while the requirements stipulated by its mandatory guidelines shall be described, leading to an effective Risk Management and the mutual Security of Ship & Port. In sequence, an amalgamation of the obligations imposed by the ISPS Code to Ship and Company, Port and Contracting Government will be diligently reported. Following, the process of ensuring the Ship's Security and the sequence of steps that are needed to be taken by the ship's personnel, performing their duty, as well as by the assisting Security Officers and Designated Authorities, will be consistently described. In addition, the role of the Master, Company Security Officer, Ship Security Officer and Port Facility Security Officer, with compliance to the Code, will be noted and their respective responsibilities outlined. Furthermore, the procedures entailed in the performance of a Port Facility's Security, with an emphasis to the Assessment of security threats and the Planning of security measures for mitigating or preventing the former, shall be detailed. Moreover, the Verifications and the endorsement of Certificates subjected to each ship, applicable by the Code, will be documented, along with a detail record of the Requirements imposed by the SOLAS Convention to every vessel for the purpose of the Safety of Navigation and the function of the International Maritime Law. Finally, in this paper, a briefing of the issue of Maritime Terrorism as a recent phenomenon, its legal entanglements and lack of authoritative definition and suppression in the name of International Law as well as its consequences and by extension its civil liabilities, will be mentioned.

Greek and International bibliography was used to culminate in the fundamentals that make up this work. Maritime organizations and companies, scientific papers by individual authors or research teams, government documents and conclusions were used to amalgamate the information that constitutes this project in the hope of approaching as best as possible the issue of the ISPS Code and Maritime Terrorism,

INTRODUCTION

In our modern era of worldwide commerce, the globalization of transportation and means of communication are in their apex with the output of technological development leading us in the process of becoming a more interconnected world. Nevertheless, this new age of novel opportunities and progress is impaired by unprecedented and previously unheard-of dangers which do not affect specific parts of the world in isolation, but have gravely impacted the security of the whole world. The threat of worldwide terrorism and especially the severity of the threat of maritime terrorism were not promptly realized by the international community nor were they adequately prepared to combat them. The necessity to reinforce maritime security, in our times, is universally demanded and acknowledged by states and the maritime industry alike, while the vital measures to fulfill this act within the framework of global transportation and international cooperation are in constant deployment and evaluation by intergovernmental organizations as the threats evolve and constantly change form themselves.

Concern about unlawful acts which imperiled the safety of ships and the security of their passengers and crews intensified during the 1980s, with reports of crews being kidnapped, ships being hi-jacked, deliberately run aground or blown up by explosives. Passengers were threatened and sometimes killed.

As a result of the Achille Lauro incident (a passenger ship hi-jacked by terrorists while on a cruise in the Mediterranean, off the coast of Egypt), in November 1985 the International Maritime Organization (IMO) Assembly adopted resolution A.584 (14) on Measures to prevent unlawful acts which threaten the safety of ships and the security of their passengers and crew, and in 1986 the Maritime Safety Committee (MSC) issued Circular MSC/Circ.443 on Measures to prevent unlawful acts against passengers and crews on board ships.

In natural sequence and common spirit in Rome, March 1988, the International Conference on the Suppression of Unlawful Acts against the Safety of Maritime Navigation, adopted the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention). The main purpose of the Convention was to ensure that appropriate action was enacted against persons committing unlawful acts against ships. Among other unlawful acts covered by the Convention, the following noteworthy provisions were outlined under Article 3: the seizure of ships by force, acts of violence against persons on board ships, and the placing of devices on board a ship which are likely to destroy or damage it. Furthermore, the Convention obliged Contracting Governments either to extradite or prosecute alleged offenders.

The 1988 SUA Convention however was entangled with shortcomings within its framework unable to address some of the grave concerns related to maritime security, specifically: using a vessel as a weapon to perpetrate a terrorist attack on a port or an offshore facility, acts of violence against persons on board if the violence does not impede the safety of navigation of the vessel, acts causing severe damage to the marine environment by spreading or dumping hazardous material or waste in territorial waters or on the open sea inflicting dreadful economic and environmental fallout or endangering human lives, acts directed at equipping and utilizing ships as a terrorist

weapon against a state undertaken in any part of the ocean except in internal waters or aimed at smuggling potential terrorists or material into the territory of a state with the purpose of perpetrating acts of terrorism against the aforementioned state.[1]

The need to fill the vacancy of a full-fledged and complete international security code to combat the threat of maritime terrorism was evident.

On 1 July 2004 a new maritime security regulatory regime was adopted into the International Convention for the Safety of Life at Sea (SOLAS), 1974 as amended, namely chapter XI-2 on Special measures to enhance maritime security, which includes the International Ship and Port Facility Security (ISPS) Code. The ISPS Code entered into force a mere 18 months after its adoption by the SOLAS Conference in December 2002.

It was adopted in response to the devastating terrorist acts of September 11 of 2001 in the United States, following which, the international community recognized the need to protect the international maritime transport sector against the threat of terrorism. IMO responded swiftly and firmly by developing these new requirements, which are a by-product of cooperation between Governments, Government agencies, local administrations and shipping and port industries.

Chapter 1: The ISPS Code

1.1. Introduction

The International Ship and Port Facility Security (ISPS) Code was adopted under the International Convention for the Safety of Life at Sea (SOLAS) 1974, as amended, through chapter XI-2 on Special Measures to enhance maritime security, is a mandatory instrument for all countries Party to the Convention and the IMO's main legislative framework to address maritime security related matters and the basis for a comprehensive mandatory security regime for international shipping.

The ISPS Code provides for considerable flexibility to allow for required security measures to be adjusted to meet the assessed risks facing particular ships or port facilities. The code contains detailed security-related requirements which SOLAS contracting Governments, port authorities and shipping companies must adhere to in order to be in compliance with the Code, and is divided into two key sections: a mandatory Part A and a non-mandatory Part B. The mandatory Part A outlines maritime and port security-related provisions covering the appointment of security officers for shipping companies, individual ships and port facilities. It also includes security matters that must be covered in security plans, prepared accordingly in respect of ships and port facilities. The non-mandatory Part B contains a series of recommendatory guidelines on how to meet the requirements and obligations set out within the provisions of Part A such as recommendations on preparing ship and port facility security plans. The extent to which guidance applies may vary depending on the nature of the port facility and of the ship, its trade or cargo.

[1] Jesus, H. E. J. (2003). Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects. The International Journal of Marine and Coastal Law, page 394.

Since the adoption of the ISPS Code, the IMO has adopted further guidance for its Member States and the Maritime Industry, with a view to safeguarding the effective implementation of the Code. A consolidated version of all the relevant guidance adopted by IMO was subsequently developed in the form of the IMO Guide to Maritime Security and the ISPS Code.

Other sources of guidance material include:

- The ILO/IMO Code of practice on security in ports
- Presentations at IMO national and regional workshops and seminars
- Relevant webpages of SOLAS Contracting Governments and multilateral organizations
- Information made available to IMO by Contracting Governments on their organizational structures, practices and procedures such as: the guidance they issue to their port facilities and shipping companies, as well as their implementation experience

1.2. Application, Objectives and Functional Requirements

The ISPS Code applies to the following types of ships engaged on international voyages:

- Passenger ships, including high-speed passenger craft
- Cargo ships, including high-speed craft, of 500 gross tonnage and upwards
- Mobile offshore drilling units
- Port facilities serving such ships engaged on international voyages

Contracting Governments ought to decide the extent of application of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required occasionally to serve ships arriving or departing on an international voyage. The Designated Authorities have to base their decisions on a port facility security assessment carried out in accordance with the Code while any decision shall not compromise the level of security intended to be achieved in accordance to chapter XI-2 or this Part of the Code.

The ISPS Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

The main objectives of the Code are:

- Establishment of an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in the international trade
- Determining the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and

port industries, at the national and international level for ensuring maritime security
- Ensuring the early and efficient collection and exchange of security-related information
- Providing a methodology for security assessments so as to have in place plans and procedures to react to changing security levels
- To ensure confidently that adequate and proportionate maritime security measures are in place on board ships and ports

In order to achieve the aforementioned objectives, the Code embodies a number of functional requirements. These include the following:

- Gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments
- Requiring the maintenance of communication protocols for ships and port facilities
- Preventing unauthorized access to ships, port facilities and their restricted areas
- Preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities
- Providing means for raising the alarm in reaction to security threats or security incidents
- Requiring ship and port facility security plans based upon security assessments
- Requiring training, drills and exercises to ensure familiarity with security plans and procedures

For the purpose of accomplishing the abovementioned objectives, SOLAS contracting governments, port authorities and shipping companies are obliged under the ISPS Code to designate appropriate security officers and personnel on each ship, port facility and shipping company. These security officers designated are the undermentioned: Port Facility Security Officer (PFSO), Ship Security Officer (SSO) and Company Security Officer (CSO) which are charged with the duties of assessing as well as preparing and implementing effective security plans that are able to handle and deter any potential security threat. The IMO has the ability to provide support to member states in need of assistance in implementing the Code through a variety of means among them being for instance: national and regional workshops, seminars and assessment missions.

1.3. Risk Management

The purpose of the ISPS Code is to provide a standardized and consistent framework for evaluating risk and enabling Governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate security levels and corresponding security measures.

In essence, the Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and in order to determine what security measures are appropriate an assessment of the risks must be made in each particular case.

As with all risk management efforts the most effective course of action is to eliminate the source of the threat. Eliminating the source of the threat, which in this case is those

that would commit acts of terrorism or otherwise threaten the security of ships or of the port facilities, is essentially a Government function.

In order to determine what security measures are appropriate Contracting Governments must assess the threat and evaluate the risk of a potential unlawful act. The Designated Authority must assay the major assets and infrastructure which are vital for the continuous operation of the port facilities as well as the areas or structures which could potentially cause significant loss of life or inflict harm to the economy or environment of the port facilities. Furthermore, the evaluation of security must examine the vulnerability of the port facilities and determine their weaknesses in the aspect of physical security breaches, structural integrity, protection and communication systems, procedural policies, transportation infrastructure and the use of high security risk areas within the grounds of the port facility. As soon as the identification of the threat is concluded, the Contracting Government is then able to properly evaluate the danger.

The ISPS Code provides specific requirements for the implementation of Risk Management within its standardized framework for the security of ships and port facilities.

For Ships, these requirements include:

- Ship Security Plans (SSP)
- Ship Security Officers (SSO)
- Company Security Officers (CSO)
- Onboard equipment

For Port facilities, these requirements include:

- Port Security Plans (PSP)
- Port Facility Security Officers (PFSO)

In Addition, requirements for Port facilities and Ships include:

- Monitoring and controlling access
- Monitoring the activities of people and cargo
- Ensuring security communications

Because each ship and each port facility is subject to different threats, the method by which they will meet the specific requirements of the ISPS Code will be determined and eventually be approved by the Administration or Contracting Government, as the case may be.

In order to communicate the threat at a port facility or for a ship and to initiate the appropriate response actions the Contracting Government must set the appropriate security level. The security level is the qualification of the degree of risk that a security incident will be attempted or will occur and it creates a link between the ship and the port facility, since it triggers the implementation of appropriate security measures for the ship and for the port facility. The security levels are numbered in sequence of 1, 2

and 3 corresponding accordingly to normal, heightened and exceptional degree of security risk.

As threat increases the only logical counteraction is to reduce vulnerability. The ISPS Code provides several ways to reduce vulnerabilities. Each ship and each port facility will have to determine the measures needed to intensify their security measures to appropriately offset the threat by reducing their vulnerability. 100% security is an aim but cannot be guaranteed, hence the risk reduction approach to lessen possibilities to the lowest practicable.

1.4. Obligations of Ship and Company, Port Facility and Responsibilities of Contracting Governments

Obligations of Ship and Company:

In accordance with the ISPS Code, shipping companies shall designate a Company Security Officer for the company and a Ship Security Officer for each of their ships. The responsibilities of the Company Security Officer incorporate the assurance that the Ship Security Assessment is carried out by persons with appropriate skills to evaluate the security of a ship and that the Ship Security Plan is complete, ready to be approved by or on behalf of the Administration, and thereafter placed onboard each ship.

The company shall ensure that the Ship Security Plan contains a clear statement emphasizing the Master's authority. Additionally, the Company shall establish in the Ship Security Plan that the Master has the overriding authority and responsibility to make decisions with respect to the safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary. Furthermore, the Company shall ensure that the Company Security Officer, the Master and the Ship Security Officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and the ISPS Code.

The Ship Security Plan should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so by the Administration or the Contracting Government. Moreover, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.

The Company and Ship Security Officer should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan for which the Administration has determined that approval is required, have to be submitted for review and approval before their incorporation in the approved plan and their implementation by the ship.

The Company shall ensure that the Master has available on board, at all times, information through which officers duly authorized by a Contracting Government can establish:

- Who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship
- Who is responsible for deciding the employment of the ship
- In cases where the ship is employed under the terms of a charter party**,** who are the parties to such charter party

Furthermore, Regulation XI-2/5 requires the company to provide the Master of the ship with information to meet the requirements of the Company under the provisions of the aforementioned regulation. This information should include items such as:

- Parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors and concessionaries
- Parties responsible for deciding the employment of the ship including, time or bareboat charterer or any other entity acting in such capacity
- In cases when the ship is employed under the terms of a charter party, the contact details of those parties including time or voyage charterers

In accordance with regulation XI-2/5 the Company is obliged to update and keep this information current as and when changes occur.

The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of the ISPS Code. Where a ship is not in compliance with the requirements of this chapter or of part A of the ISPS Code, or cannot comply with the requirements of the security level set by the Administration or by another Contracting Government and applicable to that ship, then the ship shall notify the appropriate competent authority prior to conducting any ship to port interface or prior to entry into port, whichever occurs earlier.

When a ship is at a port or is proceeding to a port of a Contracting Government, the Contracting Government has the right, under the provisions of regulation XI-2/9, to exercise various control and compliance measures with respect to that ship. The ship is subject to port State control inspections but such inspections will not normally extend to examination of the Ship Security Plan itself except in specific circumstances. The ship may also be subject to additional control measures if the Contracting Government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

The ship is also required to have onboard information to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship. When the responsibility for the operation of the ship is assumed by another Company, the information relating to the Company, which operated the ship, are not required to be left on board.

Obligations of Port Facility:

In compliance with the requirements of chapter XI-2 and part A of the ISPS Code, each Contracting Government or Designated Authority or Recognized Security Organization has to carry out and ensure completion of a Port Facility Security Assessment for every of the port facilities located within its territory that serves ships engaged on international voyages. The completed Port Facility Security Assessment has to be approved by the Contracting Government or the Designated Authority concerned, an approval which cannot be delegated. The Port Facility Security Assessment is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which parts of it are more liable and more likely to be the subject of attack.

On completion of the analysis it will be possible to produce an overall assessment of the level of risk, a security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.
The Port Facility Security Assessment will help determine which port facilities are required to appoint a Port Facility Security Officer and prepare a Port Facility Security Plan.

The Port Facility Security Assessments should be periodically reviewed and must include the following components:

- The perceived threat to port installations and infrastructure that must be determined
- The identified potential vulnerabilities
- The calculated consequences of incidents

The port facilities which have to comply with the requirements of chapter XI-2 and part A of the Code are required to designate a Port Facility Security Officer and operate in accordance with a Port Facility Security Plan approved by the Contracting Government or by the Designated Authority concerned.

The Port Facility Security Plan should indicate the operational and physical security measures the port facility ought to take to ensure that it always operates at security level 1. The plan shall indicate also the additional or intensified security measures the port facility can take to move to and operate at security level 2 when instructed to do so by the Contracting Government or Designated Authority. Furthermore, the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may be issued by those responding at security level 3 to a security incident or threat thereof.

The Port Facility Security Officer should implement the provisions and monitor the continuing effectiveness and relevance of the Port Facility Security Plan, including commissioning internal audits of the application of the plan. Amendments to any of the specified elements of an approved plan for which the Contracting Government or the Designated Authority concerned has determined that approval is required, have to be submitted for review and ratified before their incorporation in the approved plan and their implementation at the port facility. The Contracting Government or the

Designated Authority concerned may test the effectiveness of the Port Facility Security Plan potentially leading to amendment of the aforementioned approved plan.
Ships using port facilities may be subject to the Port State Control Inspections and additional control measures outlined in regulation XI-2/9. The Designated Authorities may request the provision of information regarding the ship, its cargo, passengers and personnel prior to the ship's entry into port. There may be circumstances in which entry into port could be denied.

Responsibilities of Contracting Governments:

In line with the provisions of chapter XI-2 and part A of the ISPS Code Contracting Governments have various responsibilities, which amongst others include the undermentioned:

- Setting the applicable security level
- Approving the Ship Security Plan and relevant amendments to a previously approved plan
- Verifying the compliance of ships with the provisions of chapter XI-2 and part A of the Code and issuing to ships the International Ship Security Certificate
- Determining which of the port facilities located within their territory are required to designate a Port Facility Security Officer who will be responsible for the preparation of the Port Facility Security Plan
- Ensuring completion and approval of the Port Facility Security Assessment and of any subsequent amendments to a previously approved assessment
- Approving the Port Facility Security Plan and any subsequent amendments to a previously approved plan
- Establishing the requirements for a Declaration of Security
- Exercising control and compliance measures, testing the effectiveness of approved plans or their amendments to the extent they consider appropriate and communicating information to the International Maritime Organization (IMO) and to the shipping and port industries

Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure or access to security sensitive material relating to Ship Security Assessments, Ship Security Plans, Port Facility Security Assessments and Port Facility Security Plans and to individual assessments or plans. Additionally, Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.

Contracting Governments are able to appoint or establish Designated Authorities within Government to undertake, with regard to port facilities, their security duties in accordance with the provisions of chapter XI-2 and part A of the ISPS Code while allowing Recognized Security Organizations (RSO) to conduct certain work in relation to port facilities. Nevertheless, the final decision on the acceptance and approval of this work shall be given by the Contracting Government or the Designated Authority. Contracting Governments may also delegate the undertaking of certain security duties regarding ships to Recognized Security Organizations, such as the following:

- Approving Ship Security Plans (SSP) or amendments thereto, on behalf of the Administration
- Verifying implementation of the SSP onboard ships in compliance with the requirements of chapter XI-2 and part A of the Code, on behalf of the Administration
- Issuing International Ship Security Certificates (ISSC), including Interim ISSCs
- Conducting Port Facility Security Assessments required by the Contracting Government

An RSO may also assist in the conducting of a Ship Security Assessment in preparation of a Ship Security Plan. In case an RSO has done so, the aforementioned RSO must not be authorized to approve the Ship Security Plan, verify its implementation onboard or issue an ISSC to a ship in respect of the implementation.

When delegating specific duties to a RSO, Contracting Governments should ensure that the RSO has the competencies needed to undertake the task.

1.5. Ship Security: Security Levels, Ships Security Assessment, Ship Security Plan and the Declaration of Security

Security Levels:

A ship is required to act upon the security levels set by Contracting Governments. Prior to entering a port or whilst in a port within the territory of a Contracting Government, a ship shall comply with the requirements for the security level set by that Contracting Government, if such security level is higher than the security level set by the Administration for that ship. Ships shall respond without undue delay to any change to a higher security level.

Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag. When changes in security level occur, security level information shall be updated as the circumstance dictates.
Contracting Governments shall set security levels and ensure the provision of security level information to port facilities within their territory and to ships prior to entering a port or whilst in a port within their territory. When changes in security level occur, security level information shall be updated as the circumstance dictates.

The setting of the security level applying at any particular time is under the jurisdiction of the Contracting Governments, regarding ships and port facilities alike, according to the provisions of regulation XI-2/3 and XI-2/7. In consonance with Part A of the ISPS Code there are three security levels for international use. These are in sequence:

- Security Level 1: Normal, low threat situation, the level at which ships and port facilities normally operate
- Security Level 2: Heightened, the level applying for as long as there is a heightened risk of a security incident
- Security Level 3: Exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident

In order to set the appropriate security levels there are Factors needed to be considered in advance, these include:

- The degree that the threat information is credible
- The degree that the threat information is corroborated
- The degree that the threat information is specific or imminent
- The potential consequences of such a security incident

At security level 1, the subsequent activities shall be performed on all ships through appropriate measures, taking into consideration the guidance given in part B of the ISPS Code, in order to identify and adopt preventive measures against security incidents:

- Ensuring the performance of all ship security duties
- Controlling access to the ship
- Controlling the embarkation of persons and their effects
- Monitoring restricted areas to ensure that only authorized persons have access
- Monitoring of deck areas and areas surrounding the ship
- Supervising the handling of cargo and ship's stores
- Ensuring that security communication is readily available

Under the auspices of part B of the Code, at security level 2, additional protective measures specified in the Ship Security Plan shall be implemented for each activity detailed above.

Similarly, at security level 3, further specific protective measures specified in the Ship Security Plan shall be implemented for each aforementioned activity. Contracting Governments, when they set security level 3 shall issue as necessary appropriate instructions and shall provide security related information to the ships and port facilities that may be affected.

It is of vital importance to be noted, that it is not admissible for a ship to claim that it operates at the highest state of security alertness regardless of the security level set by the Contracting Governments. There must be a progression from the measures employed at security level 1 through security level 2 to the measures employed at security level 3, or from level 1 direct to level 3.

Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level. In order to verify that this requirement has been met, records of this acknowledgement should be kept on board. This will be in addition to the requirement set by the ISPS Code which requires records to be maintained of changing security levels. This record may be in the form of a logbook or similar entry. An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the Port Facility Security Officer the initiation of the implementation of the appropriate measures and procedures as detailed in the Ship

Security Plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the Port Facility Security Officer and Ship Security Officer shall liaise and co-ordinate the appropriate actions, Records of this acknowledgement should be retained onboard.

If a ship is obliged by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall advise without delay the competent authority of the Contracting Government, within whose territory the port facility is located, and the Port Facility Security Officer of the situation. Additionally, the Ship Security Officer shall liaise with the Port Facility Security Officer and coordinate appropriate actions if deemed necessary. In this case as well, Records should be retained onboard.

When Contracting Governments set security levels and ensure the provision of security level information to ships operating in their territorial sea or having communicated an intention to enter their territorial waters, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area. When advising such ships of the applicable security level, a Contracting Government shall also advise, under the guidance provided in part B of the ISPS Code, those ships of any security measure that they should take, and if considered appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

Ship Security Assessment:

The Ship Security Assessment (SSA) is an essential and integral part of the process of developing and updating the Ship Security Plan. Companies may wish to produce a generic Ship Security Assessment (SSA) that covers the assessment of security risks across a part of their fleet or their entire fleet. Such an approach is acceptable provided an On-scene Security Survey has been carried out on each ship and the SSA reflects all relevant ship specific aspects.

The SSA shall include an On-scene Security Survey and at least the undermentioned elements:

- Identification of existing security measures, procedures and operations
- Identification and evaluation of key ship board operations that are important to protect
- Identification of possible threats to the key ship board operations and the likelihood of their occurrence in order to establish and prioritize security measures
- Identification of weaknesses, including human factors in the infrastructure, policies and procedures

In addition, a SSA should address specifically the subsequent elements on board or within the ship:

- Physical security

- Structural integrity
- Personnel Protection Systems
- Procedural policies
- Radio and telecommunication systems, including computer systems and networks (Cybersecurity)
- Other areas that may pose a risk to people, property or operations on board the ship or within a port facility, if damaged or used for an illicit observation

Those responsible for commencing a SSA must be able to draw upon expert assistance in relation to the following:

- Knowledge of current security threats and patterns
- Recognition and detection of weapons, dangerous substances and devices
- Recognition of characteristics and behavioral patterns of persons who are likely to threaten security, on a non-discriminatory basis
- Techniques used to circumvent security measures
- Methods used to cause a security incident
- Effects of explosives on ship's structures and equipment
- Ship security
- Ship to port interface business practices
- Ship to port operations
- Physical security
- Contingency planning, emergency preparedness and response
- Radio and telecommunications systems, including computer systems and networks
- Marine engineering

The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

Furthermore, the SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions and should determine security guidance including but not limited to:

- The Restricted Areas
- The response procedures to fire or other emergency conditions
- The level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.
- The frequency and effectiveness of security patrols
- The access control systems, including identification systems
- The security communications systems and procedures
- The security doors, barriers and lighting
- The security and surveillance equipment and systems

Moreover, the SSA ought to consider the persons, activities, services and operations which are crucial to protect. These include among others:

- The ship's personnel
- Passengers, visitors, vendors, repair technicians, port facility personnel, etc.
- The capacity to maintain safe navigation and emergency response
- The cargo, particularly dangerous goods or hazardous substances
- The ship's stores
- The ship security communication equipment and systems
- The ship's security surveillance equipment and systems

In sequence, the SSA shall consider all possible threats that may include the following types of security incidents:

- Damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism
- Hijacking or seizure of the ship or of persons on board
- Tampering with cargo, essential ship equipment or systems or ship's stores
- Unauthorized access or use, including presence of stowaways
- Smuggling weapons or equipment, including weapons of mass destruction
- Use of the ship to carry those intending to cause a security incident or their equipment
- Use of the ship itself as a weapon or as a means to cause damage or destruction
- Attacks from seaward whilst at berth or at anchor or whilst at sea

Finally, the SSA should take into account all possible vulnerabilities, which may include:

- Conflicts between safety and security measures
- Conflicts between shipboard duties and security assignments
- Watch-keeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance
- Any identified security training deficiencies
- Any security equipment and systems, including communication systems

When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

The Ship Security Assessment shall be documented, reviewed, accepted and retained by the Company. Upon completion of the SSA a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of counter measures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

On-scene Security Survey

The On-scene Security Survey is an integral part of any SSA. The On-scene Security Survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

- Ensuring the performance of all ship security duties
- Monitoring restricted areas to ensure that only authorized persons have access
- Controlling access to the ship, including any identification systems
- Monitoring of deck areas and areas surrounding the ship
- Controlling the embarkation of persons and their effects, including accompanied and unaccompanied baggage and ship's personnel personal effects
- Supervising the handling of cargo and the delivery of ship's stores
- Ensuring that ship security communication, information, and equipment are readily available

There should be evidence that each individual ship has been subject to an On-scene Security Survey

Ship Security Plan:

The Ship Security Plan is developed to ensure the application of measures on board the ship designed to protect persons on board, cargo**,** cargo transport units, ship's stores or the ship from the risks of a security incident. The content of each individual SSP should vary depending on the particular ship it covers. The Ship Security Assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail.
Administrations may prepare advice on the preparation and content of a SSP and each ship shall carry on board a Ship Security Plan approved by the Administration. Companies may wish to produce a generic Ship Security Plan (SSP) that covers the management of security across a part of their fleet, or their entire fleet. Such an approach is acceptable provided an "on site security survey" has been carried out on each ship and both the SSP and the SSA on which it is based reflect all relevant ship specific aspects.

The plan shall make provisions for the three security levels as defined in Part A of the ISPS Code and shall address at least the following:

- Measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship
- Identification of the restricted areas and measures for the prevention of unauthorized access to them
- Measures for the prevention of unauthorized access to the ship
- Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship to port interface
- Procedures for responding to any security instructions which Contracting Governments may give at security level 3
- Procedures for evacuation in case of security threats or breaches of security
- Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects
- Procedures for auditing the security activities
- Procedures for training, drills and exercises associated with the plan

- Procedures for interfacing with port facility security activities
- Procedures for the periodic review of the plan and for updating
- Procedures for reporting security incidents
- Identification of the Ship Security Officer
- Identification of the Company Security Officer, including 24-hour contact details
- Procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board
- Frequency for testing or calibration of any security equipment provided on board
- Identification of the locations where the Ship Security Alert System (SSAS) activation points are provided
- Procedures, instructions and guidance on the use of the Ship Security Alert System (SSAS), including the testing, activation, deactivation and resetting and to limit false alerts

The auditor should verify by interview that persons onboard are familiar with their duties and responsibilities, as specified in the SSP. Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship. Internal audits should be conducted at least once every 12 months. Copies of internal audit reports should be retained onboard, for a minimum period of 5 years, treated as confidential information and protected against unauthorized disclosure.

The SSP should be reviewed at least once every 12 months in conjunction with the SSA. The schedule of drills and training should reflect the risks to security identified in the SSA. In addition should it be identified during training, drills or following an incident that the SSP, and hence the SSA, are inappropriate, they should be reviewed and amended accordingly. Records should be maintained of the review process.

The Administration shall determine which changes to an approved Ship Security Plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and the ISPS Code. The objective of testing, calibration and maintenance should be to ensure that the equipment is fit for purpose and should be in accordance with manufacturer's recommendations.

The nature of the changes to the Ship Security Plan or the security equipment that have been specifically approved by the Administration shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the

physical and operational characteristics, including the voyage pattern, of the individual ship.

All SSPs should:

- Detail the organizational structure of security for the ship
- Detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility
- Detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities
- Detail the basic security measures for security level 1, both operational and physical, that will always be in place
- Detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3
- Provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances
- Reporting procedures to the appropriate Contracting Governments contact points

Ship Security Plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures, in compliance with regulation XI-2/9. Administrations may allow this by exception, in order to avoid compromising in any way the objective of providing on board the Ship Security Alert System, this information must be kept elsewhere on board in a document known to the Master, the Ship Security Officer and other senior shipboard personnel as may be decided by the Company.

The plan shall be protected from unauthorized access or disclosure and its containing information considered as confidential. In case the plan is kept in an electronic format, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of the Code and the only means to verify or rectify the non-compliance is to review the relevant requirements of the Ship Security Plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government or the master of the ship concerned.

Declaration of Security:

The Declaration of Security (DoS) is an agreement reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans. The agreed DoS should be signed and dated by both the port facility and the ship(s), as applicable, to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level, or levels and the relevant contact details. The Declaration of Security shall address the security

requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship to port interface or ship to ship activity poses to persons, property or the environment. A ship can request completion of a Declaration of Security when:

- The ship is operating at a higher security level than the port facility or another ship it is interfacing with
- There is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages
- There has been a security threat or a security incident involving the ship or involving the port facility, as applicable
- The ship is at a port which is not required to have and implement an approved port facility security plan
- The ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan

It is of vital importance to be noted that requests for the completion of a Declaration of Security shall be acknowledged by the applicable port facility or ship.

The Declaration of Security shall be completed by the Master or the Ship Security Officer on behalf of the ship and, if appropriate, by the Port Facility Security Officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory. Similarly, the Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary or when a ship deems it necessary. The need for a DoS may be indicated by the results of the Port Facility Security Assessment (PFSA) and the reasons and circumstances in which a DoS is required should be set out in the Port Facility Security Plan (PFSP). Likewise, the need for a DoS may be indicated by an Administration for ships entitled to fly its flag or as a result of a Ship Security Assessment and should be set out in the Ship Security Plan.

It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, or another ship with which it interfaces, and for ship to port interface or ship to ship activities that pose a higher risk to persons, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors. A change in the security level may require that a new or revised DoS be completed.

In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the Port Facility Security Officer (PFSO) or Ship Security Officer (SSO) should acknowledge the request and discuss appropriate security measures.

A PFSO may also initiate a DoS prior to ship to port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include the embarking or disembarking passengers, and the transfer, loading or unloading of dangerous goods or hazardous substances. The PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

1.6. Organization and Performance of Ship Security Duties

The duties and responsibilities of all shipboard personnel with a security role shall culminate in the safeguarding of the ship. The performance of the crew is necessary to continuously maintain, at all times, the effectiveness of the security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction. The successful organization and the smoothness of the operation of the ship's security procedures results in the timely submission and assessment of reports relating to possible breaches of security or security concerns at every Security Level imposed by the Administration or the Contracting Government.

Some critical measures taken per level are essential in order to minimize the possibility of a breach of safety and avert the consequences of potential risks while ensuring the integrity of the ship's safety. In detail the security measures that could be taken at each Security Level are covering the undermentioned issues:

- Access to the Ship by ship's personnel, passengers, visitors, etc.
- Restricted Areas on the Ship
- Handling of Cargo
- Delivery of Ship's Stores
- Handling Unaccompanied Baggage
- Monitoring the Security of the Ship

Access to the Ship:

The Ship Security Plan (SSP) should establish the security measures covering all means of access to the ship identified in the Ship Security Assessment (SSA). This should include any:

- Access ladders
- Access gangways
- Access ramps
- Access doors, side scuttles, windows and ports
- Mooring lines and anchor chains
- Cranes and hoisting gear

For each of the abovementioned the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge, this may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship's personnel and visitors respectively.

The SSP should establish the frequency of application of any access controls particularly if they are to be applied on a random, or occasional, basis.

Any ship identification system should, when it is practicable to do so, be coordinated with that applying to the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated and that abuse of procedures should be subject to disciplinary action.

Those unwilling or unable to establish their identity or to confirm the purpose of their visit when requested to do so, should be denied access to the ship and their attempt to obtain access should be reported as appropriate to the SSOs, the CSOs, the Port Facility Security Officer (PFSO) and to the national or local authorities with security responsibilities.

Security Level 1

At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

- Checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders etc.
- In liaison with the port facility the ship should ensure that designated secure areas are established in which inspections and searching of people, baggage (including carry-on items), personal effects, vehicles and their contents can take place
- In liaison with the port facility the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP
- Segregating checked persons and their personal effects from unchecked persons and their personal effects
- Segregating embarking from disembarking passengers
- Identification of access points that should be secured or attended to prevent unauthorized access
- Securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access and providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance

At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security Level 2

At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

- Assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access
- Limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them
- Deterring waterside access to the ship, including**,** for example, in liaison with the port facility, provision of boat patrols
- Establishing a restricted area on the shore-side of the ship, in close co-operation with the port facility
- Increasing the frequency and detail of searches of people, personal effects, and vehicles being embarked or loaded onto the ship
- Escorting visitors on the ship
- Providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and the stressing the need for increased vigilance
- Carrying out a full or partial search of the ship

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- Limiting access to a single, controlled, access point
- Granting access only to those responding to the security incident or threat thereof
- Directions of persons on board
- Suspension of embarkation or disembarkation
- Suspension of cargo handling operations, deliveries etc.
- Evacuation of the ship
- Movement of the ship
- Preparing for a full or partial search of the ship

Restricted Areas on the Ship:

The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purpose of restricted areas are to:

- Prevent unauthorized access
- Protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship
- Protect sensitive security areas within the ship
- Protect cargo and ship's stores from tampering

The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas. The SSP should provide that all restricted areas should be clearly marked indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

Restricted areas may include:

- Navigation Bridge, machinery spaces of category A and other control stations as defined in chapter II-2
- Spaces containing security and surveillance equipment and systems and their controls and lighting system controls
- Ventilation and air-conditioning systems and other similar spaces
- Spaces with access to potable water tanks, pumps, or manifolds
- Spaces containing dangerous goods or hazardous substances
- Spaces containing cargo pumps and their controls
- Cargo spaces and spaces containing ship’s stores
- Crew accommodation
- Any other areas as determined by the CSO, through the SSA to which access must be restricted to maintain the security of the ship

Security Level 1

At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:

- Locking or securing access points
- Using surveillance equipment to monitor the areas
- Using guards or patrols
- Using automatic intrusion detection devices to alert the ship’s personnel of unauthorized access

Security Level 2

At security level 2, the frequency and intensity of the monitoring of, and control of access to restricted areas should be increased to ensure that only authorized persons

have access. The SSP should establish the additional security measures to be applied, which may include:

- Establishing restricted areas adjacent to access points
- Continuously monitoring surveillance equipment
- Dedicating additional personnel to guard and patrol restricted areas.

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operations with those responding and the port facility, which may include:

- Setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied
- Searching of restricted areas as part of a search of the ship

Handling of Cargo:

The security measures relating to cargo handling should:

- Prevent tampering
- Prevent cargo that is not meant for carriage from being accepted and stored on board the ship

The security measures, some of which may have to be applied in liaison with the port facility, should include inventory control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship.
In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.

Security Level 1

At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:

- Routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations
- Checks to ensure that cargo being loaded matches the cargo documentation
- Ensuring, in liaison with the port facility, that vehicles to be loaded on board car carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP
- Checking of seals or other methods used to prevent tampering

Checking of cargo may be accomplished by the following means:

- Visual and physical examination

- Using scanning/detection equipment, mechanical devices, or dogs

When there are regular, or repeated, cargo movement the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

Security Level 2

At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:

- Detailed checking of cargo, cargo transport units and cargo spaces
- Intensified checks to ensure that only the intended cargo is loaded
- Intensified searching of vehicles to be loaded on car-carriers, ro-ro and passenger ships
- Increased frequency and detail in checking of seals or other methods used to prevent tampering

Detailed checking of cargo may be accomplished by the following means:

- Increasing the frequency and detail of visual and physical examination
- Increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs
- Coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- Suspension of the loading or unloading of cargo
- Verify the inventory of dangerous goods and hazardous substances carried on board, if any, and their location

Delivery of Ship's Stores:

The security measures relating to the delivery of ship's stores should:

- Ensure checking of ship's stores and package integrity
- Prevent ship's stores from being accepted without inspection
- Prevent tampering
- Prevent ship's stores from being accepted unless ordered

For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security Level 1

At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:

- Checking to ensure stores match the order prior to being loaded on board
- Ensuring immediate secure stowage of ship's stores.

Security Level 2

At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- Subjecting ship's stores to more extensive checking
- Preparation for restriction or suspension of handling of ship's stores
- Refusal to accept ship's stores on board the ship

Handling Unaccompanied Baggage:

The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship. It is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security Level 1

At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 2

At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- Subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles
- Preparation for restriction or suspension of handling of unaccompanied baggage
- Refusal to accept unaccompanied baggage on board the ship

Monitoring the Security of the Ship:

The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

- Lighting
- Watch-keepers, security guards and deck watches including patrols,
- Automatic intrusion detection devices and surveillance equipment.

When used, automatic intrusion detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

Security Level 1

At security level 1, the SSP should establish the security measures to be applied which may be a combination of lighting, watch keepers, security guards or use of security and surveillance equipment to allow ship’s security personnel to observe the ship in general, and barriers and restricted areas in particular.

The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship to port interface activities or at a port facility or anchorage when necessary. While underway, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulation for the Prevention of Collisions at Sea in force.

The following should be considered when establishing the appropriate level and location of lighting:

- The ship's personnel should be able to detect activities beyond the ship, on both the shore side and the waterside
- Coverage should include the area on and around the ship
- Coverage should facilitate personnel identification at access points
- Coverage may be provided through coordination with the port facility.

Security Level 2

At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

- Increasing the frequency and detail of security patrols
- Increasing the coverage and intensity of lighting or the use of security and surveillance and equipment
- Assigning additional personnel as security lookouts
- Ensuring coordination with waterside boat patrols, and foot or vehicle patrols on the shore-side, when provided.

Additional lighting may be necessary to protect against a heightened risk of a security incidents.

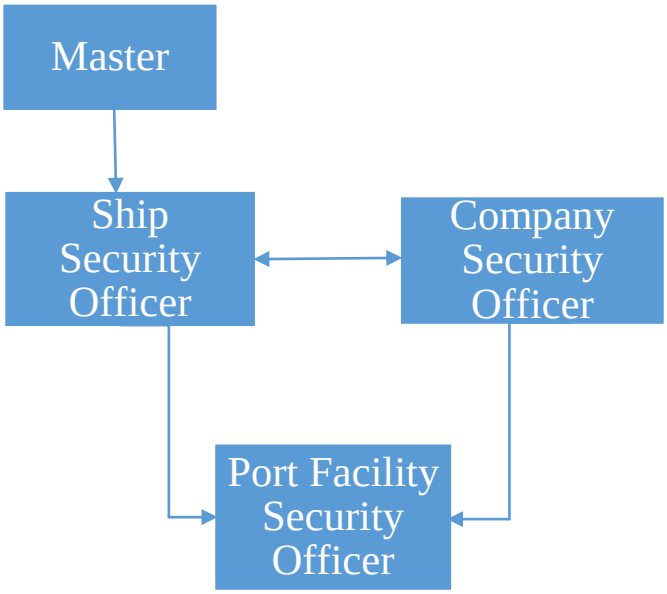
When necessary, the additional lighting requirements may be accomplished by coordinating with the port facility to provide additional shore side lighting.

Security Level 3

At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

- Switching on of all lighting on, or illuminating the vicinity of, the ship
- Switching on of all on board surveillance equipment capable of recording activities on, or in the vicinity of, the ship
- Maximizing the length of time such surveillance equipment can continue to record
- Preparation for underwater inspection of the hull of the ship
- Initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

1.7. Master, Company Security Officer, Ship Security Officer and Port Facility Officer



Master:

A Master (Mariner Master or Captain) is the professional qualification required for someone to serve as the Captain of a commercial vessel of any size and of any type, operating anywhere in the world. Masters, also known as Captains, are in overall command of the ship and are responsible for the safety, efficiency and commercial feasibility of the ship. The Master is in charge of the safety of the crew, vessel and cargo. He is charged with ensuring that all international and local laws are followed properly and that all management policies are fully complied with. Master also ensures compliance with the vessel's security plan, as required by the ISPS Code.

The Master shall not be constrained by the Company, the charterer or any other person from taking or executing any decision which, in the professional judgment of the Master, is necessary to maintain the safety and security of the ship. This includes denial of access to persons (except those identified as duly authorized by a Contracting Government) or their effects and refusal to load cargo, including containers or other closed cargo transport units.

If, in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the ship arises during its operations, the Master shall give effect to those requirements necessary to maintain the safety of the ship. In such cases, the Master may implement temporary security measures and shall forthwith inform the Administration and, if deemed appropriate, the Contracting Government in whose port the ship is operating or intends to enter. Any such temporary security measures under this regulation shall, to the highest possible degree, be commensurate with the prevailing security level. When such cases are identified, the Administration shall ensure that such conflicts are resolved and that the possibility of recurrence is minimized.

Company Security Officer:

The Company Security Officer (CSO) is the person designated by the Company for ensuring that a Ship Security Assessment is carried out, that a Ship Security Plan is developed, submitted for approval, and thereafter implemented and maintained and for liaison with Port Facility Security Officers and the Ship Security Officer.
The Company shall designate a Company Security Officer. A person designated as the company security officer may act as the Company Security Officer for one or more ships, depending on the number or types of ships the Company operates provided it is clearly identified for which ships this person is responsible.

In addition to those specified elsewhere in this paper and in accordance to the ISPS Code, the duties and responsibilities of the Company Security Officer shall include, but are not limited to the following:

- Advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information
- Ensuring that Ship Security Assessments are carried out
- Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the Ship Security Plan
- Ensuring that the Ship Security Plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship
- Arranging for internal audits and reviews of security activities
- Arranging for the initial and subsequent verifications of the ship by the Administration or the Recognized Security Organization
- Ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with
- Enhancing security awareness and vigilance
- Ensuring adequate training for personnel responsible for the security of the ship
- Ensuring effective communication and co-operation between the Ship Security Officer and the relevant Port Facility Security Officers
- Ensuring consistency between security requirements and safety requirements
- Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately
- Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

Furthermore, the CSO should obtain and record the information required to conduct an assessment, including:

- The general layout of the ship
- The location of areas which should have restricted access, such as Navigation Bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.
- The location and function of each actual or potential access point to the ship
- Changes in the tide which may have an impact on the vulnerability or security of the ship
- The cargo spaces and stowage arrangements

- The locations where the ship's stores and essential maintenance equipment is stored
- The locations where unaccompanied baggage is stored
- The emergency and stand-by equipment available to maintain essential services
- The number of ship's personnel, any existing security duties and any existing training requirement practices of the Company
- Existing security and safety equipment for the protection of passengers and ship's personnel
- Escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship
- Existing agreements with private security companies providing ship/waterside security services
- Existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

Identification of the CSO can be by name or position. Auditors may, as part of the verification process test the 24hr contact details supplied for the CSO.

Ship Security Officer:

The Ship Security Officer (SSO) is the person on board the ship accountable to the Master**,** designated by the Company as responsible for the security of the ship, including implementation and maintenance of the Ship Security Plan and for liaison with the Company Security Officer and Port Facility Security Officers.

In addition to those specified elsewhere in this paper and in compliance with the ISPS Code, the duties and responsibilities of the Ship Security Officer shall contain, but are not limited to the subsequent:

- Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained
- Maintaining and supervising the implementation of the Ship Security Plan, including any amendments to the plan
- Coordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant Port Facility Security Officers
- Proposing modifications to the Ship Security Plan
- Reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions
- Enhancing security awareness and vigilance on board
- Ensuring that adequate training has been provided to shipboard personnel, as appropriate
- Reporting all security incidents
- Coordinating implementation of the Ship Security Plan with the Company Security Officer and the relevant Port Facility Security Officer

- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

The Ship Security Officer shall have the authority onboard to enable the stated duties and responsibilities to be carried out effectively. Identification of the SSO can be by name or position. A Ship Security Officer shall be designated on each ship.

Port Facility Security Officer:

The Port Facility Security Officer (PFSO) is the person designated as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the Ship Security Officers and Company Security Officers. A Port Facility Security Officer shall be designated for each port facility. A person may be designated as the Port Facility Security Officer for one or more port facilities.

In addition to those specified elsewhere in this paper and in line with the ISPS Code, the duties and responsibilities of the Port Facility Security Officer shall cover, but not be limited to:

- Conducting an initial comprehensive security survey of the port facility taking into account the relevant Port Facility Security Assessment
- Ensuring the development and maintenance of the Port Facility Security Plan
- Implementing and exercising the Port Facility Security Plan
- Undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures
- Recommending and incorporating, as appropriate, modifications to the Port Facility Security Plan in order to correct deficiencies and to update the plan to take into account of relevant changes to the port facility
- Enhancing security awareness and vigilance of the port facility personnel
- Ensuring adequate training has been provided to personnel responsible for the security of the port facility
- Reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility
- Coordinating implementation of the Port Facility Security Plan with the appropriate Company and Ship Security Officer
- Coordinating with security services, as appropriate
- Ensuring that standards for personnel responsible for security of the port facility are met
- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any
- Assisting Ship Security Officers in confirming the identity of those seeking to board the ship when requested.

The Port Facility Security Officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and the ISPS Code.

In those exceptional instances where the Ship Security Officer has questions about the validity of identification documents of those seeking to board the ship for official

purposes, the Port Facility Security Officer should assist. However, the PFSO should not be responsible for routine confirmation of the identity of those seeking to board the ship.

1.8. Port Security: Port Facility Security Assessment and Port Facility Security Plan

Port Facility Security Assessment:

The Port Facility Security Assessment (PFSA) is an essential and integral part of the process of developing and updating the Port Facility Security Plan. The Port Facility Security Assessment may be conducted by a Recognized Security Organization (RSO). However, approval of a completed PFSA should only be given by the relevant Contracting Government. If a Contracting Government uses a RSO, to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.
The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, under the guidance given in part B of the ISPS Code. The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats or minor changes in the port facility and shall always be reviewed and updated when major changes to the port facility take place.

A PFSA should address the following elements within a port facility:

- Physical security
- Structural integrity
- Personnel protection systems
- Procedural policies
- Radio and telecommunication systems, including computer systems and networks (Cybersecurity)
- Relevant transportation infrastructure
- Utilities
- Other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility.

Furthermore, those involved in a PFSA should be able to draw upon expert assistance in relation to:

- Knowledge of current security threats and patterns
- Recognition and detection of weapons, dangerous substances and devices
- Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are likely to threaten security
- Techniques used to circumvent security measures
- Methods used to cause a security incident
- Effects of explosives on structures and port facility services
- Port facility security
- Port business practices
- Contingency planning, emergency preparedness and response

- Physical security measures e.g. fences
- Radio and telecommunications systems, including computer systems and networks
- Transport and civil engineering
- Ship and port operations.

The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established. This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident. This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

Identification and evaluation of assets and infrastructure should be used to prioritize their relative importance for protection. The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset and the extent to which rapid re-establishment of normal functioning is possible.

Assets and infrastructure that should be considered important to protect may include:

- Accesses, entrances, approaches, and anchorages, maneuvering and berthing areas
- Cargo facilities, terminals, storage areas, and cargo handling equipment
- Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks
- Port vessel traffic management systems and aids to navigation
- Power plants, cargo transfer piping, and water supplies
- Bridges, railways, roads
- Port service vessels, including pilot boats, tugs, lighters etc.
- Security and surveillance equipment and systems
- The waters adjacent to the port facility.

The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritization of protective measures, and decisions concerning the allocation of resources to better protect the port facility. The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures is of vital importance.

Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritize security

requirements to enable planning and resource allocations. Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies. While identifying and assessing threats, those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.

Moreover, the PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:

- Any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack
- The likely consequences in terms of loss of life, damage to property, economic disruption, including disruption to transport systems, of an attack on, or at, the port facility
- The capability and intent of those likely to mount such an attack
- The possible type or types of attack, producing an overall assessment of the level of risk against which security measures have to be developed.

In addition, the PFSA should consider all possible threats, which may include the following types of security incidents:

- Damage or destruction of the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism
- Hijacking or seizure of the ship or of persons on board
- Tampering with cargo, essential ship equipment or systems or ship's stores
- Unauthorized access or use including presence of stowaways
- Smuggling weapons or equipment, including weapons of mass destruction
- Use of the ship to carry those intending to cause a security incident and their equipment
- Use of the ship itself as a weapon or as a means to cause damage or destruction
- Blockage of port entrances, locks, approaches etc.
- Nuclear, biological and chemical attack.

The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

The identification, selection and prioritization of countermeasures and procedural changes is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship to port interface in the face of possible threats. Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

- Security surveys, inspections and audits
- Consultation with port facility owners and operators, and owners or operators of adjacent structures if appropriate
- Historical information on security incidents

- Operations within the port facility.

Identification of vulnerabilities

Identification of vulnerabilities in physical structures, personnel protection systems, processes or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges etc. that could be resolved through physical measures, e.g. permanent barriers, alarms, surveillance equipment etc.

Identification of vulnerabilities should include consideration of:

- Waterside and shore-side access to the port facility and ships berthing at the facility
- Structural integrity of the piers, facilities, and associated structures
- Existing security measures and procedures, including identification systems
- Existing security measures and procedures relating to port services and utilities
- Measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks
- Adjacent areas that may be exploited during, or for, an attack
- Existing agreements with private security companies providing waterside or shore side security services
- Any conflicting policies between safety and security measures and procedures
- Any conflicting port facility and security duty assignments
- Any enforcement and personnel constraints
- Any deficiencies identified during training and drills
- Any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits etc.

Port Facility Security Plan:

The Port Facility Security Plan (PFSP) shall be developed and maintained on the basis of a Port Facility Security Assessment for each port facility and ought to be adequate for the ship to port interface. The plan shall make provisions for the three security levels, as defined in the ISPS Code. Preparation of the Port Facility Security Plan (PFSP) is the responsibility of the Port Facility Security Officer (PFSO). While the PFSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual PFSO.

The content of each individual PFSP should vary depending on the particular circumstances of the port facility or facilities, it covers. The Port Facility Security (PFSA) will have identified the particular features of the port facility and the potential security risks, which have led to the need to appoint a PFSO and to prepare a PFSP. The preparation of the PFSP will require these features and other local or national security considerations to be addressed in the PFSP and for appropriate security measures to be established so as to minimize the likelihood of a breach of security and

the consequences of potential risks. Contracting Governments may prepare advice on the preparation and content of a PFSP.

All PFSPs should:

- Detail the security organization of the port facility and the organization's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organization and its links with others, including ships in port
- Detail the basic security level 1 measures, both operational and physical, that will be in place
- Detail the additional security measures that will allow the port facility to progress without delay to security level 2 and, when necessary, to security level 3
- Provide for regular review, or audit, of the PFSP and for its amendments in response to experience or changing circumstances
- Reporting procedures to the appropriate Contracting Governments contact points
- Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.

Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

The Port Facility Security Plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans. The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized access or disclosure, deletion, destruction or amendment.

Contracting Government should approve the PFSPs of the port facilities under their jurisdiction. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each measure will be in place. If there is likely to be any delay in their provision this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security Measures that provide an equivalent level of security should be agreed to cover any interim period.

The use of firearms on or near ships and in port facilities may pose particular and significant safety risks, in particular in connection with certain dangerous or hazardous substances and should be considered very carefully. In the event that a Contracting Government decides that it is necessary to use armed personnel in these areas, that

Contracting Government should ensure that these personnel are duly authorized and trained in the use of their weapons and that they are aware of the specific risks to safety that are present in these areas. If a Contracting Government authorizes the use of firearms they should issue specific safety guidelines on their use. The PFSP should contain specific guidance on this matter in particular with regard its application to ships carrying dangerous goods or hazardous substances.

1.9. Verification and Certification for Ships

Verifications:

Each ship to which the ISPS Code applies shall be subject to the verifications specified below:

- An initial verification before the ship is put in service or before the International Ship Security Certificate (ISSC) is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of chapter XI-2, the ISPS Code and the approved Ship Security Plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and the ISPS Code, is in satisfactory condition and fit for the service for which the ship is intended
- A renewal verification at intervals specified by the Administration, but not exceeding five years. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2, the ISPS Code and the approved Ship Security Plan, is in satisfactory condition and fit for the service for which the ship is intended.
- At least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second and third anniversary date of the certificate as defined in regulation I/2(n). The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate
- Any additional verifications as determined by the Administration.

The use of the term “fully complies” above means that a certificate cannot be issued unless all the requirements of the approved SSP are fully implemented and any associated security equipment and systems are present and fit for purpose. If the auditor identifies through objective evidence non-compliance in the approved SSP, this shall be communicated to the company, the Administration and the organization that approved the plan. In such cases, an ISSC shall not be issued until it can be shown that the security system, and any associated security equipment of the ship, is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A and B of the ISPS Code.

The verifications of ships shall be carried out by officers of the Administration. The Administration may, however, entrust the verifications to a Recognized Security Organization referred to in regulation XI-2/1. In every case, the Administration

concerned shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, the ISPS Code and the approved Ship Security Plan. At the Initial, Intermediate, Renewal and any additional verification, the auditor shall verify through a representative sample that at all security equipment and systems has been maintained and calibrated in accordance with the provisions of the SSP and the manufacturers' instructions. After any verification as described above has been completed, no changes shall be made in security system and in any associated security equipment or the approved Ship Security Plan without the sanction of the Administration.

Issue or Endorsement of Certificate:

An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of the ISPS Code.

Such certificate shall be issued or endorsed either by the Administration or by the Recognized Security Organization acting on behalf of the Administration. Another Contracting Government may, at the request of the Administration, cause the ship to be verified and if satisfied that the provisions of the Code are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship and where appropriate, endorse or authorize the endorsement of that certificate on the ship, in accordance with the Code. A copy of the certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Administration. A certificate so issued shall contain a statement to the effect that it has been issued at the request of the Administration.

The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix of the ISPS Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

Duration and Validity of Certificate:

An International Ship Security Certificate shall be issued for a period specified by the Administration which shall not exceed five years.

On completion of an audit, and to facilitate the review process by the audit organization, a certificate with validity not exceeding five (5) months may be issued by the auditor.

When the renewal verification is completed within three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

When the renewal verification is completed after the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing certificate.

When the renewal verification is completed more than three months before the expiry date of the existing certificate, the new certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

If a certificate is issued for a period of less than five years, the Administration may extend the validity of the certificate beyond the expiry date to the maximum possible period, provided that the aforementioned verifications, applicable when a certificate is issued for a period of five years, are carried out as appropriate.

If a renewal verification has been completed and a new certificate cannot be issued or placed on board the ship before the expiry date of the existing certificate, the Administration or Recognized Security Organization acting on behalf of the Administration may endorse the existing certificate and such a certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

If a ship at the time when a certificate expires is not in a port in which it is to be verified, the Administration may extend the period of validity of the certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is verified and then only in cases where it appears proper and reasonable to do so. No certificate shall be extended for a period longer than three months and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new certificate. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the expiry date of the existing certificate before the extension was granted.

A certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new certificate shall be valid to a date not exceeding five years from the date of expiry of the existing certificate before the extension was granted.

If an intermediate verification is completed before the period between the second and third anniversary date of the certificate, then:

- The expiry date shown on the certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed
- The expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the aforesaid verifications not exceeded.

An endorsed certificate shall cease to be valid in any of the following cases:

- If the relevant verifications are not completed within the periods already specified

- If the certificate is not endorsed within the applicable time limits set by the ISPS Code
- When a Company assumes the responsibility for the operation of a ship not previously operated by that Company
- Upon transfer of the ship to the flag of another State.

In the case of:

- A transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports

  OR

- A Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described below.

Interim Certification:

The certificates shall be issued only when the Administration issuing the certificate is fully satisfied that the ship complies with the requirements of the ISPS Code. However, after the 1st of July 2004, until the International Ship Security Certificate is issued, the Administration may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the Appendix of the ISPS Code, for the purposes of:

- A ship without a certificate, on delivery or prior to its entry or re-entry into service
- Transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government
- Transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government or
- When a Company assumes the responsibility for the operation of a ship not previously operated by that Company

If the ship re-enters the management of a company after a reasonable period of time under the management of others, conformation should be sought from the Administration as to whether it is appropriate to issue an Interim Certification.
An Interim International Ship Security Certificate shall only be issued when the Administration or Recognized Security Organization, on behalf of the Administration, has verified that:

- The Ship Security Assessment required by the Code has been completed and a copy of the Ship Security Plan meeting the requirements of chapter XI-2 and

part A of the ISPS Code is provided on board, has been submitted for review and approval, and is being implemented on the ship

- The ship is provided with a Ship Security Alert System meeting the requirements of regulation XI-2/6 and if required the Company Security Officer has ensured the review of the Ship Security Plan for compliance with the Code and that the plan has been submitted for approval and is being implemented on the ship while establishing the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the CSO is satisfied that the ship's arrangements have been made and will successfully complete the required verifications within 6 months
- The Master, the Ship's Security Officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified by the Code and with the relevant provisions of the Ship Security Plan placed on board and have been provided such information in the working language of the ship's personnel or languages understood by them
- The Ship Security Officer meets the requirements of the Code.

There should be evidence onboard that the company intends to conduct an internal security audit on the ship within three months and that the ship is planned to be offered for full term certification within the validity of the Interim ISSC.

An Interim International Ship Security Certificate may be issued by the Administration or by a Recognized Security Organization authorized to act on its behalf.

An Interim International Ship Security Certificate shall be valid for 6 months, or until the ISSC is issued, whichever comes first, and may not be extended.

No Contracting Government shall cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgment of the Administration or the Recognized Security Organization, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and the ISPS Code beyond the aforesaid period of the initial Interim Certificate.

For the purposes of regulation XI-2/9, Contracting Governments may, prior to accepting an Interim International Ship Security Certificate as a valid certificate, ensure that the previously described requirements have been fully met.

1.10. Additional Requirements of SOLAS

Automatic Identification Systems:

The Automatic Identification Systems (AIS) transponders are designed to be capable of providing position, identification and other information about the ship to other ships and to coastal authorities automatically.

SOLAS regulation V/19 (Carriage requirements for shipborne navigational systems and equipment) sets out navigational equipment to be carried on board ships, according to ship type. In 2000, IMO adopted a new requirement (as part of a revised new chapter

V) for all ships to carry Automatic Identification Systems (AISs) capable of providing information about the ship to other ships and to coastal authorities automatically.

The regulation requires AIS to be fitted aboard all ships of 300 gross tonnage and upwards engaged on international voyages, cargo ships of 500 gross tonnage and upwards not engaged on international voyages and all passenger ships irrespective of size. The requirement became effective for all ships by 31 December 2004.

Ships fitted with AIS shall maintain AIS in operation at all times except where international agreements, rules or standards provide for the protection of navigational information. A flag State may exempt certain ships from carrying an AIS. Performance standards for AIS were adopted in 1998.

The regulation requires that AIS shall:

- Provide information including the ship's identity, type, position, course, speed, navigational status and other safety-related information automatically to appropriately equipped shore stations, other ships and aircraft
- Receive automatically such information from similarly fitted ships
- Monitor and track ships
- Exchange data with shore-based facilities.

Ship Identification Number:

The Ship's Identification Number shall be permanently marked:

- In a visible place either on the stern of the ship or on either side of the hull, amidships port or starboard, above the deepest assigned load line or either side of the superstructure, port and starboard or on the front of the superstructure or, in the case of passenger ships, on a horizontal surface visible from the air. The permanent marking shall be not less than 200 mm in height.

  OR

- In an easily accessible place either on one of the end transverse bulkheads of the machinery spaces, as defined in regulation II-2/3.30, or on one of the hatchways or, in the case of tankers, in the pump-room or, in the case of ships with ro-ro spaces, as defined in regulation II-2/3.41, on one of the end transverse bulkheads of the ro-ro spaces. The permanent marking shall be plainly visible, clear of any other markings on the hull and shall be painted in a contrasting color. In addition the permanent marking shall not be less than 100 mm in height while the width of the marks shall be proportionate to the height.

The permanent marking may be made by raised lettering or by cutting it in or by centre punching it or by any other equivalent method of marking the ship identification number which ensures that the marking is not easily expunged.

On ships constructed of material other than steel or metal, the Administration shall approve the method of marking the Ship Identification Number.

Ship Security Alert System:

All ships shall be provided with a Ship Security Alert System (SSAS), as follows:

- Ships constructed on or after 1 July 2004
- Passenger ships, including high-speed passenger craft, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004
- Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004
- Other cargo ships of 500 gross tonnage and upward and mobile offshore drilling units constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.

The Ship Security Alert System when activated shall:

- Initiate and transmit a ship-to-shore security alert to a competent authority designated by the Administration, which in these circumstances may include the Company, identifying the ship, its location and indicating that the security of the ship is under threat or it has been compromised
- Not send the ship security alert to any other ships
- Not raise any alarm on-board the ship
- Continue the ship security alert until deactivated or reset

The Ship Security Alert System shall be capable of being activated from the navigation bridge and in at least one other location and conform to performance standards not inferior to those adopted by the Organization. The Ship Security Alert System activation points shall be designed so as to prevent the inadvertent initiation of the ship security alert. The requirement for a Ship Security Alert System may be complied with by using the radio installation fitted for compliance with the requirements of chapter IV, provided all requirements of this regulation are complied with.

When an Administration receives notification of a ship security alert, that Administration shall immediately notify the State(s) in the vicinity of which the ship is presently operating. Similarly, when a Contracting Government receives notification of a ship security alert from a ship which is not entitled to fly its flag, that Contracting Government shall immediately notify the relevant Administration and if appropriate, the State(s) in the vicinity of which the ship is presently operating.

Continuous Synopsis Record:

Every ship to which chapter I applies shall be issued with a Continuous Synopsis Record. The Continuous Synopsis Record is intended to provide an on-board record of the history of the ship with respect to the information recorded therein. The Continuous Synopsis Record shall be kept on board the ship and shall be available for inspection at all times. For ships constructed before 1 July 2004, the Continuous Synopsis Record shall, at least, provide the history of the ship as from 1 July 2004.
The Continuous Synopsis Record shall be issued by the Administration to each ship that is entitled to fly its flag and it shall contain at least, the following information:

- The name of the State whose flag the ship is entitled to fly
- The date on which the ship was registered with that State
- The Ship's Identification Number
- The name of the ship
- The port at which the ship is registered
- The name of the registered owner(s) and their registered address (es)
- The name of the registered bareboat charterer(s) and their registered address (es), if applicable
- The name of the Company, as defined in regulation IX/1, its registered address and the address(es) from where it carries out the safety management activities
- The name of all classification society (ies) with which the ship is classed
- The name of the Administration or of the Contracting Government or of the Recognized Organization which has issued the Document of Compliance (or the Interim Document of Compliance), specified in the ISM Code as defined in regulation IX/1, to the Company operating the ship and the name of the body which has carried out the audit on the basis of which the document was issued, if other than that issuing the document
- The name of the Administration or of the Contracting Government or of the Recognized Organization that has issued the Safety Management Certificate (or the Interim Safety Management Certificate), specified in the ISM Code as defined in regulation IX/1, to the ship and the name of the body which has carried out the audit on the basis of which the certificate was issued, if other than that issuing the certificate
- The name of the Administration or of the Contracting Government or of the recognized security organization that has issued the International Ship Security Certificate (or an Interim International Ship Security Certificate), specified in part A of the ISPS Code as defined in regulation XI-2/1, to the ship and the name of the body which has carried out the verification on the basis of which the certificate was issued, if other than that issuing the certificate
- The date on which the ship ceased to be registered with that State.

Any changes relating to the aforementioned information shall be recorded in the Continuous Synopsis Record so as to provide updated and current information together with the history of the changes. In case of any changes, the Administration shall issue, as soon as is practically possible but not later than three months from the date of the change, to the ships entitled to fly its flag either a revised and updated version of the Continuous Synopsis Record or appropriate amendments thereto.

Furthermore, the Administration, pending the issue of a revised and updated version of the Continuous Synopsis Record, shall authorize and require either the Company as defined in regulation IX/1 or the master of the ship to amend the Continuous Synopsis Record to reflect the changes. In such cases, after the Continuous Synopsis Record has been amended the Company shall, without delay, inform the Administration accordingly.

The Continuous Synopsis Record shall be in English, French or Spanish language. Additionally, a translation of the Continuous Synopsis Record into the official language or languages of the Administration may be provided. The Continuous Synopsis Record shall be in the format developed by the Organization and shall be maintained in

accordance with guidelines developed by the Organization. Any previous entries in the Continuous Synopsis Record shall not be modified, deleted or, in any way, erased or defaced.

Whenever a ship is transferred to the flag of another State or the ship is sold to another owner (or is taken over by another bareboat charterer) or another Company assumes the responsibility for the operation of the ship, the Continuous Synopsis Record shall be left on board.

When a ship is to be transferred to the flag of another State, the Company shall notify the Administration of the name of the State under whose flag the ship is to be transferred so as to enable the Administration to forward to that State a copy of the Continuous Synopsis Record covering the period during which the ship was under their jurisdiction.

When a ship is transferred to the flag of another State the Government of which is a Contracting Government, the Contracting Government of the State whose flag the ship was flying hitherto shall transmit to the Administration as soon as possible after the transfer takes place a copy of the relevant Continuous Synopsis Record covering the period during which the ship was under their jurisdiction together with any Continuous Synopsis Records previous issued to the ship by other States.

When a ship is transferred to the flag of another State, the Administration shall append the previous Continuous Synopsis Records to the Continuous Synopsis Record the Administration will issue to the ship so to provide the continuous history record intended by this regulation.

Ships intending to enter a port of another Contracting Government:

A Contracting Government may require that ships intending to enter its ports provide the following information to officers duly authorized by that Government to ensure compliance with this chapter prior to entry into port with the aim of avoiding the need to impose control measures or steps:

- That the ship possesses a valid Certificate and the name of its issuing authority
- The security level at which the ship is currently operating
- The security level at which the ship operated in any previous port where it has conducted a ship to port interface within the timeframe specified by the ISPS Code
- Any special or additional security measures that were taken by the ship in any previous port where it has conducted a ship to port interface within the timeframe specified by the ISPS Code
- That the appropriate ship security procedures were maintained during any ship to ship activity within the timeframe specified by the ISPS Code
- Other practical security related information (but not details of the Ship Security Plan), taking into account the guidance given in part B of the ISPS Code.

If requested by the Contracting Government, the ship or the Company shall provide confirmation acceptable to that Contracting Government, of the information required above. The ship shall keep records of the information for the last 10 calls at port facilities.

Every ship, to which the ISPS Code applies, intending to enter the port of another Contracting Government shall provide the abovementioned information on the request of the officers duly authorized by that Government. The Master may decline to provide such information on the understanding that failure to do so may result in denial of entry into port.

If, after receipt of the information described above, officers duly authorized by the Contracting Government of the port in which the ship intends to enter have clear grounds for believing that the ship is in non-compliance with the requirements of part A of the ISPS Code, such officers shall attempt to establish communication with and between the ship and the Administration in order to rectify the non-compliance. If such communication does not result in rectification or if such officers have clear grounds otherwise for believing that the ship is in non-compliance with the requirements of part A of the ISPS Code, such officers may take steps in relation to that ship. Any such steps taken must be proportionate, taking into account the guidance given in part B of the ISPS Code. Such steps are as follows:

- A requirement for the rectification of the non-compliance
- A requirement that the ship proceed to a location specified in the territorial sea or internal waters of that Contracting Government
- Inspection of the ship, if the ship is in the territorial sea of the Contracting Government the port of which the ship intends to enter denial of entry into port.

Prior to initiating any such steps, the ship shall be informed by the Contracting Government of its intentions. Upon this information the Master may withdraw the intention to enter that port. In such cases, these regulations shall not apply.

<u>Additional Provisions:</u>

Indicative control measures in order to control and enforce the compliance of ships are as follows:

- Inspection of the ship
- Delaying the ship
- Detention of the ship
- Restriction of operations including movement within the port or expulsion of the ship from port.

Such control measures may additionally or alternatively include other lesser administrative or corrective measures.
In the event:

- Of the imposition of a control measure, other than a lesser administrative or corrective measure

  OR

- Any of the steps referred above are taken, an officer duly authorized by the Contracting Government shall forthwith inform in writing the Administration

specifying which control measures have been imposed or steps taken and the reasons thereof. The Contracting Government imposing the control measures or steps shall also notify the Recognized Security Organization, which issued the Certificate relating to the ship concerned and the Organization when any such control measures have been imposed or steps taken.

When entry into port is denied or the ship is expelled from port, the authorities of the port State should communicate the appropriate facts to the authorities of the State of the next appropriate ports of call, when known, and any other appropriate coastal States, taking into account guidelines to be developed by the Organization. Confidentiality and security of such notification shall be ensured.
Denial of entry into port or expulsion from port shall only be imposed where the officers duly authorized by the Contracting Government have clear grounds to believe that the ship poses an immediate threat to the security or safety of persons, or of ships or other property and there are no other appropriate means for removing that threat.

The control measures and the steps previously referred, shall only be imposed pursuant to the SOLAS regulations, until the non-compliance giving rise to the control measures or steps has been corrected to the satisfaction of the Contracting Government, taking into account actions proposed by the ship or the Administration, if any.

When Contracting Governments exercise control or take the aforementioned steps, all possible efforts shall be made to avoid a ship being unduly detained or delayed. If a ship is thereby unduly detained or delayed, it shall be entitled to compensation for any loss or damage suffered. In addition, necessary access to the ship shall not be prevented for emergency or humanitarian reasons and for security purposes.

Chapter 2: Maritime Terrorism

2.1. Introduction

Maritime Terrorism is often defined as a form of terrorism perpetrated at sea with a political, ideological or religious incentive and violent dimensions within the maritime commerce and shipping sector. With a worldwide area of effect, the repercussions of terrorism on the safety of sea transportation, navigation and marine environment, along with the threat on human lives and capital, call for effective counter-measures. Amongst such measures of suppression, those that enforce the legal protection of shipping are of paramount importance.[2]

Nevertheless, despite the aforementioned, there is no universally accepted definition of Maritime Terrorism among the legal experts, as there is no authoritative definition of Terrorism, which is hard to define in consensus, without accumulating confrontation.[3]

[2] Jesus, H. E. J. (2003), Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects, page 363.
[3] Bjørn Møller, Piracy, Maritime Terrorism and Naval Strategy. Danish Institute for International Studies, DIIS, 2009, page 23.

Maritime Terrorism is a serious concern for the International and National Security, the spectrum of which encompasses premeditated, politically motivated acts performed in the open sea or within territorial waters against non-combatant targets such as passengers or civilian personnel, the maritime environment, merchant or commercial vessels and fixed platforms, or port, coastal and land-based facilities or settlements, namely tourist resorts and port towns or cities. Furthermore, critical infrastructure of vessels and port facilities such as maritime navigation systems, oil and gas facilities on the sea, submerged pipelines and communications cables may be within the scope of an attack by a potential terrorist breach using a maritime approach. Moreover, many other commercial interests can be affected and set in peril, for instance: the tourism sector and the fishing industries. The above acts of violence and terrorist maliciousness are, in many cases, perpetrated by sub-national groups or clandestine agents. In the eyes of many, particularly in the legal community, terrorism has a political dimension with objectives of a primarily ideological origin. In this framework of thought, a vicious incident utilizing violent means at sea, can only be termed to be an act of terrorism if its ideological and political motives are clearly outlined. On an another thread of thought, all political violence (incorporating maritime piracy and armed robbery alike) is a form of terrorism, their root causes and enabling factors being similar in nature.[4]

In order to establish operational guidelines of counter-measurements, a straightforward way is preemptively need so as to understand, in due course, the phenomenon of maritime terrorism from a practical perspective. A typology based on the utilization of the maritime space and the selection of targets fulfills that purpose[5], as follows:

I. "Where the sea is only a medium for terrorist attacks on land-based targets: An example is the Mumbai bombings on 26 November 2008, when ten terrorists landed on the city shores using speedboats and carried out a series of coordinated attacks on land targets.
II. The hijacking of naval vessels and hostage taking by terrorists: One of the most widely utilized maritime terror tactics in conflict-prone regions. Examples are the series of hijackings by the Abu Sayyaf in the Sulu Sea, the subsequent taking of hostages and their brutal treatment.
III. An attack in ports, facilities and coastal installations: In June 2018, terrorists attacked the Libyan oil ports of Ras Lanuf and Es Sider, setting at least one storage tank on fire, following which the 16 facilities were closed and evacuated.
IV. Terrorist attacks against civilian ships and warships: Two Al Qaeda suicide bombers rammed an explosives-laden dingy into the USS Cole on October 12, 2000, killing 17 US service members. Two years later in October 2002, a terrorist strike on French oil tanker, M/V Limburg killed 16 people and injured scores others, also causing an environmental catastrophe with a massive crude oil spill into the Gulf of Aden."[6]

[4] Abhijit Singh, Maritime Terrorism in Asia: An Assessment. ORF Occasional Paper No. 215, October 2019, Observer Research Foundation, page 4.
[5] Abhijit Singh, Maritime Terrorism in Asia: An Assessment, page 4.
[6] Abhijit Singh, Maritime Terrorism in Asia: An Assessment, page 5.

For a long time, due to the fact that there was no legal framework addressing terrorist acts perpetrated at sea, a penal indictment framing them as piracy was enacted by some national judicial courts and publicists, even though they did not display such a profile of action or qualify any requirements, having in mind that, normally, only one ship was involved while at the same time the act of terrorism was not undertaken with the intention of accomplishing private ends. Therefore, in the pursuit of administrating justice, since there was no definite international law directed at terrorist attacks and faced with dilemma of a concrete situation, the need was felt to treat them as cases of piracy in order to circumvent the case of offenders going unpunished.[7]

Political turmoil and struggles amplifying over the last decades were the breeding factors of acts of terrorism on land that would eventually extend to the sea. Evidently, terrorism at sea is a recent phenomenon in comparison to piracy. Indeed, only after the incident of passenger liner Achille Lauro did the international community agree consensually on some particular rules applicable to maritime terrorism, through the adoption of the SUA Convention. The 1985 attack on Achille Lauro is perhaps the most well-known undisputed case of maritime terrorism in our modern times. [8]

In 1985 the Italian-flagged commercial cruise ship Achille Lauro was seized while on the high seas, on course from Alexandria to Port Said, Egypt. The perpetrators were allegedly a Palestinian guerrilla group that threatened to murder the British and American passengers unless Israel was to liberate 50 Palestinian political prisoners. When the demands imposed were not fulfilled, an American passenger was killed. The Achille Lauro hijacking was qualified by a number of states, the United States included, as an act of piracy. Nevertheless, under the auspices of International maritime piracy law this was not, in its nature, an act of piracy since there was no private end being pursued. Moreover, the seizure did not meet the essential two-vessel requirement expected for the characterization of piracy. The terrorists were motivated to act by sheer political goals and thus they would not have fallen in the definition of piracy under the law of nations. However, from a judicial point of view, pragmatically, in order to deal with efficacy in anticipation of future cases of maritime terrorism, an exact set of international regulations was necessitated to secure the prosecution and indictment of the offenders, since the piracy laws seemed to be inadequate of that purpose. The position of the Achille Lauro flag state, Italy, was of the same opinion, a fact which soon lead, after the conclusion of the Achille Lauro affair, to the international community's attention to the requirement for a Convention on maritime terrorism, in an effort to fill a lacuna in the legal framework of the fight against International terrorism.[9]

[7] Jesus, H. E. J. (2003), Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects, page 387.
[8] Jesus, H. E. J. (2003), Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects, page 388.
[9] Jesus, H. E. J. (2003), Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects, page 388.

2.2. The Contemporary Threat of Maritime Terrorism

The potential capability of terrorist groups perpetuating acts of aggression in an extent of encompassing the worldwide maritime commerce is a cause of an accumulating concern conducted by Intelligence analysts, law enforcement officials, and policymakers.[10]

In the recent past, a plurality of terrorist organizations were unable nor possessed the prerequisite means to extend their physical area of effect beyond coastal regions and purely local theaters. Even for those groups that did have the aforesaid potential of amplifying their area of operations, there were several impediments conjoined with carrying through marine borne strikes that have persistently worked to counterbalance a number of the tactical advantages situated in the maritime environment. In consequence, maritime terrorism did not correlate well in all respects to the terrorist's obtainable opportunities, capabilities, or intentions.[11]

Limited resources while in a sea operation has confined the outlined options at a terrorist's disposal, since for most groups, traditionally, mariner skills are non-existent as is any level of familiarity with certain specialist capabilities (for instance, surface and underwater demolition techniques) while access to appropriate assault and transport vehicles in order to mount and sustain operations from a non–land-based environment is beyond reach.[12]

The inadequate operational finances and insufficient skill sets compel most terrorist groups to coerce their targets through a path of least effort, in the spirit of adhering to methods that are known to effectively work, hence offering a reasonable chance of success with predictable risks of vulnerability. Therefore, forming an inherently conservative nature of terrorists bound to finite human and material assets and lack of technical skills. Moreover, the costs of unpredictability associated with the expansion of terrorist excursions deter, the majority of groups, from exploiting such a change in operational direction in order to materialize the potential benefits that may output. A further consideration concerns the nature of maritime targets themselves, as many of them are for the most part unreachable, especially commercial vessels operating in the open ocean. An aggressive ship with ill intent is, thus, unlikely to prompt the same level of publicity, in immediacy or magnitude, as for example a strike to a land-based facility, which being in a fixed position and located near an urban area, is far more media-accessible, even though this might not be the case with regards to a heavily laden cruise liner or passenger ferry. This is of vital importance to be noted, since terrorism, fundamentally, can only be effective while illustratively demonstrating its prominence and effect through the visual propaganda of its actions.[13]

In spite of the abovementioned considerations, the discernable threat of maritime terrorism has been amplified notably with an augmentative manner over the past several years and in sequence formulating the dire need for counterterrorism planning, within

[10] Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz. Maritime Terrorism: Risk and Liability. RAND Corporation, 2006, page 9.
[11] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 10.
[12] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 10.
[13] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 10-11

national and international terms. The activating causes for this heightened level of attention are complicated and multifaceted but can be summarized in the concerns that can be found in terms of vulnerability, capability, and intent.[14]

2.3. Consequences of Maritime Terrorism

The consequences entailed in the phenomenon of maritime terrorism can be materialized in various forms that might affect individuals, the private and public sector. In general terms, these ramifications are categorized into one of the three following groups: human, economic, and intangible effects. Human consequences refers to effects on lives brought about by fatalities and injuries. Economic consequences are those effects that can easily be assessed in financial terms. Intangible effects address those effects that are difficult to measure in human lives or financial accounts because they are measured in metrics that cannot be easily translatable into lives or financial metrics or because the cause-and-effect linkage is not understood well enough to allow precise evaluation and attribution of effects.[15]

Human Consequences of Terrorism:

Individuals suffer the most from the consequences of terrorism. The people are vulnerable to injuries or fatalities and endure severe psychological repercussions as a fallout from terrorist attacks. Moreover, the aforesaid consequences can indirectly affect the public and private sectors alike, especially when economic costs are concerned. Again, the costs anticipated with fatalities and injuries may be mitigated partially through compensatory fail-safe mechanisms like civil insurance claims, with a substantial of the burdens inflicted be borne by the private sector. In addition, fatalities are shared both by the public and private sectors in terms of loss of human capital. To the public sector, the most frequent outcome of this is a temporary loss of potential degree of effectiveness until organizations can be reorganized. If a substantial proportion of people with a particular specialty skill vital for serving a specific function were affected by a terrorist attack, the repercussions could be grave and severely disruptive, potentially leading to a loss of years needed for recovery. In the private sector the scales of impact are different, loss of human capital that will not affect a nation's production capabilities can terminate an individual firm.[16]

Economic and Intangible Consequences of Property Damage:

Terrorist attacks can dismantle physical and intellectual property alike. Attacks that are capable of inflicting damage to facilities, infrastructure, products or raw materials, can lower the quantity and quality of assets of private firms. Damage to the infrastructure of facilities and information systems may culminate into economic disruptions and loss of data while delivery delays and a diminished revenue is to be expected from the interruption of business. Power source failure may also downsize firm assets that might have enabled future revenues, which could outweigh the economic instability, while at the same time reduction of demand or loss of supply could eliminate the economic activity at a large scale, until facilities and infrastructure can be replaced. As the

[14] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*., page 10-11
[15] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*., page 33
[16] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 33-34.

magnitude and duration of disruptions intensifies, the consequences can be more permanent and even irreversible until a far later point in time. Firms may experience long-term transportation inefficiencies and in the most extreme of cases, disruptions can lead to long-term or permanent loss of business. The private-sector fallout effects can transfer into the public sector as well. Consequently, business disruptions will result to significant loss of revenue for local and state governments. The amalgamated effects of destruction of private infrastructure along with public infrastructure will prompt to a decreased functionality of public services, such public transportation, leading to a rise in freights, while delivery delays and loss of revenue in the transport sector will be the general norm.[17]

Economic and Intangible Consequences of Responding to Terrorism:

The unraveling of events and the interconnected reactions subsequent to a terrorist attack can produce a sequence of secondary consequences. Apart from the direct costs in material and human capital that stem from the emergency response to the attack, an evident change in the nation's stance towards the suppression and prevention of terrorism is observed while the economic impact of those changes that emerge to facilitate the new way of thinking can also be interpreted as a consequence of terrorism. For instance, experience from the events of September 11, 2001, firmly suggest that the fall out of terrorist events will be accompanied by an increase in the public and private sector's expenses directed towards security investments, this will naturally be followed up by an increase in insurance rates as firms and the public sector react to the new anticipated and naturalized threats. Terrorism-induced alterations concerning risk perception may also prompt individuals and firms to change their consumption and investment priority attitudes and preferences.[18]

2.4. Civil Liability and Maritime Terrorism

A terrorist attack is defined within the lines of destruction and harm brought upon people and property outside the context of conventional warfare. The victims of an act of terrorist aggression are commonly private citizens and commercial interests, for whom the dire request in the follow up of a terrorist attack is to recover and seek compensation for the damages they suffered. Despite all that, terrorism, still, presents problems regarding lawsuits filed by victims against terrorist perpetrators or state sponsors of terrorism owing to the difficulty of locating the terrorist fugitives or investigating the requisite evidence for enacting the penal indictment. [19]

Civil liability is a consequential aspect to evaluate when in the process of examining the totality of ramifications emerged from the threat of maritime terrorism. Liability is connected not only to the harmful consequences actually inflicted by an attack, but also in addition, to the complicated legal rules that shift associated costs from one party to another. Commercial shippers, ports, and vessel owners are liable for the terrorist attacks that strike at their own operations and are amongst the parties responsible for redistributing a substantial and potentially catastrophic set of terrorism risks. [20]

---

[17] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 35-36.
[18] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 36-37.
[19] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 39-41.
[20] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 39-41.

In the aftermath of an actual terrorist event, the costs of civil liability to the aforementioned parties could become enormous. Nevertheless, quantifying the magnitude of liability risk in conjunction with terrorist attacks remains a difficult prospect, since principles of accountability associated with such attacks are not fully settled under law. Liability problems related with maritime terrorism are particularly complicated since maritime commerce more than often incorporates entangled relations between numerous business entities that may share accountability for their shipping operations and that owe contractual obligations to one another. The means and guidelines of apportioning a terrorism liability risk among the aforesaid parties in association with a particular attack, necessitates detailed factual and legal questions. For the lawmaker the management of maritime terrorism liability and risk is hampered by constant overwhelming challenges constituting a warren of legal rules and jurisdictional issues. [21]

[21] Greenberg, Michael D., et al. *Maritime Terrorism: Risk and Liability*, page 39-41.

RECOMMENDATIONS

Maritime security has long been a serious concern for the International merchant shipping and maritime community, particularly since the 1980s. In order to ensure and enhance maritime security, our imperative must go beyond specific security measures and equal importance should be attached to both precaution and suppression. A summary of specific recommendations for improvement is reported below:

First and foremost, a culture of consciousness and a state of general wakefulness with respect to security matters should be maintained by governments and industry alike. Complementary, the self-activation of the employee should be encouraged by the maritime administration with incentives (economical or promotional) and proper guidance, highlighting the reciprocating benefits for the safety of the employed and the overall contribution to combating terrorism. Since, adding a security culture to worldwide shipping and cultivating a positive state of action by those who contribute in the daily running of the maritime industry, is the most cost-effective and efficient method of mitigating the malicious ramifications of a terrorist act or preventing it entirely, by making the security defenses of the industrious facilities impregnable.

In addition, the maritime administration and maritime police should amplify their coordination and cooperation in parallel, at an operational level, concluding in concerted efforts towards the domestic implementation of global treaty obligations and in compliance to the safety regulations sanctioned by the international maritime organizations.

Maritime security is a global concern in the current world with no exceptions for any maritime nation. However, every country is not capable of materializing the international requirements set for the prevention and suppression of terrorist incidents. Often enough, culpable for the lack of security measures is not the will or disinterest of the corresponding government but the absence of the necessary resources and minimal funding, needed in order to implement a security plan and enforce counter-terrorism measures within the country's maritime industrial sector, port facilities and territorial waters. Economic incentives and contributions formulated by the International policy makers and backed by its more affluent member-states should be considered, due to the fact that it is not feasible only by means of efforts conducted unilaterally by individual countries to address globally, through legal and technical measures, the phenomenon of maritime terrorism. Hence, by enabling less wealthy states to acquire the essential resources and technical knowledge to contribute to the world effort of combating terrorism, the global security level will be increased while at the same time limiting the effective range of terrorism, thus protecting worldwide shipping and the maritime transport sector by making every port a safe harbor and the sea waters of the world an area of free undisturbed commerce. Therefore, the investment of the wealthier maritime nations will be reciprocated and be mutually beneficial, as the benefits of such an act outweigh the costs in a modern interconnected mercantile world.

The Internationally enacted legislation for implementing the ISPS Code and its clauses is a fundamental requisite for the safety and the associated supervision and regulation of ships and ports. Nevertheless, shortcomings in the institutional legislation of

maritime security can be accumulated by the phenomenon of overregulation. Overregulation stems from the responsibilities and documentary requirements imposed on ships, companies and port authorities which many a time overwhelm the employees (officers on board and auditors alike), since time restraints, work fatigue and stress impair the proper implementation and evaluation of security measures. Leading, consequently, to bureaucratic formalism, when the training, tests, security plans, guidelines and measures of protection are formulated superficially due to the fatigue of the crew and anxiousness to complete the aforementioned tasks within the outlined time limits. Therefore, creating gaps in the security defenses of ships and ports and undermining the procedures preventing security threats from materializing. In consequence of the aforementioned, it is evident that a sufficient amount of time to repose should be given to the crew, during ship to port interface operations, and an auditor should ensure that the personnel involved are refreshed and in a healthy condition to respond to the demands of the security regulations prior to the berthing of the ship and the cargo operations of the port.

Finally, it is of vital importance to be noted, that inadequate consideration of cyber security in maritime regulations and a lack of worldwide cooperation for the suppression of cyber terrorism are observed within the maritime sector. It is essential, in our modern era, to acknowledge the need to define appropriate measures for ensuring the protection of critical infrastructure against cyber threats and cyber induced terrorism, while amplifying worldwide awareness towards this particular ascending type of menace. A direct consequence of inaction, absence of training and insufficient preparation for this newly emerged aspect of maritime security, would be the consistent exploitation of this breach in the security defenses of worldwide shipping in the foreseeable future, negating the inherited efforts of the world to suppress the phenomenon of maritime terrorism.

CONCLUSION

Maritime shipping is the backbone of world trade, the aspects of which, are regulated through multilateral treaties. The effectiveness of these agreed instruments is dependent on how the relevant provisions are implemented and enforced. The ISPS Code regulations form the international framework through which governments, ships and port facilities can co-operate to detect and deter acts which threaten the security of the maritime transport sector. The Code formalizes and standardizes globally the security measures while reducing the vulnerability of the maritime industry to an attack, thus countering the threat and reducing the risk. In addition, there are potential commercial benefits to the maritime industry in implementing the Code. Since evidently, in the long run, implementation of the Code shall provide considerable cost-benefits for the port industry as a whole and for the individual ports. As through the enactment of an effective and compliant security regime, ports will be able to continue to participate fully in the global trade and therefore the potential economic consequences of a major security breach, which might result in disruption or even port closure, can be averted.

The security requirements of the ISPS Code are a part of a wider United Nations effort for combating terrorism and should not be seen in isolation, since terrorism is not a matter of concern to one country or a group of countries, it is a global issue and should be addressed as such.

It is in the hands of governments and the maritime industry to adopt the internationally sanctioned measures, in order to enhance the maritime security and enforce successfully the protection of ships and port facilities from unlawful acts. Hence, in effect, establishing an entirely new culture amongst those involved in the day-to-day running of the shipping and port industry.

Prevention is always much better than the cure and failure to ensure compliance may have catastrophic repercussions on human life and the environment, it has also the ability to impair the commercial interests of the countries concerned while having harmful ramifications on the international trade and negatively impacting the world economy.

SOURCES

- ISPS Code 2003 Edition, International Ship & Port Facility Security Code and SOLAS Amendments 2002.

- IACS Recommendations, Recommendation 81, Guidance on the ISPS Code for Maritime Security Auditors, May 2003.

- Jesus, H. E. J. (2003), Protection of Foreign Ships against Piracy and Terrorism at Sea: Legal Aspects. The International Journal of Marine and Coastal Law, 18(3), 363–400.

- Greenberg, Michael D., Peter Chalk, Henry H. Willis, Ivan Khilko, and David S. Ortiz. Maritime Terrorism: Risk and Liability. RAND Corporation, 2006. http://www.jstor.org/stable/10.7249/mg520ctrmp.

- Bjørn Møller, Piracy, Maritime Terrorism and Naval Strategy. Danish Institute for International Studies, DIIS, 2009.

- Sam Bateman, Assessing the Threat of Maritime Terrorism: Issues for the Asia-Pacific Region.

- Abhijit Singh, Maritime Terrorism in Asia: An Assessment. ORF Occasional Paper No. 215, October 2019, Observer Research Foundation.

- Lutz Feldt, Dr. Peter Roell, Ralph D. Thiele, Maritime Security – Perspectives for a Comprehensive Approach, April 2013.

- Χριστόφορος Γ. Μπίσιας, International Ship & Port Facility Security Code, Εφαρμογή & Αντίκτυπος στην Ναυτιλία, Νοέμβριος 2003.

- Yingping Li, Addressing major maritime security issues of global regional and national significances: Law and Policy implications in the context of China, World Maritime University, Sweden, 2003.

- European Network and Information Security Agency, Analysis of Cyber Security Aspects in the Maritime Sector, November 2011.

- IMO,https://www.imo.org/en/OurWork/Security/Pages/GuideMaritimeSecurityDefault.aspx,«Maritime Security».

- IMO, https://www.imo.org/en/OurWork/Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx, «SOLAS XI-2 and the ISPS Code».

- IMO, https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/IMO%20and%20Maritime%20Security%20-%20Historic%20Background.pdf, «IMO and Maritime Security Historic background».

- IMO, https://www.imo.org/en/OurWork/Security/Pages/FAQ.aspx#What_is_the_ISPS_Code, «Frequently Asked Questions on Maritime Security».

- IMO, https://www.imo.org/en/OurWork/Safety/Pages/AIS.aspx, «AIS transponders».

- Edumaritime, https://www.edumaritime.net/stcw/general-requirements-for-masters, «What are the STCW Requirements for Master Mariner? ».

- INSBS Class, International Naval Surveys Bureau, https://insb.gr/Marine-Systems.ISPS-Code-related, «ISPS Code related».