2013

Progress and challenges : ten years after the ISPS code

Jibkwon Jeong
World Maritime University

World MARITIME UNIVERSITY
Malmö, Sweden

PROGRESS AND CHALLENGES: TEN YEARS AFTER THE ISPS CODE

Lessons from the Korean Experience

By

JEONG, JIBKWON

Republic of Korea

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

MASTER OF SCIENCE

In

MARITIME AFFAIRS

(MARITIME LAW AND POLICY)

2013

DECLARATION

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

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

Signature:

Date: 11 October 2013

Supervised by: **Lecturer Erin Williams**
World Maritime University

Assessor: **Professor Max Mejia**
World Maritime University

Co-assessor: **LCDR Mark Sawyer**
The United States Coast Guard

ACKNOWLEGMENTS

First of all, I would like to express my gratitude to the Korean Government and the Ministry of Security and Public Administration (MOSPA) that gave me the precious opportunity to study at prestigious university, WMU, and expand expertise in the maritime field in the belief that my studying will be highly beneficial for country.

My sincere appreciation also must go to my distinguished supervisor, lecturer Erin Williams who guided me in writing dissertation and provided me with valuable advices and comments which were eye-opening for me. In addition, I would like to thank former professor Max Mejia who is now working for his country, the Philippines, who accepted my proposal, and professor Carolina Romero who has delivered the valuable legal lectures to all of MLP students throughout the whole semesters.

Furthermore, I appreciate guidance from Professor Daniel Moon who has always encouraged me to maintain academic passion as well as balance of life in Sweden far away from my country. Besides, I must express my special gratitude to Professor Neil Bellefontaine, Ms. Lyndell Lundahl and Professor Patrick Donner who gave me an once-in-a-life time opportunity to continue studying, which will be definitely unforgettable for the rest of my life.

Throughout the whole period of time at WMU, the ESSP language course and passionate teachers, Anne Pazaver and Inger Battista, were indispensable for my studying. I dare to say that it would have been much more difficult if it had not been for the ESSP. In particular, I appreciate Anne’s sincere language review on my dissertation.

Lastly, my special thanks from the bottom of my heart go to my lovely wife, Jongjae Chung and my kids, Victoria and Hojin who stayed by me and encouraged my studying

for the whole period of time in Sweden as well as in Korea. Obviously, my dissertation would have been impossible without love and prayers from my mother Bunja Ahn and parents in law, Jinhee Chung and Munsook Choi.

I fully understand that the dissertation is not the final station of my academic journey but new beginning. I will not forget all the experiences as well as the sense of accomplishment in the process of writing dissertation, preparing examinations, making presentations and getting accustomed to new environment. I do believe every single moment at WMU will be valuable baseline for my life.

ABSTRACT

Title of Dissertation: **Progress and Challenges: Ten years after the ISPS Code**
- Lessons from the Korean experience

Degree: MSc

This dissertation is a study on the progress and challenges of the ISPS Code which has a ten-year history since it entered into force in 2004. The study started from the baseline that it was the right time to think about how effective this relatively young IMO instrument has been. The study has been done based on the real experiences of Korea in respect of the implementation of the ISPS Code.

In Korea, the ISPS Code has contributed to the enhancement of maritime security in many aspects; building capacity and infrastructure, raising awareness, successful hosting of internationally significant events and reduction of security incidents. However, there have been challenges; confusion out of discrepancy between the Korean ISPS Code Act and the IMO ISPS Code, narrow focus on ship/port interface, essential lack of IMO enforceability and lack of response to incidents.

Based on the progress and challenges of the ISPS Code in Korea, this dissertation provides recommendations to improve the security of the international maritime world; sophisticated legislation at the national and international level, buildup of IMO enforceability and response to incidents and so forth.

KEY WORDS : Maritime Security, ISPS Code, IMO, Security Level, Security Measures, Terrorism, National Legislation, Model Legislation, Supply Chain Security, USCG

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AEO	Advanced Economic Operator
AIS	Automatic Identification System
APEC	Asia-Pacific Economic Cooperation
CBP	Customs and Border Protection
CIC	Concentrated Inspection Campaign
CLC	International Convention on Civil Liability for Oil Pollution Damage
COLREG	Convention on the International Regulations for Prevention Collisions at Sea, 1972
CSI	Container Security Initiative
CSO	Company Security Officer
CSR	Continuous Synopsis Record
DA	Designated Authority
FAL	Convention on Facilitation of International Maritime Traffic
FBI	Federal Bureau of Investigation
FOC	Flag of Convenience
FUND	International Fund for Compensation for Oil Pollution Damage
GICOMS	General Information Center on Maritime Safety and Security
ICAO	International Civil Aviation Organization
ICIAP	ISPS Code Implementation Assistance Program
ILO	International Labour Organization
IPS Program	International Port Security Program
IMB	International Maritime Bureau
IMO	International Maritime Organization

ISPS Code	International Ship and Port Facility Security
ISSC	International Ship Security Certificate
KCG	Korea Coast Guard
KCS	Korea Customs Service
KIMFT	Korea Institute of Maritime and Fisheries Technology
KPA	Korea Police Agency
KRS	Korea Register of Shipping
MARPOL 73/78	International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto, as amended
LL	International Convention on Load Line, 1966
MI	Megaports Initiative
MOHW	Ministry of Health and Welfare
MND	Ministry of National Defense
MOF	Ministry of Oceans and Fisheries
MOJ	Ministry of Justice
MOLEG	Ministry of Government Legislation
MSC	Maritime Safety Committee
MTSA	Maritime Transport Security Act, 2002
NCI	National Critical Infrastructure
NIMASA	Nigerian Maritime Administration and Safety Agency
NIR	New Inspection Regime
NNSA	National Nuclear Security Administration
NPSP	National Port Security Program
OMA	Office of the Maritime Administration of Republic of the Marshall Islands
PFSA	Port Facility Security Assessment
PFSO	Port Facility Security Officer

PFSP	Port Facility Security Plan
Port-MIS	Port Management Information System
PSA	Port Security Advisory
PSC	Port State Control
PSVP	Port Security Visit Program
RFID	Radio Frequency Identification
RPSP	Regional Port Security Program
RSO	Recognized Security Organization
SOLAS	International Convention for the Safety of Life at Sea, 1974, as amended
SSAS	Ship Security Alert System
SSO	Ship Security Officer
SSP	Ship Security Plan
STCW	International Convention for Standards of Training, Certification and Watchkeeping for Seafarers, as amended
SUA	Convention for the Suppression of Unlawful Acts of Violence against the Safety of Maritime Navigation
SVSS	Small Vessel Security Strategy
SVS-IP	Small Vessel Security Implementation Plan
Tonnage	International Convention on Tonnage Measurement of ships, 1969
USCG	United States Coast Guard
VIMSAS	Voluntary IMO Member State Audit Scheme
WCO	World Customs Organization
WMD	Weapon of Mass Destruction

CHAPTER 1
INTRODUCTION

1.1 Study background

Quite a few people around the globe may think that the 9/11 terrorist attacks in 2001 is an old story which resulted in tremendous ramifications in many ways in terms of national security and anti-terrorism. However, the threat arising out of terrorism is an ongoing situation which was clearly evidenced in the Benghazi terrorist attack that killed the US ambassador to Libya on September 11, 2012 (Stephen, 2013). In addition, most recently, amid growing warnings of terrorism in August 2013, a number of Western countries including the US and UK stopped the activities of their embassies throughout the Middle East and Northern African countries. In particular, the UK raised its maritime Security Level to the highest (Level 3) in response to threats of terrorists in accordance with the International Convention for the Safety of Life at Sea, 1974, as amended (SOLAS 1974) chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code (Craig, et al., 2013). In other words, the threat of terrorism posed to security around the globe remains unchanged over time since 2001 and it is really an ongoing significant issue.

Totally 60 Conventions of the International Maritime Organization (IMO) have been adopted and 49 Conventions among them have entered into force as of 31 July (IMO, 2013f). Usually the adoption and the entry into force of conventions have resulted from disastrous maritime accidents; for example, the International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto, as amended (MARPOL 73/78) was introduced by the Torrey Canyon disaster in 1967, in which 120,000 ton of oil was spilled. Likewise, the International Convention on Civil Liability for Oil Pollution Damage (CLC) and the International Convention on the Establishment of an International Fund for Compensation for Oil Pollution Damage (FUND) were in the same path following maritime disasters.

In contrast, the ISPS Code, including the SOLAS chapter XI-2, is an exceptional case because it was introduced due to a non-maritime tragic incident, the 9/11 terrorist attacks. Though there have been maritime-oriented security incidents such as the hi-jacking of the Achille Lauro in 1985 and the USS Cole explosion in 2000, it is the author's opinion that the decisive driving force of the entry into force of the ISPS Code was the 9/11 incident, originating from outside the maritime field. The horrific effects of the 9/11 terrorist attacks on the World Trade Center and Pentagon in the United States shocked the world (McNaught, 2005). This tragedy showed explicitly that a ship also can be used as a weapon, as a means of transporting weapons or perpetrators, and as a means of directing funds to finance terrorist activities (Charalambous, 2003). This unprecedented and, moreover, catastrophic incident required drastic changes to the existing paradigm and structures.

The ISPS Code is the first maritime security regime to cope with terrorism. It has made a significant contribution to the enhancement of maritime security in many ways despite some shortcomings, which can be understood given the highly-speedy process from the drafting of the Code to its entry into force. This year, 2013, marks the tenth year since the ISPS Code took effect in 2004 and it will be highly meaningful and informative to look into the effectiveness of the relatively young IMO Convention and find ways to maximize the value of the existence of the ISPS Code through enhancement of its implementation.

Since the entry into force of the ISPS Code in 2004, the experiences and lessons Korea has acquired in the process of the implementation of the ISPS Code are worth sharing for the IMO Member States as well as for Korea itself. In this context, this paper will, first, look into the background and development of the maritime security regime, and salient features of the ISPS Code. It will then examine the effectiveness of the ISPS Code since its implementation in Korea, along with challenges that have appeared. Finally, it will suggest recommendations to mitigate these challenges in order to continuously promote maritime security.

1.2 Objectives

Before and after the entry into force of the ISPS Code, there have been numerous worldwide research activities in respect of its effectiveness, and expected consequences. In addition, Contracting Governments ranging from the Middle East to South America have submitted reports regarding the implementation of the ISPS Code in the form of documents to Maritime Safety Committee (MSC) meeting (IMO, 2009; IMO, 2010a). The real lessons experienced by the each Member State are worth considering given the short period of time since the ISPS Code has taken effect, in order for other Member States to be able to benchmark.

The Republic of Korea, as an active participant in the introduction and implementation of the IMO Instruments including the ISPS Code, proactively introduced national legislation and domestically implemented the ISPS Code in line with the initiation of the Code in June 2004. Even though the Korean government presented a report on the implementation of the ISPS Code to the IMO MSC eighty-ninth meeting in May 2011, the brief document was not enough to give sufficient information to other Contracting

Governments (IMO, 2011b) as it included summarized results and positive aspects without challenges and shortcomings evidenced in the process of the implementation of the ISPS Code.

This dissertation on the progress and challenges of the ISPS Code from the perspective of Korea based on practical experiences and lessons aims to achieve objectives as follows:

(a) Describe the background and evolution of the ISPS Code;
(b) Explain the process of the implementation and development of the ISPS Code in the Republic of Korea;
(c) Analyze the uniqueness and salient features of the Korean ISPS Code Act and practices in Korea in terms of effectiveness as well as challenges of the ISPS Code;
(d) Share information and lessons with the IMO Contracting Governments; and
(e) Make recommendations to enhance the enforceability and effectiveness of the ISPS Code at the national and international levels.

1.3 Scope of the study

This dissertation briefly deals with the background and implementation of the ISPS Code at the international level as a jumping-off point, and then looks into the cases and practices inside the Republic of Korea and identifies noteworthy points which are worth considering for Korea as well as the IMO Member States.

The effectiveness and challenges of the ISPS Code discussed in this paper are drawn from the Korean experiences and lessons; however, internationally valuable and remarkable references are also mentioned in this dissertation given the fact that Korean cases are not enough in some fields, and that internationally-recognized materials are highly recommended and relevant for the enhancement of the ISPS Code.

1.4 Research methodology

This dissertation makes use of quantitative and qualitative analysis. In terms of quantitative methodology, the study reviews the publicized reports of the Contracting Governments to the IMO including Korean reports and official materials. In contrast, the qualitative analysis is also used to extract the substantial key point from the intact data and materials; for example, the effectiveness of the ISPS Code from the reports of the International Maritime Bureau (IMB) on the piracy and armed robbery.

Chapter 2
Maritime Security and the ISPS CODE

2.1 Maritime security and terrorism

Maritime security is not a new issue. It has been a serious concern at the IMO since the 1980s (Mukherjee, et al., 2004). For the development of this paper, there is a need to clarify the difference in meaning between safety and security because the two concepts are hard to differentiate, and are, to some extent, confused by the general public and even by government officials in some cases. Maritime security can be defined as "those measures employed by owners, operators, and administrators of vessels, port facilities, offshore installations, and other marine organizations or establishments to protect against security incidents, terrorist attacks, seizure, sabotage, piracy, pilferage, annoyance, or surprise" while maritime safety is considered as being "those measures to prevent or minimize the occurrence of accidents at sea that may be caused by substandard ships, unqualified crew, or operator error" (Mejia, et al, 2004).

Among these threats, terrorism is the main target that the ISPS Code is primarily focused on, which can be defined by the US Federal Bureau of Investigation (FBI) as the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

The International legal regime to protect maritime security has been developed and adapted over the years to respond to different threats to the safety of maritime navigation. The development of the legal regime has gone through three main stages. The objective of the first stage was to protect ships and crews from attacks by persons on board another ship (Mensah, 2003). At that time, the issue centered on piratical attacks upon merchant ships and it soon evolved to include practically-performed acts in coastal water jurisdictions, which has been termed armed robbery (Mukherjee, et al., 2004).

Then, as the second stage, the subject of maritime security has been high on the agenda of the IMO since the deliberations leading to the adoption of the Suppression of Unlawful Acts Convention (SUA) in 1988, which itself was triggered by the Achille Lauro incident in 1985. The Achille Lauro incident, where a group of Palestinians seized a cruise ship in the Mediterranean Sea and murdered a disabled passenger on board, convinced the international community that the traditional law of piracy was not adequate to deal with new and emerging forms of violence against shipping. Consequently, it was agreed that a new legal regime was needed to address the new situation. In response to this incident, the IMO adopted the new treaty, SUA Convention in 1988. This Convention imposed an obligation on all States Parties to make offenses punishable under their national laws and required that the penalties should be appropriate, taking into account the grave nature of the offences.

The tragedy of 11 September 2001, the direct cause of the third stage of maritime security, together with a number of security incidents involving vessels such as the Our Lady of Mediatrix (2000), USS Cole (2000), Limburg (2002), Superferry 14 (2004) and the dramatic rise in acts of maritime violence against merchant ships, particularly in southeast Asian waters, brought maritime security to the forefront of concerns in the shipping world. In particular, the use of hijacked planes demonstrated clearly that additional measures were needed not only to prevent attacks that endanger ships and persons and property on board the ships but also to prevent ships from being used as instruments or threats of terrorist activities (Mensah, 2003). Finally, the era of the ISPS Code began in 2004 through a relatively short period of preparation.

2.2 Development and implementation of the ISPS Code

In December of 2002, the twenty-second session of the Assembly of the IMO agreed on the development of new measures relating to the security of ships and port facilities for adoption by a Conference of Contracting Governments to SOLAS and thus, preparation for the diplomatic conference was entrusted to the Maritime Safety Committee (MSC). The diplomatic conference convened by the IMO adopted new provisions in the SOLAS (chapter XI-2) and other SOLAS amendments including the requirement for ships to fit Automatic Identification Systems (AIS), to carry a Continuous Synopsis Record (CSR), and to standardize ship identification markings (IMO, 2012c). At the beginning, the revision of the legal framework had been undertaken in respect of the two relevant treaties, i.e., the 1988 SUA Convention and the 1974 International Convention on Safety of Life at Sea (SOLAS). In the meantime, work has been completed on amendments to the 1974 SOLAS Conventions (Mensah, 2003).

The ISPS Code was promulgated in 2003, and came into force 1 July 2004 in a speedy manner while there were concerns held in some quarters about the unrealistic timeframe (Botelho, 2004) and potential disruptions to international trade. However, the US, devastated and shocked by the unthinkable terrorist attacks, pressured the IMO, and an international agreement was reached on the introduction of the ISPS Code (Robertson, 2011). Indeed, the environment was highly political and emotionally charged (Franson, 2003).

Naturally, the objectives and contents of the ISPS Code are largely equivalent to the US

Maritime Transportation Security Act (MTSA) which was enacted in 2002 (Ng, 2009). The rationale for the ISPS Code being introduced is a security issue, driven by the political impetus and reaching into the sphere of State security (Burmester, 2006).

2.3 Salient features of the ISPS Code

The security regime of the IMO is encompassed in SOLAS Chapter XI-2, in which Regulations (1~13) are stipulated and there is a sub-regime, the ISPS Code, which consists of two main components. Part A provides the minimum mandatory requirements that ships and port facilities must follow while Part B, not mandatory, provides more detailed guidelines and recommendations. This Section will look into key points of the Code which are relevant and closely related to the ISPS Code's effectiveness and challenges.

The main objectives of the Code are as follows (IMO, 2012c):

(a) To establish an international framework involving cooperation between Contracting Governments, government agencies, local administrators, the shipping and port industries to detect/assess security threats, take preventive measures against security incident;
(b) To establish the respective roles and responsibilities of all these parties concerned;
(c) To ensure the early and efficient collection and exchange of security-related information;
(d) To provide a methodology for security assessments so as to have in place plans and procedures to react to changing Security Levels;
(e) To ensure confidence that adequate and proportionate maritime security measures are in place.

In terms of the scope of application of the ISPS Code, ships engaged on international voyages, as stated below, and port facilities serving international ships are subject to the ISPS Code. Not all international vessels are subject to the ISPS Code in case of cargo ships under 500 gross tonnage and, moreover, small vessels which are able to navigate internationally in practice but are classified legally as domestic vessels can cause vulnerability to maritime security.

(a) Passenger ships, including high-speed passenger craft;
(b) Cargo ships, including high speed craft, of 500 gross tonnage and upward;
(c) Mobile offshore drilling units.

Part A of the ISPS Code, which is mandatory, overall stipulates Responsibilities of Contracting Governments (Section 4), Ship Security (Section 6 to 12) and Port Facility Security (Section 14, 15 and 16). In particular, each Contracting Government has authority to set out the Security Level in accordance with the following criteria stipulated in Part A of the Code as follows:

(a) Level 1 : Normal, the level at which the ship or port facility normally operates; minimum appropriate protective security measures;

(b) Level 2 : Heightened, the level applying for as long as there is a heighted risk of a security incident; additional protective security measures;

(c) Level 3 : Exceptional, when there is the probable or imminent risk of a security incident; further specific protective security measures.

Security Level and detailed security measures under each level are essential elements of this paper whose main topic is the effectiveness and challenges of the ISPS Code as security level and related measures were verified as the source of effectiveness and challenges based on Korean experiences.

Part B which is recommendatory stipulates more detailed regulations in respect of Part A. Specifically, Part B stipulates the precise security measures of ship and port facilities under Security Levels 1, 2 and 3, respectively. Part B is essentially not mandatory but in the case of Korea some parts of Part B became mandatory through the process of national legislation, which was the source of a problematic situation amid actually raising the Security Level.

CHAPTER 3

IMPLEMENTATION OF THE ISPS CODE IN KOREA

3.1 Introduction

The 9/11 terrorist attacks drastically impacted not only on air transportation and shipping but on the world as a whole (Franson, 2003). The disaster took place in the heart of the US but the repercussions spread around the world as evidenced by the introduction of the ISPS Code in the maritime field. The Republic of Korea was not an exception. Actually, Korea was also tremendously affected because Korea, as a trade-oriented country, is highly dependent on international trade in which carriage of goods by sea accounts for an overwhelming portion. New systems and regulations resulting from the 9/11 incident and the ISPS Code led to significant changes in Korea.

3.2 Social and historic uniqueness of security in Korea

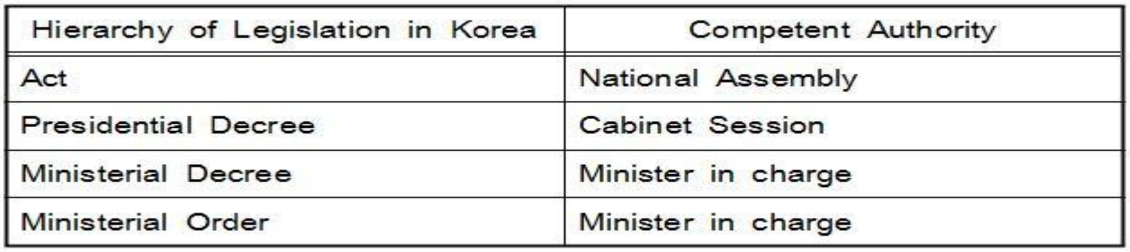
When it comes to maritime security, the Republic of Korea has a long history compared to other countries, which mostly have focused on security issues following the catastrophic terrorist attacks in 2001. The Korean peninsula was divided right after Japan surrendered to the US and its allies at the end of World War 2 in 1945 because the former Soviet Union and the US respectively took control of half of the Korean Peninsula; the US was stationed in South Korea and the Soviet Union was on the opposite side, the Northern region of the Peninsula.

At first, both superpower countries were in a good relationship but sooner or later there started the Cold War, in other words, confrontation between the US and Soviet Union. One ramification of the beginning of the Cold war was the Korean War during which North Korea, with the support of the Soviet Union, unilaterally and unexpectedly invaded South Korea in 1950 and failed to communize the Southern region of the Peninsula.

In the aftermath of the Civil War, the South Korean government came up with a wide range of national defense regimes ranging from civil readiness to a military system. Naturally, the top priority of the Korean government was to maintain national security, and to detect and deter North Korean provocation. In this context, there have been several security regimes in South Korea ranging from military mobilization system in case of all-out war to protection of National Critical Infrastructure (NCI) such as airports, seaports, dams and government buildings. Strictly speaking, it is also true that the 9/11 terrorist attacks aroused the sense of security awareness in the Korean people in terms of terrorism, but Korea already had an established system to address security threats.

3.3 Existing maritime security regime

The structure of Korean national legislation is established in this hierarchical order; Act, Presidential Decree (equivalent to Executive Order in the US), Ministerial Decree and Ministerial Order, which is the lowest level of the legal framework.



Hierarchy of Legislation in Korea	Competent Authority
Act	National Assembly
Presidential Decree	Cabinet Session
Ministerial Decree	Minister in charge
Ministerial Order	Minister in charge

Table 1 The Structure of Legislations in Korea (Source : Edited by Author)

These four types of legislation have different enforceability. An act passed by the National Assembly has the highest enforcing power in the private as well as public sector with penalty articles, which can impose fines or terms in prison. In contrast, the remaining legislations do not have authority to impose fines or terms in prison; in other words, sub-Act legislations cannot carry out punitive measures in the private sector. However, they can impose administrative measures such as a negligence fine on the private sector in case of violation of legislation.

In Korea, there have always been strict security and safety systems to protect sovereignty, social stability and peace from a neighboring country that has posed a threat to Korea. In respect of the maritime field, there is a preexistent security regime called "Presidential Decree on National Security" with articles relevant to the security of port facilities and significant vessels. This law designates the National Critical Infrastructure (NCI) which includes port facilities and significant vessels vital for the nation in terms of economic impact and strategic importance in the event of war (MOLEG, 2008).

This legislation has been applied to the security and physical protection of NCI but it is also true that it had significant limitations in terms of effectiveness because it was not passed at the National Assembly (Legislature of Korea) which is equivalent to the Congress in the US. In the Korean legal system, low-level legislation which has not passed the National Assembly, such as the Presidential Decree, cannot stipulate penalty articles in case of violation from the civil side even though it has controlling power when it comes to the public sector under the influence of the president who is the commander in chief in respect of administration. Of course, nuclear power plant-related legislation was passed by the National Assembly but this was actually an isolated case before the enactment of the Korean ISPS Code Act (formally called 'Act on the Security of International Ships and Port Facilities') in Korea.

For a long time, therefore, there had been demand for a higher level of legislation for the security and physical protection of NCI including port facilities and ships which are significant for national security. However, these demands ended in a failure out of concerns about overregulation amid a social atmosphere aspiring to more and more freedom and rights of access and knowledge of NCI in the process of democratization.

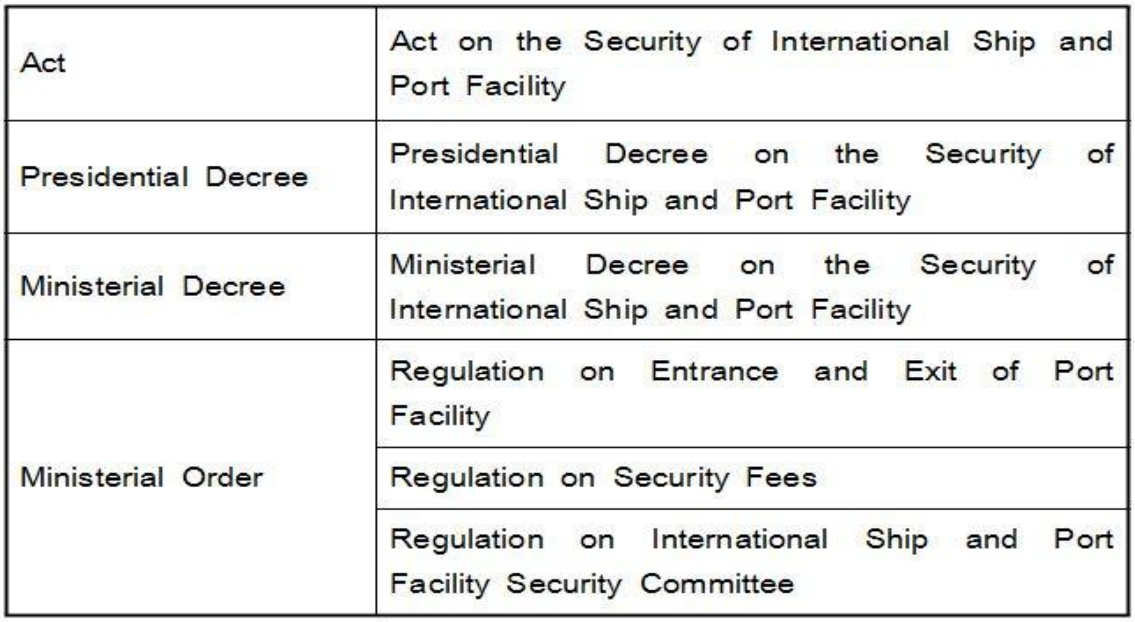
3.4 National legislation of the ISPS Code

The Republic of Korea was also devastated by the 9/11 terrorist attacks given the close relationship between Korea and the US in almost every way, including security alliance. It is a widely-recognized fact that Korea and the US are aligned through a mutual defense treaty when it comes to security issues, facing almost the same threats in the Asian region. Korea proactively joined the movement to adopt a whole new international maritime security regime under the leadership of the IMO and spearheaded by the US. In fact, the Korean Government legislated a domestic Ministerial Order in October 2003, which is the lowest legal regime, to enforce the ISPS Code which was scheduled to enter into force in July 2004 because there was not enough time for the Korean government to enact Act-level legislation. An existing Presidential Decree on National Security handled a wide range of National Critical Infrastructure (NCI) so new legal regime relevant to the ISPS Code was necessary.

Over time, demand for higher level legislation had been continuously raised and finally the Korean ISPS Code Act passed the National Assembly in February 2007. This new Act was well-stipulated with penalty articles and, overall, reflected the IMO ISPS Code to a satisfactory level, notwithstanding some parts to be desired .

3.5 Salient features of Korean ISPS Code Act

The Korean ISPS Code Act is a domestic version of the ISPS Code adopted by the IMO, but the Korean Act has several unique characteristics, different from the IMO ISPS Code, reflecting the Korean social and legal circumstances as follows:



Act	Act on the Security of International Ship and Port Facility
Presidential Decree	Presidential Decree on the Security of International Ship and Port Facility
Ministerial Decree	Ministerial Decree on the Security of International Ship and Port Facility
Ministerial Order	Regulation on Entrance and Exit of Port Facility
	Regulation on Security Fees
	Regulation on International Ship and Port Facility Security Committee

Table 2 The ISPS Code legislations in Korea
(Source :Edited by Author from www.law.go.kr)

(a) Article 5 – National Port Security Program

The Korea Act stipulates the National Port Security Program (NPSP) in line with existing Korean Acts. In most cases, Korean Acts set up national plans and national committees to deal with national plans and strategy. Newly-legislated Korean ISPS Code Act also followed the Korean legal practice. This NPSP must be endorsed by the Korean International Ship and Port Facility Security Committee (ISPS Committee) which is regulated in Article 34. The National Port Security Program is aimed at the consolidation and harmonization of maritime security measures at the national level and establishment of security measures and contingency plans against security incidents to the National Critical Infrastructure.

Basically, this plan was set up with the principle that it must be valid and useful for the upcoming decade based on the reasonable forecast for the future threats and circumstances. The current NPSP was set up by the Ministry of Oceans and Fisheries (MOF) and finally approved by the International Ship and Port Facility Security Committee (ISPS Committee) in 2008, which is explained below.

The National Port Security Program includes long-term policy, strategy and planning in respect of maritime security. The Korean maritime world must follow this program as the baseline of security. This program is nationwide and stipulates the Regional Port Security Program (RPSP) in accordance with National Port Security Program. 11 Regional Port Offices drew up the Regional Port Security Program through coordination with other agencies concerned on the basis of the National Port Security Program.

(b) Article 6 - Setting and change of Security Level

The setting and change of Security Level must be discussed and decided by the Security Committee well-stipulated in Article 34. Security measures in detail under each Security Level from 1 to 3, are regulated in the Ministerial Decree on the ISPS Code.

(c) Article 19 – Port State Control

The Korean government can carry out Port State Control inspections on foreign vessels entering Korean ports pursuant to this Article. Detention, limitation of movement inside the port facility, requirement for corrective measures and banishment measures can be taken against security-substandard foreign vessels based on the results of Port State Control. In addition, according to the results of reviewing the ship security information transmitted from the vessel to the competent authority, limitation of movement, requirements for corrective measures, inspection of the vessel and even refusal of call of a port can be enforced.

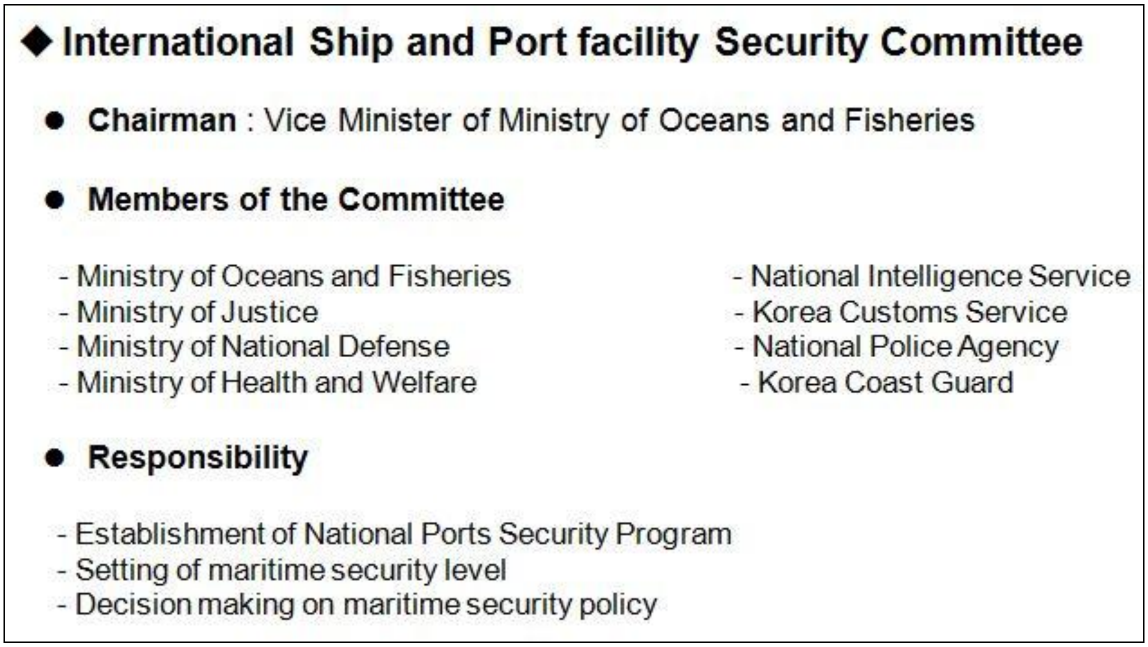
(d) Article 31 – Acquisition of security personnel, equipment and facilities

The owner of a port facility or an international ship must obtain personnel, equipment and facilities necessary to maintain security at his or her own expense. This article is in line with other existing security legislation. Given the shortage of national budget, the Korean Government has enacted domestic legislation giving obligation to the owners of National Critical Infrastructure falling outside the scope of the public sector; to meet security requirements at their own expenses.

Indeed, the private sector sometimes complains that security affairs belong to the public sector and, therefore, the expenses must be granted and, at least, partially, supported by the government. Demand from the private sector looks reasonable on the one side but the Korean government has taken a stance that the private sector must also assume a financial burden because security is also an essential prerequisite of business prosperity in the sense that good business is guaranteed by good security. This standpoint has been applied in the process of legislation of the ISPS Code in Korea.

(e) Article 34 – International Ship and Port facility Security Committee

The International Ship and Port Facility Security Committee (ISPS Committee) is presided over by the Deputy Minister of Oceans and Fisheries and composed of high-level representatives of governmental agencies concerned; Ministry of Justice (MOJ, in charge of immigration), Ministry of National Defense (MND), Ministry of Health and Welfare (MOHW, in charge of quarantine), Korean Customs Service (KCS), National Intelligence Service (NIS, in charge of intelligence collecting and sharing), Korean Police Agency (KPA) and Korea Coast Guard (KCG).



◆ **International Ship and Port facility Security Committee**

- **Chairman** : Vice Minister of Ministry of Oceans and Fisheries
- **Members of the Committee**

  - Ministry of Oceans and Fisheries
  - Ministry of Justice
  - Ministry of National Defense
  - Ministry of Health and Welfare
  - National Intelligence Service
  - Korea Customs Service
  - National Police Agency
  - Korea Coast Guard

- **Responsibility**

  - Establishment of National Ports Security Program
  - Setting of maritime security level
  - Decision making on maritime security policy

Figure 1 Korean International Ship and Port Facility Committee

(Source : Edited by Author from the Korean ISPS Code Act Article 34)

The responsibility of the ISPS Committee is established under the National Port Security Program and includes setting and changing national maritime Security Level and decision making on maritime security policy and systems. Even though the ISPS mission belongs to the jurisdiction of the Ministry of Oceans and Fisheries, this Committee was created in order to maximize the effectiveness of national security policy because inter-agency cooperation and close coordination is required.

(e) Article 42 – Port facility security fees

This Article is closely related to Article 31. Given the financial burden arising out of security requirements ranging from hiring security personnel to acquisition of security equipment, the Korean government came up with a policy regarding security fees. The owner of a port facility may garner security fees from port users ranging from international passengers to shipping companies to cover expenses in accordance with Article 31; it is not compulsory and the final decision to garner fees is up to the owners of the port facilities. However, this Article is not popular in the field because newly-created security fees can undermine the competitiveness of port facilities and it has made private port facilities reluctant to collect security fees. In total, seven private port facilities started to garner security fees in accordance with Article 42 since 2011.

(f) Articles 47 through 52 – penalties

In cases of violation of the Act, strict law enforcement became legally possible by means of fine or imprisonment, which is hugely different in comparison with the existing 'Presidential Decree on National Security', which have not legal authority to impose penalties to the private sector. In the realm of Korean legislation, the existence of penalty articles is significantly important in enhancing the enforceability of the legislation.

3.6 Implementation of the ISPS Code in Korea

As mentioned in section 3.4 (National legislation of the ISPS Code), the legal framework of the ISPS Code in Korea has been evolved from lowest-level Ministerial Order in 2003 to the highest-level Act which passed the National Assembly in 2007. At the beginning of the ISPS Code regime, the legal basis was not fully robust but there was not much confusion or opposition from the private sector.

In preparation for the entry into force of the ISPS Code, the Ministry of Oceans and Fisheries (MOF) formed a professional group to reflect SOLAS chapter XI-2 and the ISPS Code in domestic law in order to develop and provide a model for a ship security plan (SSP) and a port facility security plan (PFSP). The government also fully supported the industry by appointing security training organizations and recognized security organization (RSO). These efforts were so successful that, as of July 1 2004, the Republic of Korea had established SOLAS and ISPS Code-compliant security systems for 425 Korean flagged vessels and 123 port facilities called upon by foreign vessels and implemented corresponding security activities (IMO 2011b).

CHAPTER 4

EFFECTIVENESS OF THE ISPS CODE IN KOREA

4.1 Introduction

With the rapid implementation of the ISPS Code, there were concerns held in some quarters about the unrealistic timeframe and potential disruptions to international trade (Botelho, 2004); however, the predicted chaos did not eventuate (Wright, 2005). In addition, the IMO reported that ships had reached a 'high degree of compliance' with minimal disruption to world trade, and that Contracting Governments had approved security plans for 97 percent of declared port facilities (IMO, 2005a). The Code has achieved many of the desired goals, particularly when compared to many other similar initiatives, which were either abandoned or have yet to be widely implemented in terms of creation, implementation and enforcement (Timlen, 2007). This chapter reviews the positive results of the ISPS Code implementation in Korea based on real experiences and lessons.

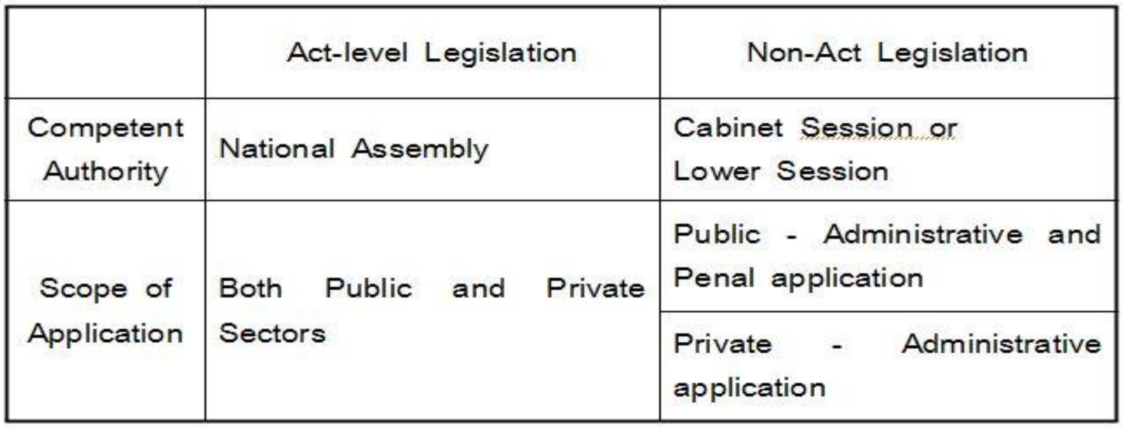
4.2 Building capacity and infrastructure in respect of maritime security

The ISPS Code is the first IMO instrument to address maritime security threats and requires Contracting Governments to enact domestic legislation to enforce security measures based on the SOLAS Chapter XI-2. Even though some countries such as the Republic of Korea and the Islamic Republic of Iran had existing legislations in respect of maritime security in the forms of ship and port security measures, most countries did not have such legislations to enforce security measures prior to implementing the Code

(IMO, 2009; IMO, 2011b).

In the case of the Republic of Korea, it had designated port facilities as National Critical Infrastructure (NCI) in accordance with the Presidential Decree on National Security even before the Code came into force. The Korean government, however, took advantage of the new international convention to step up maritime security during the time between 2004 and 2013 as follows (IMO, 2011b):

(a) Act-level legislation endows more legal and administrative enforceability to relevant government organizations with articles stipulating offenses and penalties;



	Act-level Legislation	Non-Act Legislation
Competent Authority	National Assembly	Cabinet Session or Lower Session
Scope of Application	Both Public and Private Sectors	Public - Administrative and Penal application
		Private - Administrative application

Table 3 Comparison between Act-level and non-Act legislations
(Source : Edited by Author)

(b) Established General Information Center on Maritime Safety and Security (GICOMS) as a single national contact point to receive all ship security alerts from Korean-flagged vessels and to share information concerning security. In fact, the establishment of the GICOMS was the outcome of the implementation of the ISPS Code and afterwards it turned out to be effective in protecting vessels and seafarers from attacks by pirates in dangerous waters. The primary reason to establish the GICOMS was that the IMO made it mandatory to install Automatic Identification System (AIS) and Ship Security Alert System (SSAS) onboard ships after the 9/11 incident. At the heart of Korea, the Korean government could track the movement of international vessels navigating dangerous waters, off the coast of Somalia or at the Western Indian Ocean and share information transmitted from the vessel under attack with naval vessels or other merchant fleets;

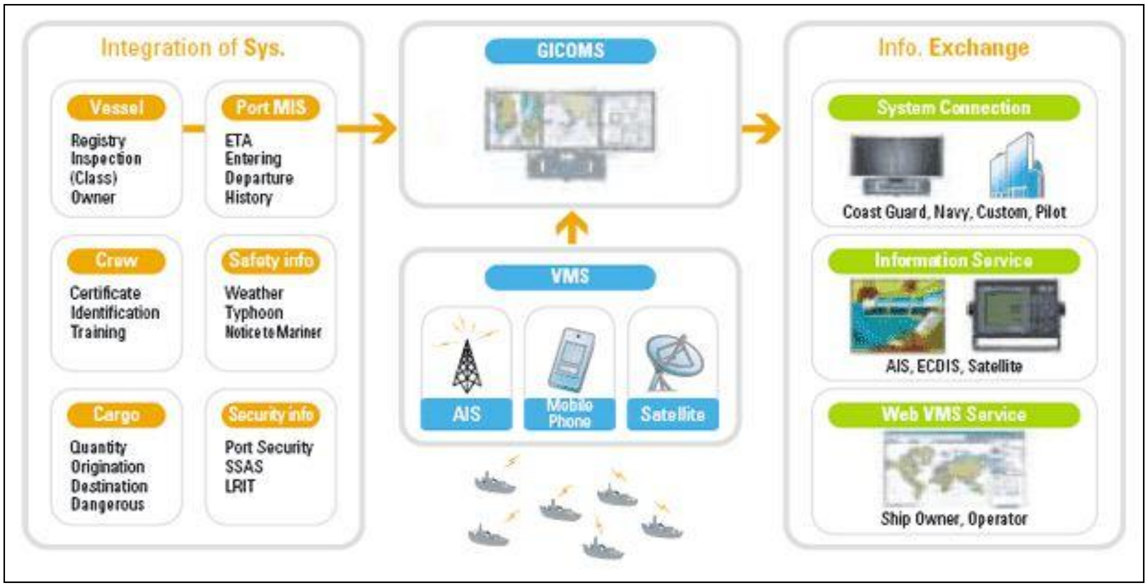


Figure 2 Composition of GICOMS

(Source : Captured by Author from http://www.yesport.go.kr/eng.2010/infGicoms.htm)

(c) Issued International Ship Security Certificates (ISSC) and approved Ship Security Plans (SSP) for approximately 1,191 Korean-flagged vessels to which the ISPS Code applies;

(d) Designated 177 port facilities, as of September 2013, within Korean territorial waters to apply the ISPS Code. Korea approved Port Facility Security Plans (PFSPs) on the basis of Port Facility Security Assessment (PFSA) in compliance with the ISPS Code, and issued Statements of Compliance of a Port Facility to all designated port facilities.

(e) The Designated Authority (DA) appointed the Korea Institute of Maritime and Fisheries Technology (KIMFT) and the Korean Register of Shipping (KRS) as the organizations for ship security training. A total of 6,105 personnel under KIMFT, and 1,506 personnel under KRS have completed the training course for ship security officers since 2003. In addition, a total of 1,009 new personnel have completed the training course for PFSOs from KRS and 1,476 personnel have completed refresher course to obtain the latest security information;

(f) The DA has carried out exercises recommended in the ISPS Code Part B 13.7 yearly since 2005 and posted the names of participants on a website to make it easier for shipping companies to access the data for the exercises as evidence for Port State Control (PSC) inspections and other ISPS verifications;

(g) In order to have appropriate capability as a flag State to undertake ISPS Code verification for Korean-flagged vessels, 80 Port State Control Officers (PSCO) for ship inspection and ISPS Code verification were newly employed before 1 July 2004. This number has been supplemented with an additional 35 PSCOs since then;

(h) In 2011, Korea established an access control system based on Radio Frequency Identification (RFID) at six major ports as the first step of the enhancement of access control as well as the flow of cargo. Since the introduction of the ISPS Code, Korean government and agencies concerned have tried to determine how to optimally balance between security and facilitation of trade.

When it comes to only security, facilitation of trade and swift flow of goods could be under-evaluated topics. However, the Korean government realized the importance of the facilitation of trade in that it must be done in tandem with the strengthening of security.

In this context, as an example, six major ports installed the advanced access control system, RFID, which can detect registered information regarding vehicles and personnel. The effectiveness of the advanced access control system has been proved and, therefore, the Korean Government has been trying to broaden the installation of the RFID to the remaining ports (Park, 2011; IMO, 2011b);

(i) Ship security information has been able to be transmitted inside the framework of the Port Management Information System (Port-MIS), which is the electronic system to be able to collect, share and process the information with regard to vessels calling or departing port facilities. At the moment, the Port-MIS of Korea has numerous functions relating to port management as well as security information. Once the personnel in charge of Port-MIS in a specific port accept the request of calling or departing port, this decision and information about the vessel is automatically disseminated through government agencies concerned with immigration, customs clearance, quarantine and so on;

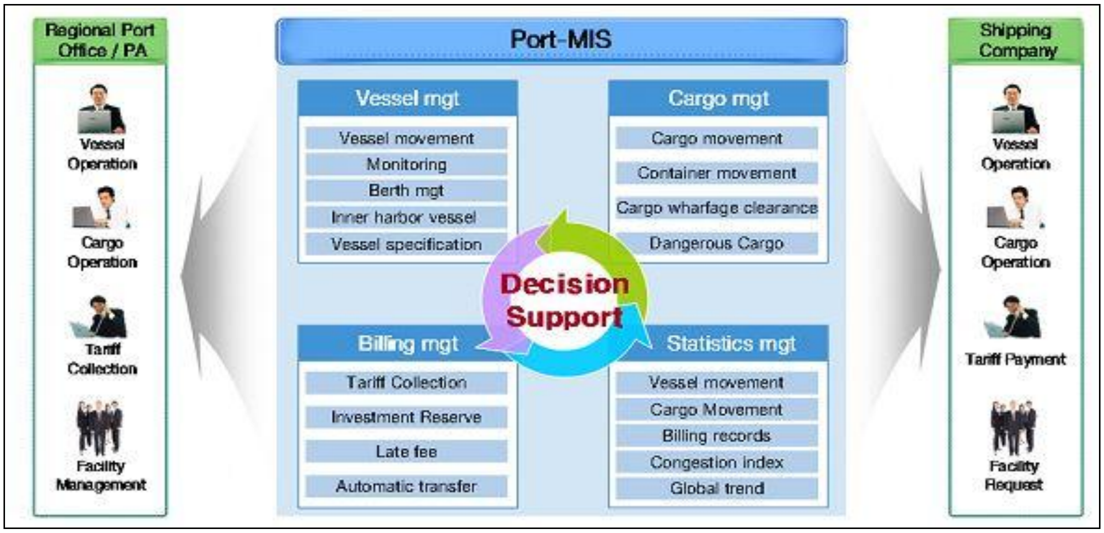


Figure 3 Concept of Port-MIS

(Source : Captured by Author from http://www.klnet.co.kr/english/product)

(j) At the end of 2011, a meaningful measure was accomplished; sharing of surveillance cameras between Port Authority and Customs Service in order to achieve an enhanced security system and utilize the national budget in a more efficient and reasonable manner. This unprecedented cooperation between government agencies was worth commending in that the agencies, in a sense, gave up established and exclusive rights to the equipment bought and installed by means of tax-payers money. In particular, Korea Customs Service (KCS) has installed the most advanced and high-end surveillance cameras in and around the port facilities so as to deter and detect smuggling attempts, so the Port Authority can now take advantage of the KCS's equipment (MOF, 2011).

4.3 Raising the maritime security awareness

The level of awareness of maritime vulnerability to terrorist attack has been increased through the implementation of Part A of the ISPS Code, and if nothing else, the maritime industry should be better prepared for any future terrorist attack (McNaught, 2005). The raising of the awareness level is a right step given the IMO standpoint and goal "To create the necessary security culture and raise our defenses so high that the shipping industry does not become a target for terrorist activities" (IMO, 2004b).

The ISPS Code has raised the security awareness of Korea in two categories. The first one is the ISPS Code made Korean people realize that threats to security could come from outside Korea such as international terrorists groups, not only from inside Korea. Secondly, it removed, to some extent, the sense of honorable treatment from the government side when government officials do business with the private sector.

(a) Raising security awareness

As mentioned in Chapter 3 and section 3.2 (Social and historic uniqueness of security in Korea), Korea primarily focused on the protection of the country and prevention of provocation from its neighboring country, North Korea. However, it has not always been the case that both South and North Korea were in the relationship of military or rhetorically-hostile confrontation. From 1998 through 2007, there was drastic change between the two countries; close collaboration in terms of economic cooperation, a series of reunions of families who were forced to separate during the Civil War from 1950 to 1953 and even the first Summit meeting in 2000.

Amid this kind of social atmosphere inside South Korea, the awareness of people to security issues declined noticeably and, subsequently, attention to national security and possible enemy of the state was regarded as outdated. During those ten years, the overall social atmosphere in respect of security and national defense was undermined and rights of free speech and right to know of the general public outweighed the importance of security and safety issues.

In this atmosphere, the introduction of the ISPS Code enlightened the general public that security is vital not only inside the Korean Peninsula but also around the world. Korea is basically a trade country which imports raw material and exports manufactured goods by sea. In order to address threats from terrorist attacks in the maritime field, a newly-created security regime was useful in regaining the security awareness of Korean people. As an example, in 2004 there was a warning that a terrorist group might attack Korean-flagged vessels or even Korean port facilities in protest against Korean collaboration with the US over the Iraqi reconstruction plan (Cho, 2004).

Without cease, maintained security awareness was vital for in addressing real attacks and provocation such as detonation of nuclear bombs, launch of long-range missiles and artillery attacks on Korean territory from its neighboring country when the 10 year period of relative friendliness ended. Even during those years, there had been numerous small and large provocations such as sudden attacks on Korean naval patrol vessels with casualties. The importance of an appropriate level of security and seamless preparedness cannot be stressed enough. The ISPS Code has made it possible for Korean people, including the private sector as well as public sector, to maintain security awareness and security measures stipulated in the ISPS Code and Korean legislation.

(b) Strict adherence to identification requirements

As Timlen (2007) pointed out, even various officials who were initially hesitant to comply with requests to provide their identification at ships' gangways are familiar with the need to do so. Given the officials' speed of response to the new regime and the sense of authority, awareness of security has been heightened at all levels, in the private and public sector.

Korea, like other Asian countries, has a long culture wherein government officials are regarded as privileged social elites to be exempted from complying with legislation in some cases such as showing identification when entering a port facility. It was a longstanding practice but now it has become common sense for any government official to show identification when he or she enters a port facility or board a vessel by virtue of the implementation of the ISPS Code, which was an international regime.

In 2004, the USCG visited the Korean ports with a view to checking the level of compliance of Korean ports with the ISPS Code as part of the International Port Security (IPS) Program. At that time, the Korean government and agencies concerned were so worried about the result of the USCG inspection that Korea prepared for the visiting inspection in every possible way. Finally, on that day the USCG inspection team arrived in Busan port, they were allowed to enter the port without any kind of checking control at the gate. From the Korean perspective, allowing visitors to enter a port facility without a security check is a consideration for important and high-level visitors. However, this act was pointed out by the inspection team as non-compliant with the ISPS Code. This incident became the alarm bell to the whole maritime field in Korea and, since then, at the gates of port facilities and ships, it has become normal for visitors to show their identification and explain the objectives of their visit.

The ISPS Code and a series of visiting programs from overseas has removed the longstanding bad practice of the public sector and as a consequence facilitated the soft-landing of the ISPS Code in Korea.

4.4 Achievements of the ISPS Code in Korea

4.4.1 International recognition

(a) IMO Audit Program

Korea accepted the Voluntary IMO Contracting Government Audit Scheme (VIMSAS) from the IMO audit team in April 2007 in respect of six significant IMO instruments; International Convention for the Safety of Life at Sea, 1974, as amended (SOLAS), International Convention for the Prevention of Pollution from Ships, 1973, as modified by the Protocol of 1978 relating thereto and by the Protocol of 1997 (MARPOL), International Convention for Standards of Training, Certification and Watchkeeping for Seafarers as amended, including the 1995 and 2010 Manila Amendments (STCW), International Convention on Load Lines, 1966 (LL), International Convention on Tonnage Measurement of Ships, 1969 (Tonnage) and Convention on the International Regulations for Prevention Collisions at Sea, 1972 (COLREG).

It was found that Korea had been carrying out the implementation of the IMO Mandatory Instruments successfully, without any non-conformities, and with only three observations and without any non-conformities; the difficulty to find the status of the Korean legislations of the IMO Conventions, the difference in legal interpretation of the certification of ship inspector between Korean regulations and IMO Conventions and thirdly, the lack of post-measures after inspection on Korean-flagged vessels. The ISPS Code is also one element of SOLAS and it can be reasonably inferred that the implementation of the Code in Korea was found appropriate by the IMO audit team (Lee, 2007).

(b) USCG IPS Program

Since 2004, USCG experts have visited Korean international port facilities four times; 2004 July, 2008 February, 2010 May and 2012 July. The USCG recognized that Korean port facilities are well-organized for the implementation of the new maritime security regime (Kim, 2004). In return, a Korean delegation has visited US port facilities three times on a reciprocal basis in order to look at best practices and create framework for information sharing and international cooperation between Korea and the US.

(c) Asia-Pacific Economic Cooperation (APEC) Program

Along with the IMO, APEC has been trying to enhance maritime security by means of its own program, the ISPS Code Implementation Assistance Program (ICIAP). The aim of the ICIAP program is to assist APEC Economies in developing the capacity required to effectively implement the ISPS Code through three-phase activities as follow. Phase 1 is raising awareness of the ISPS Code requirements and assisting developing Economies to develop a framework for implementing these requirements. Phase 2 is building capacity of developing Economies to conduct the ISPS Code compliance related to drills, exercises and assessment. Lastly, Phase 3 is the Port Security Visit Program (PSVP) to identify strengths and weaknesses in the implementation of the ISPS Code and this program is voluntary for APEC Economies (APEC, 2010).

In April 2009, the APEC Maritime Security Expert Group visited Busan and Incheon ports in response to an invitation by the Korean government, which intended to show Korea's advanced maritime security system. The expert group consisted of the Maritime Security Experts of APEC, the Australian government and the Philippine government. They acquired information about laws and institutions designed to implement the ISPS Code through visits to major ports such Busan and Incheon. During the visit, the Ministry of Oceans and Fisheries introduced the Korean ISPS Code Act which entered into force in 2008, and which embraces the measures of the ISPS Code and the 'National Port Security Program (2008~2017)', and stressed that Korea was strengthening both the institutional and physical security of national ports to achieve higher security levels than stipulated in the ISPS Code (MOF, 2009).

4.4.2 Proactive implementation by means of raising security level

Among a number of key articles of the ISPS Code, security level and security measures under each security level are significant in terms of the implementation of the Code. Korea has relatively abundant experiences in raising its Security Level from 1 to 2 or 3 in case of a wide range of situations, which are worthy of attention worldwide because raising the security level is quite a rare case.

As a matter of a fact, the real cases of raising the Security Level are noticed in the UK and India in recent months; however, raising the Security Level was not prevalent and hard to find until last year. In August 2013, the UK unprecedentedly raised the Security Level of UK-flagged vessels off the coast of Yemen to Level 3 and that of vessels in dangerous waters to Level 2 (Craig, et al., 2013). The Indian government raised the Security Level of some ports to Level 2 in June and July 2013 in preparation for possible terrorist attacks (OMA, 2013a; OMA, 2013b). The USCG has issued the Port Security Advisory (PSA) which is the outcome of the International Port Security Program (IPS Program) and indicated that vessels that called or will call specific ports found not in compliance with the ISPS Code must elevate their ship Security Level or take additional security measures (USCG, 2012a: USCG, 2012b). In particular, it is noteworthy that the USCG issued the PSA for Libya in March 2011 due to civil unrest which raised the US concern regarding whether port security of Libya was still being executed and maintained (USCG, 2011). The threat of terrorism related to Libya was well evidenced by the terrorist attack against the US consulate in Benghazi on September 11 2012 (Stephen, 2013).

Other than cases mentioned in the above paragraph, raising the Security Level under the ISPS Code is not common around the world. Therefore, the experiences of Korea in raising the Security Level and the subsequent lessons acquired will be valuable and meaningful for Contracting Governments to the ISPS Code.

4.4.2.1 Internationally significant events

(a) APEC Summit in November 2005

The Asia-Pacific Economic Cooperation (AEPC) Summit is hosted annually by one of its Member States. In 2005, Korea was a host country for the first time. At that time the social atmosphere and situation when it comes to security was not so severe under the seemingly non-hostile relationship between the two Koreas. However, there was clear concern about possible threats to security from outside the Korean Peninsula such as attacks by Al-Qaeda on the US and its allies. In addition, a minor incident could impair the prestige of Korea as a host country so the Korean government needed to be alert for any cases.

Despite the argument regarding raising maritime Security Level, the Korean government raised its Security Level from 1 to 2 for the first time, pursuant to the Ministerial Order in respect of the ISPS Code. At that time, the Korean ISPS Code Act was not yet enacted. Given the economic impact on the shipping industry and port-related activities, raising of the Security Level was implemented locally following discussion between the government agencies concerned; Busan Port and ships in and around the Busan Port (Ji, 2005).

(b) Group of 20 (G20) Summit in November 2010

Korea is also a Member State of economically advanced countries' meeting, G20, and hosted the G20 Summit in November 2010. Circumstances in Korea when it came to security were quite different from those in 2005. In March 2010, a Korean naval vessel sank as a result of North Korea's torpedo attack (BBC, 2010) and tensions between South and North Korea were the highest ever since the entry into force of the ISPS Code in 2004 (Euronews, 2010).

For the success of the largest international Summit for Korea, the Korean government took a strong stance in respect of maintaining security and raised the Security Level from 1 to 2 for all international port facilities and vessels calling them, and even raised the Security Level of ports adjacent to the venue, Seoul, to Level 3 just before and after the Summit in tandem with raising the Security Level of Aviation and Anti-terrorism (MOF, 2010). Of course, the raising of the Security Level was to address threats not only inside the Korean Peninsula but also those coming from around the world, given the importance of international Summit meeting just as the APEC Summit in 2005.

(c) Nuclear Security Summit in March 2012

Just two years following the G20 Summit, Korea became the host country of a newly-created international summit called the Nuclear Security Summit which was held in the US for the first time in 2010. As the second host country of the Nuclear Security Summit, Korea was desperate to maintain security during the Summit in Seoul once again. This time the number of Summit-level participants was twice that of the G20 Summit in 2010.

It can be reasonably inferred that government agencies involved were more alert than at the G20 Summit given the importance of the event and aggravated relationship inside the Korean Peninsula. However, this time, another issue, economic impact, was also vital to decision making on the heightening of Security Levels because the leadership of Korea tried to avoid negative impact on trade and economic activities arising out of reinforced security measures at international ports.

Given the risk assessment and closeness to the venue city, Seoul, ports whose Security Level was raised were limited to a minimum. The number of ports whose Security Level was elevated was reduced compared to that of the G20 Summit in 2010 in order to minimize the economically-adverse impact amid the ceaseless global economic and financial crisis. The Korean Government and inter-agency meeting at that time tried to fully consider the importance of harmony between maintaining seamless security and economic activities in relation to international port facilities and sea-going merchant vessels (MOF, 2012).

4.4.2.2 Responding to emergencies

(a) Terrorist group’s threats on Korea in 2004

Korea was concerned about regional threats rather than global ones such as attempted or actual attacks from international terrorist group, Al-Qaeda. However, in 2004, the Korean government decided to dispatch special forces as part of the Iraqi reconstruction plan led by the US. Due to this policy, threats from terrorist group, Al-Qaeda, on Korean vessels and port facilities were collected and disseminated in July and October 2004.

In response to these threats, the Korean government ordered the shipping industry and Busan port authority, the biggest international port, to reinforce security measures to the extent equivalent to Security Level 2 (quasi-Level 2) in accordance with the Ministerial Order as there was no Act-level legislation in respect of the ISPS Code in 2004 (Cho, 2004).

Quasi-Level 2 means that security measures under Security Level 2 must be done with the exception of security measures related to facilitation of trade and logistics; for example, access to ports or vessels and handling of cargo remains unchanged in the middle of reinforcing security through frequented patrol, inspection on personnel and vehicles seeking to enter and depart ports.

(b) The sinking of Korean naval vessel in March 2010

Late at night on 28 March 2010, a Korean naval vessel sank suddenly. It was later verified scientifically by an international fact-finding team made up of the US, Sweden and other countries that North Korea had attacked the vessel with a torpedo (BBC, 2010; Euronews, 2010). The Korean government ordered the shipping industry and every port authority to reinforce security measures to the extent equivalent to Security Level 2 (quasi-Level 2) which became valid on 24 May 2010 to raise awareness of maritime border security and prevent security incidents.

(c) Artillery attack by neighboring country on Korean territory in November 2010

The most unprecedented direct attack on Korean territory since the Civil War truce required immediate security actions (McDonald, 2010). Since the Civil War truce, normally North Korea has provoked in a secret way and denied its involvement. However, this case was quite different from previous provocations. This was unmistakably artillery attacks on Korean maritime territory near the maritime border line between the two Koreas a few days after the successful hosting of the G20 Summit in November 2010. As a result, there were casualties of civilians as well as marines. In accordance with the Korean ISPS Code Act, the Ministry of Oceans and Fisheries collected the opinion of agencies concerned and promptly raised the Security Level from 1 to 2 on designated ports and vessels calling those ports.

4.5 Reduction of security incidents

It is regrettable, but understandable that finding specific data resources in relation to security incidents at the national and international level was, as a matter of a fact, impossible unless authorities make it public because most countries, including Korea, classify such information as confidential. However, given the credibility of the official documents submitted to the IMO and some reports of trustworthy international organizations, it can be concluded that the Code has been conducive to reducing security incidents.

(a) Republic of Korea

As a result of the application of security measures and activities on Korean-flagged vessels, unauthorized access has been reduced and prevented. In addition, security incidents related to smuggling and stowaways at the ship/port interface have also decreased dramatically (IMO, 2011b).

(b) Islamic Republic of Iran

Since implementation of the ISPS Code, Iran has not experienced any kind of security problems in its ports or territorial waters; thanks to well-organized precautionary measures adopted by related authorities. A noticeable reduction in the number and/or severity of security events occurring in the waters under the jurisdiction of the Islamic Republic of Iran, or involving Iranian flagged vessels has been the most important and valuable outcome of the successful implementation of the ISPS Code (IMO, 2009).

(c) Australia

The Australian maritime security regime, which fully implements the requirements of SOLAS chapter XI-2 and the ISPS Code, has been in place since 2003. Australia is fully compliant with the requirements of SOLAS chapter XI-2 and the ISPS Code. There are no outstanding issues to be resolved in relation to the implementation of the provisions of SOLAS chapter XI-2 and the ISPS Code (IMO, 2012a).

(d) International Maritime Bureau reports

In addition to the reports of Member States to the IMO, one noteworthy improvement has been in place in terms of attacks against ships at anchorage or alongside berth. The statistics compiled and published by the International Maritime Bureau (IMB) show a continued decline in the number of reported attacks during the past four years (Timlen, 2007). According to the IMB survey and analysis, the number of attacks on vessels in the first half of 2012 decreased compared to the same period of last year; from 266 to 177.

The IMB determined that the decline of piracy activities was the result of preemptive and aggressive naval operations and reinforced security on board including hiring armed guards (IMB, 2012). Besides, the reduction in the frequency of persons able to stow away on ships is a positive result. This activity has not been eliminated, but there have been signs of improvement (Timlen, 2007).

According to IMB annual reports from 2004 to 2012, the fluctuation of piracy and armed robbery incidents around the world is shown in Figure 4.

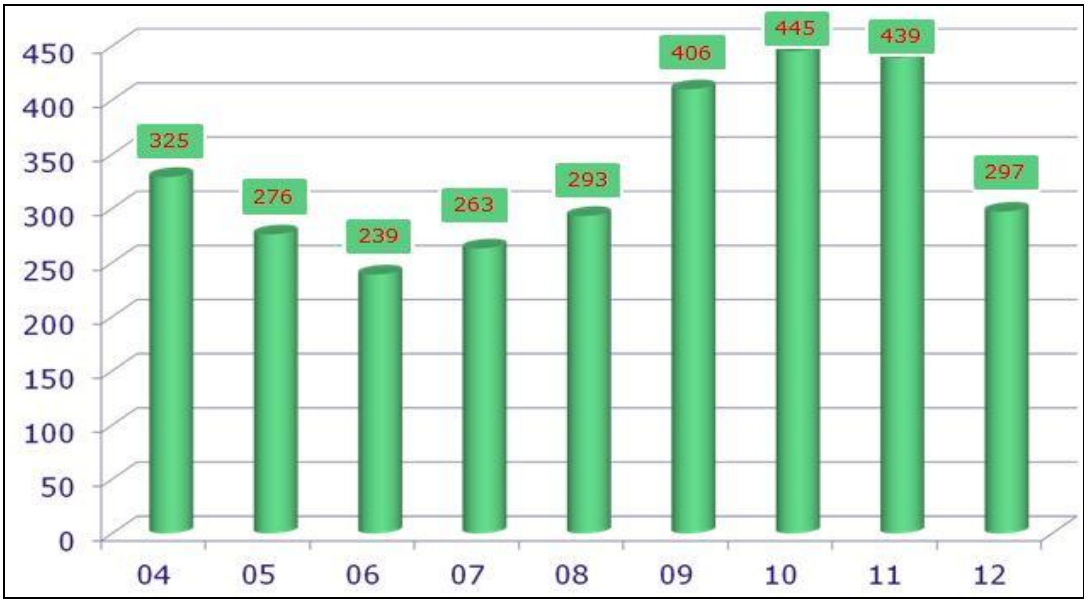


Figure 4 Piracy and armed robbery statistics from 2004 to 2012

(Source : Edited by Author from the IMB annual reports from 2004 to 2012)

IMB annual reports analyze the statistics of piracy and armed robbery from various perspectives, including the status of ships during attack; berthed, anchored and steaming. While the status of steaming is the situation in which vessels are in navigation, for example, off the coast of Somalia or in and around the Gulf of Aden, the status of being berthed and anchored can be considered as the static situation in which vessels are under direct application of the ISPS Code in and around the port facility.

Piracy during navigation can take place regardless of how much the vessel is well prepared in terms of ship security. Therefore, statistics in respect of the status of the vessel, being berthed or anchored, during attack can represent the effectiveness of the ISPS Code. In the absence of available information in respect of fluctuation of security incidents in a particular country where such sensitive information is not published, an analysis of statistics on attacks on ships at berth or anchor can be used to verify the effectiveness of the ISPS Code.

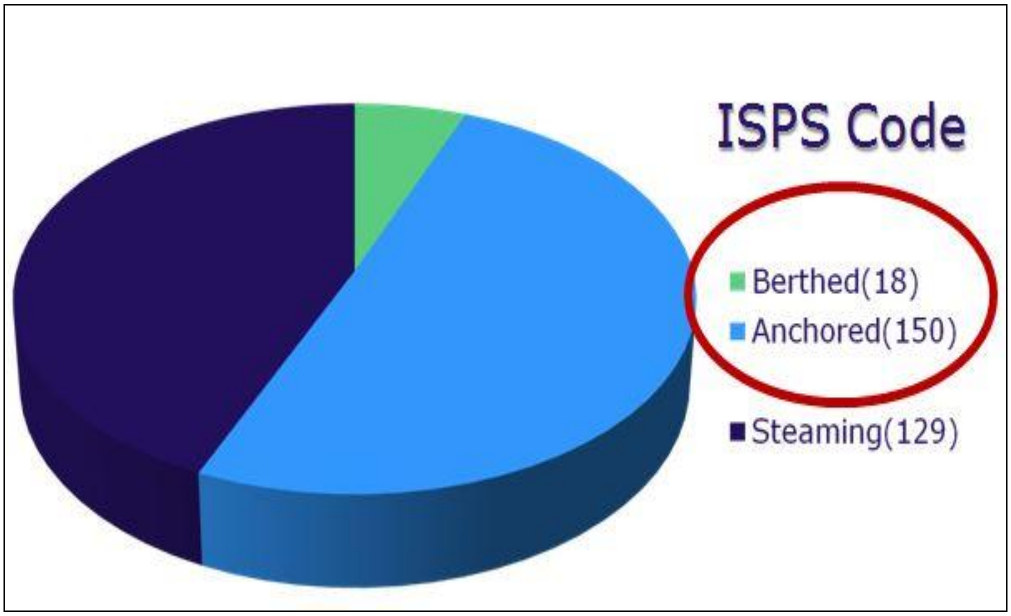


Figure 5 Status of ships during attacks in 2012

(Source : Edited by Author from the IMB annual report 2012)

In addition, the percentage of attacks while berthed or anchored over the total number of attacks on vessels can show how useful the ISPS Code is for preventing security incidents in and around port facilities and onboard vessels. The author searched the annual reports of the IMB from 2004, the year of entry into force of the ISPS Code, to 2012 and extracted the following data; percentage of the number of attacks on vessels while berthed or anchored over the whole number of attacks each year.

Percentages shown in Figure 6 indicate that the number of attacks while berthed and anchored has decreased on the whole with the exception of 2012 in which the number of piracy dropped dramatically owing to worldwide efforts to tackle piracy and armed robbery. So, the percentage in 2012 is just an outlier and can be dismissed.

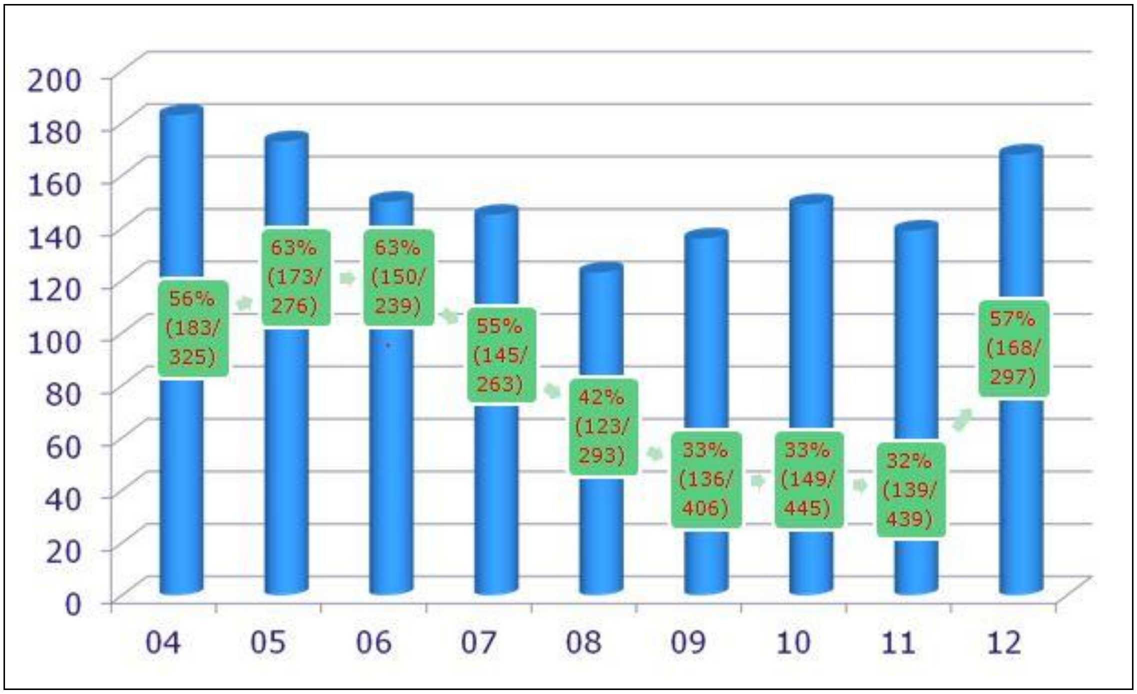


Figure 6 The percentage of attacks during being berthed and anchored over the whole attacks (Source : Edited by Author from the IMB annual reports from 2004 to 2012)

The ISPS Code has been effective in Korea in terms of building capacity and infrastructure of maritime security, enhancement of security awareness and raising Security Level. Such effectiveness was verified through international recognition from the IMO, USCG and APEC. Moreover, the reduction of security incidents was also contribution of the ISPS Code but it was hard to find real date other than the official report of Korea to the IMO. Despite the lack of specific data regarding security incidents, the reports of Iran, Australia and the IMB show that the ISPS Code has contributed to the decrease of security incidents in the maritime field.

CHAPTER 5

CHALLENGES OF THE ISPS CODE

5.1 Introduction

The creation of the ISPS Code is a painful brainchild of the distinguished maritime experts given the circumstances; the intensity of desperation of the maritime world after 9/11 and the short period of time due to the urgency to introduce a new regime to address the terrorism. However, it is also truly right there is no perfect regime; therefore, it will be highly meaningful to reflect on the shortcomings and challenges that have appeared in the process of the implementation of the ISPS Code, and reflect on those points in the process of sharpening existing IMO Instruments.

5.2 Problems in case of raising Security Level

5.2.1 Security measures in each Security Level

Under the Korean ISPS Code Act and Ministerial Decree, several security measures in case of Security Level 3 have been regarded as unrealistic given the importance of the free flow of logistics and economic activities. Problematic measures in my opinion of the author are as follows:

(a) Suspending the loading or unloading of cargo and ship’s stores;
(b) Refusal to accept unaccompanied baggage on board the passenger ship;
(c) Suspension of access to port facility;

(d) Suspension of movement of cargo and vehicles within port facility;

(e) Suspension of port operation within port facility;

(f) Suspension of handling of unaccompanied baggage within port facility;

(g) Suspension of the delivery of ship's stores within port facility.

In fact, the original ISPS Code Part B adopted by the IMO shows the flexibility of implementation of security measures even under Security Level 3 as follows:

(a) Restriction or suspension of handling of ship's stores and unaccompanied baggage

(b) Suspension of access to all, or part, of the port facility;

(c) Suspension of pedestrian or vehicular movement within all, or part, of the port facility;

(d) Suspension of port operation within all, or part, of the port facility;

(e) Restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships;

(f) Restriction or suspension of handling of unaccompanied baggage;

(g) Restriction or suspension of the delivery of ship's stores within all, or part, of the port facility

The ISPS Code Part B recommends specific gradually-intensifying security measures under Security Level 1 through 3 with flexibility of implementation, within all, or part, of the port facility. However, this flexibility was not fully reflected in the process of national legislation of the ISPS Code in the Republic of Korea. The strict implementation of security measures was legislated and has been a barrier to economic activities and the government fully realized this problem arising out of the discrepancy between the original ISPS Code and the Korea Act.

Here some questions arise. Should there be restraint in raising the Security Level up to

3? Is it not enough to maintain Security Level 2 unless there is an imminent threat, given the importance of harmony between security and the economic activities of the private sector? Why has the Korean government been actively in favor of raising the Security Level to the highest stage? In respect of these questions, Section 5.2 will offer reasonable explanation. This chapter will further look into the discord between several security regimes in Korea in terms of stage of Security Level.

5.2.2 An expedient heightening of Security Level

As pointed out in Section 4.3.2.2, the Korean government sometimes reinforced security measures while maintaining the Security Level unchanged in accordance with the decision of the International Ship and Port Facility Security Committee (ISPS Committee), ordering the Designated Authority and shipping industry to take stronger security measures equivalent to those under the higher Security Level in the Port Facility Security Plan (PFSP) and Ship Security Plan (SSP).

This policy resulted from consideration of the private sector needs because heightened Security Level requires reinforced security measures and, in the end, leads to the impact on access to vessels, movement of cargo and vehicles within port facilities and restriction on the handling of cargo, unaccompanied baggage and ship's stores. In other words, the Korean government has tried to give due considerations to minimize the negative impact on the economic activities of the private sector while achieving the objectives of security measures.

However, raising security measures equivalent to a higher Security Level, while officially leaving the Security Level unchanged, is legally groundless so many government officials involved have expressed concern that, strictly speaking, a legitimate organization (ISPS Committee) has made a literally expedient decision. This measure was groundless in terms of legality because the Korean legislations did not stipulate an expedient raising of Security Level. Several instances of making expedient decisions on raising the Security Level risked causing disregard of the heightened Security Level from both the public and private sector even though this decision resulted from thoughtful consideration for economic activities. Essentially, these expedient decisions would be attributable to the lack of flexibility of the Korean ISPS Code Act as opposed to the original IMO ISPS Code, which is well-evidenced by Section 5.2.1.

5.3 Discrepancy with other Korean security regimes

The ISPS Code stipulates the three-stage Security Level as follows:

(a) Level 1 : Normal, the level at which the ship or port facility normally operates; minimum appropriate protective security measures;

(b) Level 2 : Heightened, the level applying for as long as there is a heighted risk of a security incident; additional protective security measures;

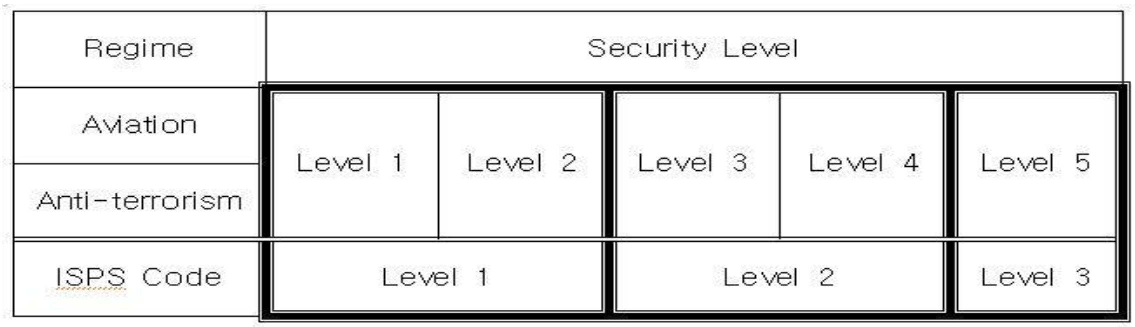
(c) Level 3 : Exceptional, when there is the probable or imminent risk of a security incident; further specific protective security measures.

One of the salient features of the newly-adopted maritime security regime of the IMO is the stages of security measures because pre-existent security measures such as the Aviation Security and Anti-terrorism mechanism of Korea are equally composed of five stage security levels which have more stages than the ISPS Code.

The Security level of Aviation is regulated in the ‘Aviation Safety and Security Act’ and related low-level ‘National Civil Aviation Contingency Plan’. This contingency plan is made based on Article 31 of the Aviation Safety and Security Act' (MOLEG, 2009). The Korean Aviation Security Level is made of five stages using color; Green (Normal, 1) – Blue (Observation, 2) – Yellow (Advisory, 3) – Orange (Vigilant, 4) – Red (Serious, 5). Just as the Maritime Security Level was elevated to Level 3 in preparation for the Nuclear Security Summit in 2012, the Aviation Security Level was also raised to the highest level at that time (South Korea to heighten airport security, 2012).

Additionally, the anti-terrorism regime is also more closely related to the aviation sector rather than the maritime field due to the ramifications of the 9/11 terrorist attacks. This regime is also composed of five stages in accordance with Article 35 and Article 36 of the 'Presidential Decree on National Anti-terrorism Activities'; Normal – Observation – Advisory – Vigilant – Red (MOLEG, 2013a). In fact, the Aviation and Anti-terrorism regimes are identical to each other in terms of Security Level.

The discrepancy between the ISPS Code and existing security regimes in Korea caused confusion from the beginning but the Korean government had no choice but to follow the system of the ISPS Code. To address this problem, the Korean government created a 'Table' indicating as clearly as possible the stage in accordance with the development of an urgent situation. For example, Security Level 2 of the ISPS Code corresponds with Level 3 and 4 of the Aviation and Anti-terrorism regimes.



Regime	Security Level				
Aviation	Level 1	Level 2	Level 3	Level 4	Level 5
Anti-terrorism					
ISPS Code	Level 1		Level 2		Level 3

Table 4 Comparison of security level between security regimes in Korea.

(Source : Edited by Author government officials concerned)

However, there still exists confusion and difference of intensity of security measures between security regimes. For example, Level 3 of the ISPS Code must suspend every movement of cargo and vehicle within a port facility, and handling of unaccompanied baggage and ship's stores whereas the highest Security Level of Aviation does not suspend the flow of logistics within an airport. Therefore, the maritime field has been inevitably more reluctant about raising the Security Level to the highest than the aviation field.

In reality, international trade overwhelmingly depends on the maritime world and a small portion of trade is dependent on the aviation industry, which is predominantly focused on the movement of passengers. Fundamentally, there is a significant gap between the ISPS Code and other security regimes when it comes to harmony between security and economic activities. In other words, the maritime security regime must think about the ramifications of raising the Security Level, in terms of economic impacts, much more than other security regimes.

5.4 Narrow focus on ships and ports facility

Security measures covered by the ISPS Code are limited to matters involving the ship/port interface (McNaught, 2005). The Preamble of the ISPS Code also states that the provisions relating to port facilities should relate solely to the ship/port interface; therefore, the wider issue of the security of port areas will be the subject of further joint work between the IMO and the International Labour Organization (ILO) (IMO, 2012c). In a sense, the ISPS Code suffers from 'built-in' limitations that undermine its ultimate effectiveness (Cox, 2013)

Narrow focal points of the ISPS Code ignore major issues such as container security and vulnerability of the supply chain to tampering by criminals including terrorists (McNaught, 2005) As a matter of fact, inspection of the contents of containers falls outside the scope of the Code. As a result, contrary to the improvement in the number of security incidents such as attacks on ships and stowaway, smuggling of drugs has not been reduced because drugs are usually hidden inside containers. Concealments made within cargo and containers would involve activities taking place outside the scope of the ISPS Code (Timlen, 2007).

In this context, the ISPS Code is unlikely to adequately mitigate the risk posed by containerized cargo as it cannot prevent or effectively detect terrorist threats. For example, the placement of a weapon of mass destruction (WMD) within a shipping container is likely to be installed during another phase of the supply chain. This concern is expressly appearing in Korea and over time pan-governmental efforts in respect of supply chain security encompassing the application of the ISPS Code have been discussed.

The US also stressed the shortcoming of the ISPS Code when it comes to handling of cargo (IMO, 2007); the ISPS Code focuses on the physical security of the port facility and vessel. There are some basic container security measures within the ISPS Code and Convention on Facilitation of International Maritime Traffic (FAL), but a tenet of the design of the ISPS Code is that a secure facility and secure vessel will by default maintain the integrity of a container within these segments of the supply chain. In this sense, it is appropriate to consider methods to enhance security measures that are already contained within the ISPS Code, to include safeguards for maintaining the integrity of containers while within the port facility's or vessel's control.

5.5 Lack of the IMO enforceability

5.5.1 The IMO Member States audit scheme

In 2005, the IMO introduced audit scheme on Contracting Governments in respect of the application and implementation of Mandatory IMO Instruments as the IMO realized that unceasing maritime accidents came from the inadequate and improper implementation of IMO instruments from the side of Contracting Governments. The introduction of the audit scheme on Contracting Governments was itself a groundbreaking commencement, but it is also true that the IMO can only monitor Contracting Governments' compliance with the IMO mandatory Instrument when the Contracting Government agrees to receive an IMO audit on a voluntary basis. In fact, the enforcement of IMO Instruments is the domain of Contracting Governments, which have authority to carry out Port State Control (PSC) on foreign vessels and Flag State Administration on national vessels and port facilities.

At the present moment, the audit scheme of the IMO is carried out on a voluntary basis even though it is supposed to be transformed into a mandatory regime in the future. The current audit scheme called VIMSAS (Voluntary IMO Member States Audit Scheme) has been carried out voluntarily and, furthermore, there are no sanctions on Contracting Governments if their implementation of the IMO instruments is found inappropriate. Given the fact that the IMO VIMSAS benchmarked the International Civil Aviation Organization (ICAO) mandatory audit scheme which has impacted the aviation world around the world and contributed to upgrade the level of compliance with mandatory ICAO Instruments (IMO, 2004a; IMO 2005c), the current VIMSAS has clear limitation in enhancing the level of compliance with IMO Instruments.

As an active participant in the international maritime world, Korea received an IMO audit in April 2007. The IMO audit team determined that Korea was faithfully implementing IMO instruments. Korea took every possible action ranging from national legislation to rectification of problems evidenced by self-assessment prior to this audit (Lee, 2007). Even though Korea achieved numerous positive results by means of receiving the IMO audit voluntarily, not every Contracting Government of the IMO has the same perspective and standpoint on the audit scheme. Up to now there has not been sufficient cooperation of Contracting Governments with the IMO efforts to encourage VIMSAS and a total of 69 Contracting Governments and two Associate Members received IMO audits as of 3 June 2013 (IMO, 2013d).

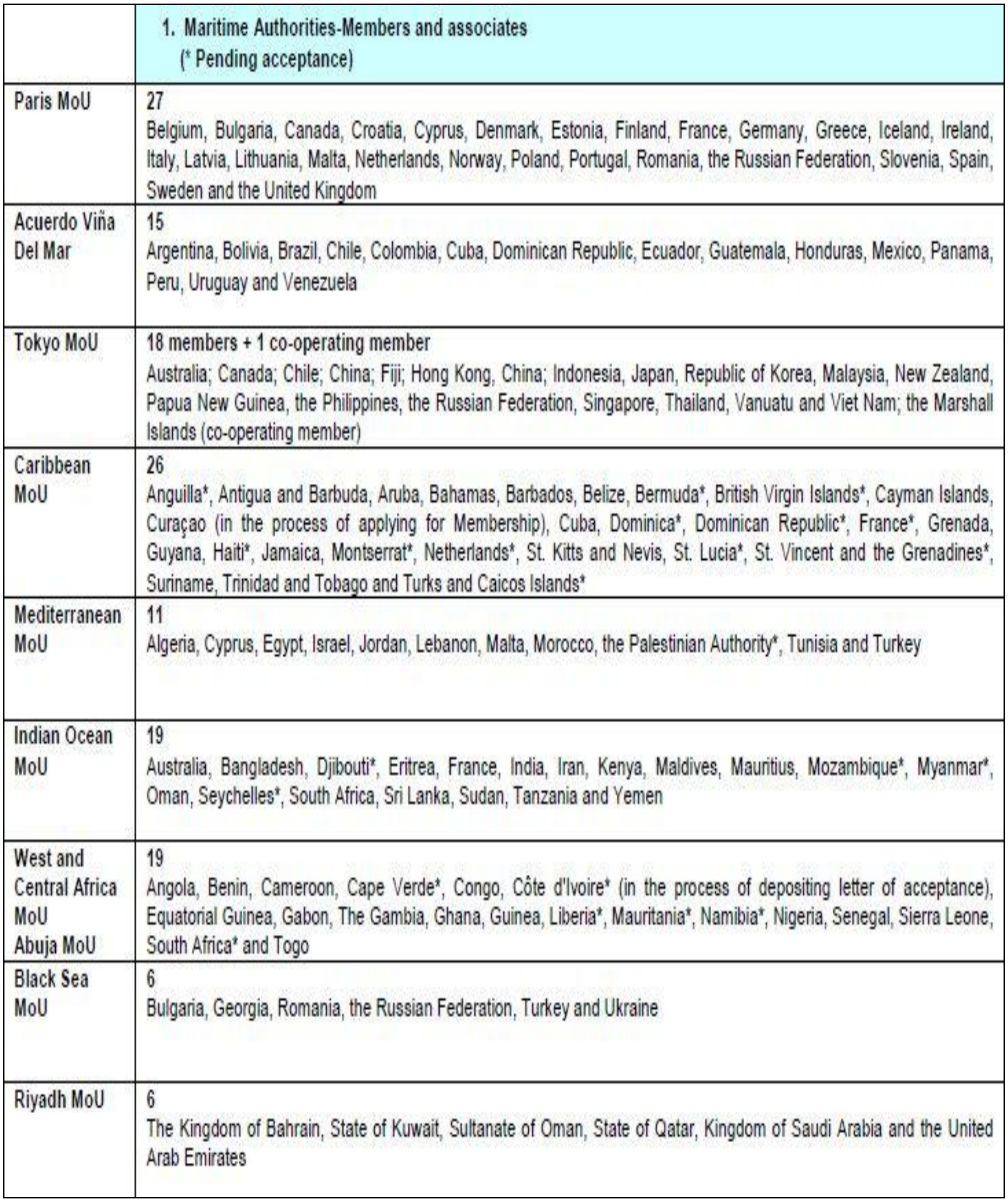
In addition, the fact itself that one country received an IMO audit does not guarantee high-level of compliance with IMO Instruments because it is impossible to gain detailed and named information with regard to the result of an audit under the current system. Without the consent of the Contracting Government, the IMO cannot make the result public. The report of the IMO audit is classified into three stages; interim, final and summary report. Interim and final reports are handled confidentially and available only to audited states, audit team and Secretary-General (IMO, 2005d). The periodical summary report which encompasses several audit reports drawn up by the Secretariat can be circulated for the information to all member states after consultation with states involved; however, it is still limited to enhance the implementation of the IMO Instruments.

In fact, ratification of international conventions adopted by the IMO including national legislation is one thing and strict compliance with the ISPS Code is another, which is well evidenced in Nigeria whose ISPS Code was proved unfeasible through the ISP program of USCG (Oritse, 2013a). This result was, to a large extent, forecast in the previously-done research; Nigeria has implemented the ISPS Code but it has been found that the agency in charge of the Code has been remiss in providing clear guidelines and directives, for example, on the Recognized Security Organizations (RSOs) (Okoroji, et al., 2011). In addition, it has been observed that most vessels have not complied with the Code due mainly to financial constraints. Therefore, it is recommended that Nigeria should adopt a pragmatic approach to the Code's implementation, by complementing security gadgets with human resource training and development within the maritime industry.

Unfortunately, it looks like that the situation in Nigeria has not been improved despite the research and efforts taken by the stakeholder. Pursuant to the Maritime Transport Security Act of 2002, the USCG assessed the compliance of Nigerian port facilities with the ISPS Code in May this year but it has turned out that Nigeria does not have accurate reports on the number of port facilities that currently exit in the country. The USCG noted that Nigeria as a contracting government to the convention does not know the total number of facilities where the Code applies. Even though there has been an increase in the number of attacks on vessels in and around Nigeria's territorial waters, Nigeria is currently operating at only Security Level one in most of the facilities across the nation (Oritse, 2013b). As a result, the US gave an ultimatum, 90 days, to Nigeria before revisiting scheduled in late August. It seems that there has been a positive change in Nigeria during the 90 days (Iwori, 2013).

5.5.2 Limitations of Port State Control regime

Port State Control (PSC) is the implementation of the rights of the Port State over foreign vessels' compliance with international mandatory conventions, mostly adopted by the IMO. In the absence of the IMO mandatory Contracting Governments audit scheme, PSC has been playing a significant role in enhancing the compliance of vessels with IMO mandatory instruments. Around the world, there exist nine PSC regimes such as Tokyo MOU, Paris MOU and USCG. In addition, each regime inspects foreign vessels based on its own criteria and publishes annual reports.



	1. Maritime Authorities-Members and associates (* Pending acceptance)
Paris MoU	27 Belgium, Bulgaria, Canada, Croatia, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Iceland, Ireland, Italy, Latvia, Lithuania, Malta, Netherlands, Norway, Poland, Portugal, Romania, the Russian Federation, Slovenia, Spain, Sweden and the United Kingdom
Acuerdo Viña Del Mar	15 Argentina, Bolivia, Brazil, Chile, Colombia, Cuba, Dominican Republic, Ecuador, Guatemala, Honduras, Mexico, Panama, Peru, Uruguay and Venezuela
Tokyo MoU	18 members + 1 co-operating member Australia; Canada; Chile; China; Fiji; Hong Kong, China; Indonesia, Japan, Republic of Korea, Malaysia, New Zealand, Papua New Guinea, the Philippines, the Russian Federation, Singapore, Thailand, Vanuatu and Viet Nam; the Marshall Islands (co-operating member)
Caribbean MoU	26 Anguilla*, Antigua and Barbuda, Aruba, Bahamas, Barbados, Belize, Bermuda*, British Virgin Islands*, Cayman Islands, Curaçao (in the process of applying for Membership), Cuba, Dominica*, Dominican Republic*, France*, Grenada, Guyana, Haiti*, Jamaica, Montserrat*, Netherlands*, St. Kitts and Nevis, St. Lucia*, St. Vincent and the Grenadines*, Suriname, Trinidad and Tobago and Turks and Caicos Islands*
Mediterranean MoU	11 Algeria, Cyprus, Egypt, Israel, Jordan, Lebanon, Malta, Morocco, the Palestinian Authority*, Tunisia and Turkey
Indian Ocean MoU	19 Australia, Bangladesh, Djibouti*, Eritrea, France, India, Iran, Kenya, Maldives, Mauritius, Mozambique*, Myanmar*, Oman, Seychelles*, South Africa, Sri Lanka, Sudan, Tanzania and Yemen
West and Central Africa MoU Abuja MoU	19 Angola, Benin, Cameroon, Cape Verde*, Congo, Côte d'Ivoire* (in the process of depositing letter of acceptance), Equatorial Guinea, Gabon, The Gambia, Ghana, Guinea, Liberia*, Mauritania*, Namibia*, Nigeria, Senegal, Sierra Leone, South Africa* and Togo
Black Sea MoU	6 Bulgaria, Georgia, Romania, the Russian Federation, Turkey and Ukraine
Riyadh MoU	6 The Kingdom of Bahrain, State of Kuwait, Sultanate of Oman, State of Qatar, Kingdom of Saudi Arabia and the United Arab Emirates

Table 5 PSC regimes worldwide (Source : FSI 19/6/2 2010)

Despite these functions of PSC, it is also true that PSC has focused on safety and environmental elements rather than security. Of course, the ISPS Code is just one chapter of SOLAS and PSC inspection is done with regard to a wide range of IMO mandatory instruments. Therefore, it is not uncommon that PSC officers have been primarily committed to inspecting whether the vessel concerned has complied with the IMO instruments regarding safety and protection of environment. The number of inspections on compliance with the ISPS Code is not enough to strengthen security on board a vessel and the reports of inspection have not sufficiently reflected security matters. Amid this situation, it is quite noteworthy for the USCG to publish an annual report on PSC inspections which encompass deficiencies regarding security issues as well as normal PSC inspections.

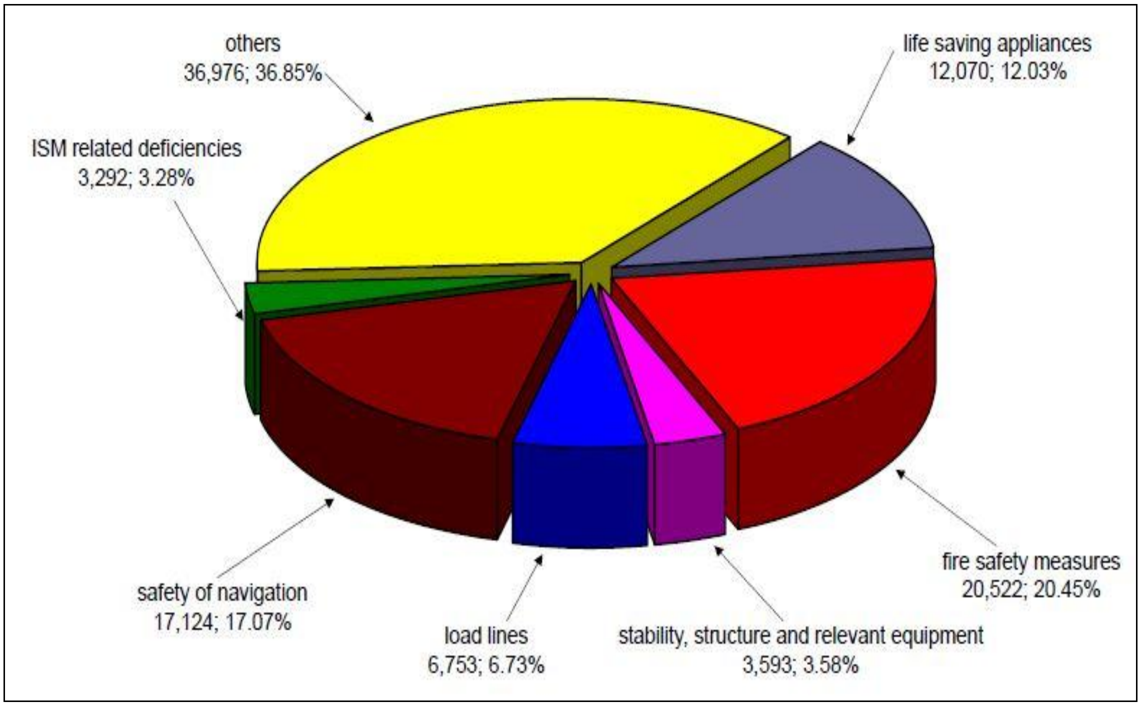


Figure 7 Deficiencies by Category (Source : Tokyo MoU 2012 Report)

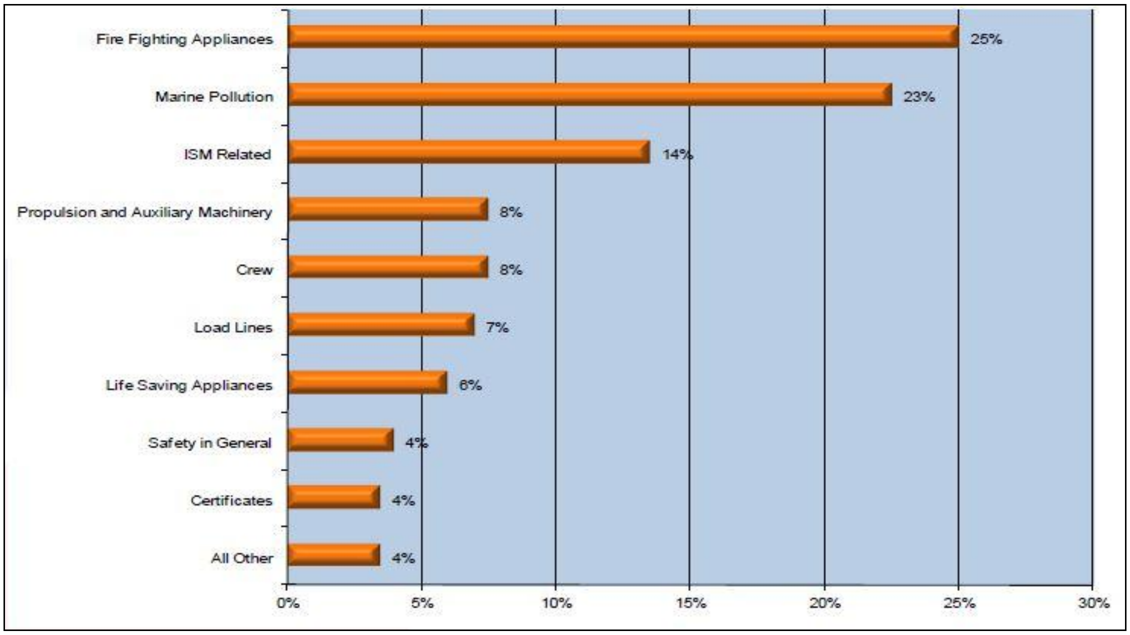


Figure 8 Types of Safety Deficiencies (Source : USCG 2011 Report on PSC)

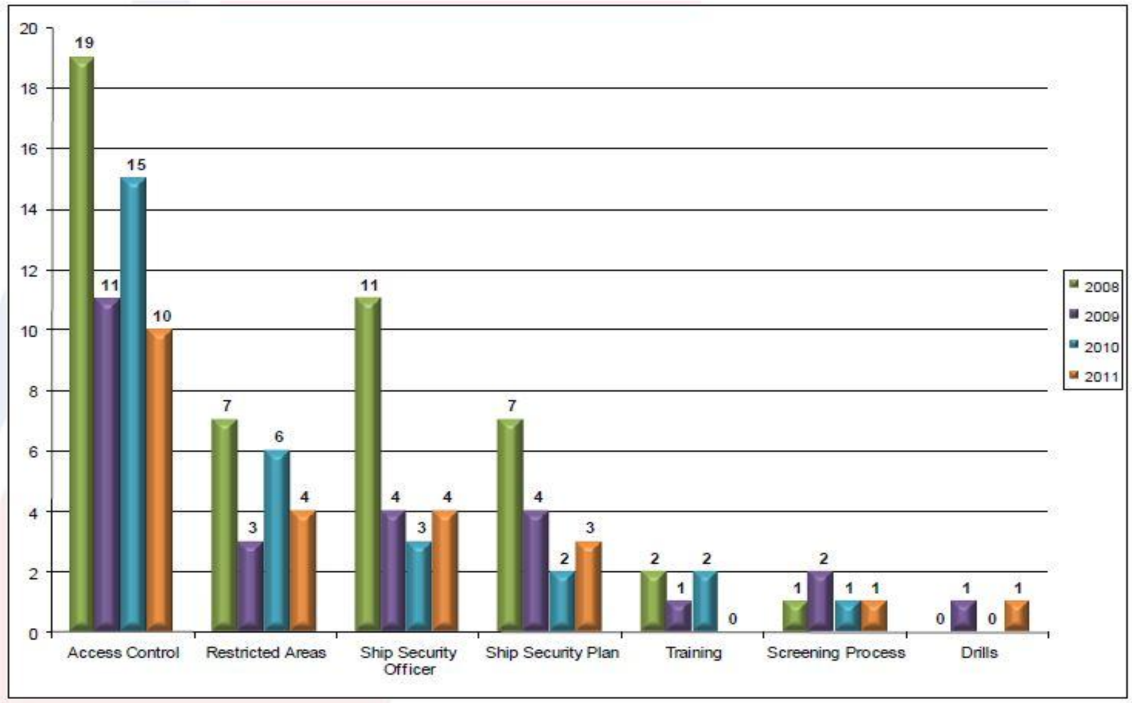


Figure 9 Security Deficiencies by Category (Source : USCG 2011 Report on PSC)

In addition, inconsistency and lack of uniformity is another problem for PSC inspection. Currently, there is no unified international convention to regulate PSC affairs worldwide. Subsequently, the independent implementation of PSC inspection under the discretion of each PSC regime is functioning as a negative factor for the effective and efficient implementation of IMO instruments including the ISPS Code despite the new efforts such as the Concentrated Inspection Campaign (CIC), spearheaded by the Paris MOU and Tokyo MOU.

5.6 Lack of response system to incidents

The aftermath of security incidents is not mentioned in the ISPS Code and the Preamble states that the provisions in this Code should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack (IMO, 2012c). This aspect is another built-in limitation of the ISPS Code according to Cox (2013). Therefore, the Code is preventative in nature and does not address the issue of response to attacks or remediation issues following an attack (IMO, 2005b). It is important to note that the ISPS Code primarily addresses how terrorist attacks can be deterred and minimized whereas detailed procedures in addressing the aftermath of a significant security incident are not mentioned (Ng, 2009).

Given the preventive characteristics of the ISPS Code as pointed out by several researchers in the above paragraph, the Korean government included a contingency plan to address real attacks or security incidents in the National Port Security Program (NPSP) and Regional Port Security Program (RPSP) from the moment when those programs were drawn up in 2008. However, domestic legislation in respect of the ISPS Code can be different nation by nation. In essence, preparedness and response are closely related to each other so in the mid and long term it is necessary to find ways to solve the lack of response systems to security incidents.

5.7 Existence of variation among Member States

Each Contracting Government is responsible for determining and enforcing appropriate security measures for its ships and ports, which are bound to be significantly different between nations in the standards of these measures (McNaught, 2005). Some Contracting Governments, especially Flag of Convenience (FOC) registries, have been identified as either corrupt, therefore vulnerable to exploitation by terrorists groups (Botelho, 2004) or lacking the resources or expertise to enforce acceptable standards (Raymond, 2005). In addition, Recognized Security Organizations (RSOs) expertise in the maritime field varies significantly (Heathcote, 2004).

Given the limitations of enforceability of IMO instruments on account of the voluntary audit scheme on Contracting Governments, it has been reasonably anticipated that a great deal of discretion has been given to each Contracting Government and, inevitably, there has been inconsistency and unannounced non-conformity with the ISPS Code. In particular, the recommendatory Part B of the ISPS Code is one of sources of variations worldwide. As an example, as written in Section 5.1, the Korean government enacted the strict security measures under Security Level 3, which are apparently different from the paragraphs of Part B including to some extent flexibility of implementation of security measures.

Among variations, lack of standardization at port facilities was more serious than ships. The implementation of the Code on board ships went smoothly, whereas effective implementation in port facilities in different countries varies significantly. These difficulties are mostly caused by limited economic potential, differing positions on the status of national and international maritime security systems, and finally, different understandings of what mitigation measures should be accepted as appropriate in different countries (Zec, et al. 2009).

5.8 Existence of vessels falling outside the scope of the ISPS Code

Applicability of the ISPS Code to vessel types is also a weakness when it comes to addressing the terrorism threat. The ISPS Code does not apply to many kinds of vessels that are vulnerable to, or capable of, terrorist attack or exploitation. These include fishing vessels, high speed container vessels built prior to July 2001, vessels not engaged in international voyages and cargo ships less than 500 tonnage (McNaught, 2005).

Part B of the ISPS Code (Paragraph 4.20) advises that Contracting Governments should consider establishing appropriate security measures to enhance the security of ships to which the SOLAS XI-2 and Part A of this Code do not apply and ensure that any security provisions applying to such ships allow interaction with ships to which Part A of the Code applies; however, Part B is not mandatory and unlikely to result in practical actions by Contracting Governments.

Yachts and marinas are not covered by the Code due to the fact that yachts are in most cases less than 500 tonnage and marinas cannot accommodate ISPS vessels (Zec, et al., 2009). Small vessels and ports pose threats to security as they are essentially outside the scope of the ISPS Code and even when there is no domestic legislation and law enforcement function. Up to now, the IMO also presented non-mandatory guidelines to address threats arising out of non-SOLAS vessels (IMO, 2008c)

CHAPTER 6

RECOMMENDATIONS

6.1 Introduction

The previous chapters of this paper look into the effectiveness and challenges of the ISPS Code, which have been evidenced primarily in Korea. Based on the experiences of Korea, this chapter recommends feasible measures which can be taken at the national and international level for the purpose of better implementation and enhancement of international maritime security regime.

6.2 Sophisticated legislation at the national and international level

6.2.1 International standard legal framework

It is fully understandable that the ISPS Code did not became wholly mandatory, given the short period of time from draft to entry into force. However, due in part to the recommendatory Part B of the ISPS Code and standpoint of the IMO to provide, to some extent, flexibility in the process of national legislation, there exist variations among national legislations enacted by Contracting Governments to the ISPS Code. As pointed out in chapter 5.1, the Korean ISPS Code Act was not enacted with the same extent of flexibility of security measures as the original ISPS Code part B. This could be attributed to the absence of adequate guidelines regarding national legislation or model legislation.

In this context, the MSC, at its eighty-second session agreed to the development of the model legislation on maritime security and subsequently 29 Member States and the European Commission suggested the minimum contents of model legislation on maritime security (IMO, 2008b). This movement is quite meaningful but there is a long way to the introduction because work on a draft is still on-going (IMO, 2013g). Meanwhile, the action to introduce a maritime security manual for the facilitation of the implementation of the ISPS Code and narrow the gap between Member States was highly commendable (IMO, 2011a).

In fact, developing a code that is internationally comprehensible is a challenge. However, such a model must be concise and straightforward enough to be widely accessible (Cox, 2013). In the process of development of model legislation, there are some points that need to be considered sufficiently to reduce the variations derived from the recommendatory Part B, and to address built-in limitations stipulated in the Preamble paragraph 5 of the ISPS Code, which states "It was further agreed that the provisions relating to port facilities should be related solely to the ship/port interface. It was also agreed that the provisions should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack." (IMO, 2012c).

For the most Member States, the international mandatory convention can be a strong driving force for them to introduce and implement corresponding domestic legislation. Loosely-made international convention could trigger confusion and poor performance at the national level and give room for non-conformity. Therefore, the sophisticated international legislations in respect of maritime security, which can narrow the gap between the ISPS Code and national legislations of Member States, are necessary.

6.2.2 Sophisticated legislation at the national level

The existence of globally-acceptable good model legislation on maritime security does not guarantee the desirable national legislation so there is need for Member States to make utmost efforts to enact or amend national legislations in a sophisticated manner, even prior to the introduction of model legislation.

The Korean government has a precious experience with its own legislation. In accordance with the Korean Act, strict suspension of handling of cargo and ship's stores and banning movement of cargo and vehicles within port facility was regulated without any flexible conditions. This strict legislation has raised concerns regarding the flow of goods in and around the facilities and further overall supply chain.

In order to address this problem, Korea amended existent legislation to endow flexibility on maritime security measures in June 2013. This amendment added "Minister of Oceans and Fisheries can temporarily rule out the application of specific security measures which must be taken under certain Security Level, or make use of security measures in other Security Level if this action is recognized in order to prevent security incident in port facilities or ocean-going vessels or address security threats. In this case, Minister of Oceans and Fisheries must immediately notify the owners of port facilities or vessels of governmental decision" (MOLEG, 2013b).

Ultimately, it is truly up to each Member State to enact national legislation in a reasonable way based on the international conventions, rules and regulations. The Korean experience to amend national legislation in respect of the ISPS Code, based on the real lessons acquired from the process of raising the Security Level, is noteworthy for other Member States. This move was taken to remove unreasonableness of legislation giving negative impact on the economic activities of the private sector, and to harmonize security and smooth flow of cargo.

6.3 Coordination among security regimes

Addressing the confusion arising out of the discrepancy of Security Levels between national security regimes such as the ISPS Code, Anti-terrorism and Aviation security is another tough, yet subtle issue in Korea. Even though Korea is dealing with the discrepancy of Security Level among security regimes using a ‘Coordination Table’ as well as repeated training and drills, it is difficult to eliminate the root cause of confusion and lack of distinction.

Given the urgency of security measures, a fewer-stage Security Level (three-stage of the ISPS Code) is more desirable and adequate in tackling the situation than multi-layered Security Levels (five-stage of Anti-terrorism and Aviation). In fact, the US government reduced the Security Level of Anti-terrorism from ‘color-base five stage’ to ‘two stage’ in order to enhance the capacity of response to emergency situations in 2011 (DHS, 2011). In addition, Russia also introduced a three-level Anti-terrorism system to promptly inform people about the emergency of a terrorism threat and to organize activities to counter its realization (Russia introduces, 2012).

In this context, the Korean government and other Member States need to abbreviate Security Levels of non-maritime security regimes. Around 70 countries use color-coded terror alert systems and levels vary from three to five (Russia to adopt, 2010). Considering the essential purport of a security regime, it is reasonable to reduce the number of stages of security level and enhance the feasibility and speed of security measures to imminent or expected threats.

6.4 Reinforcement of supply chain security

According to McNaught (2005), the ISPS Code like many other IMO Instruments must be viewed not as a stand-alone solution to the maritime security threat, but rather as one component of a system in the fight against terrorism. However, the ISPS Code may seem stand-alone due to built-in limitations (Cox, 2013). To address the narrow scope of the ISPS Code implementation, there is a strong need for collaboration between organizations at the international as well as national level, and for supplementary measures in the name of global supply chain security.

In this sense, in July 2013 there was a meaningful meeting in respect of cooperation between security regimes. Heads of the IMO, ICAO (International Civil Aviation Organization) and WCO (World Customs Organization) met in the IMO headquarters in London to strengthen supply chain security through close cooperation between the three organizations (IMO, 2013e). They stressed the importance of collaboration in order to enhance overall security in the process of movement of goods by sea, air and other modes. When it comes to global supply chain security, the IMO has the ISPS Code, the ICAO has Aviation Security regime and the WCO has the Advanced Economic Operator (AEO). Along with the international dimension, they urged Member States to cooperate closely with agencies mandated for security at the national level.

In addition to the cooperation and collaboration between organizations concerned when it comes to security, it is also necessary to implement a series of supply regimes closely related to the supply chain; Advanced Economic Operator (AEO), Container Security Initiative (CSI), Megaports Initiative (MI) and so on. These regimes are for detecting forbidden items such as WMDs and radioactive materials inside the cargo. Detecting items, posing threats to security, hidden inside the cargo or container is not implemented by the ISPS Code.

(a) Advanced Economic Operator (AEO)

The World Customs Organization (WCO) has decided to introduce a new logistics security system and regulations for trade security, security of international trade flow from producers to ultimate consumers, or Supply Chain Security based on the experiences from the 9/11 terrorist attacks. In order to complement global security regimes in the maritime and aviation fields, the WCO established the Framework of Standards to Secure and Facilitate Global Trade, which is the WCO SAFE Framework, in June 2005 (KCS, 2013).

The core concept of this international Framework is the AEO program. AEO means “a party involved in the international movement of goods in whatever function that has been approved by or on behalf of a national Customs Administration as complying with WCO or equivalent supply chain security standards. AEOs include inter alia manufacturers, importers, exporters, brokers, carriers, consolidators, intermediaries, ports, airports, terminal operators, integrated operators, warehouses, distributors” (Polner, 2010).

Even though the AEO program is not a mechanism to inspect cargo or containers, the benefit of this system differentiate the verified operators and non-verified ones in the field. Therefore, it is conducive to focus resources and personnel into non-verified cargo and containers and eventually the security of the supply chain.

(b) Container Security Initiative (CSI)

In January 2002, the US Customs and Border Protection’s (CBP) created the Container Security Initiative (CSI) in the aftermath of the 9/11 terrorist attacks. CSI places CBP officers at select foreign seaports to work with host-country customs officials to identify and scan high-risk cargo before it is shipped to the United States. When it comes to the timing of introduction, CSI is the first one among a variety of security-related regimes created following the 9/11 tragedy.

The three core elements of CSI are to identify high-risk containers, to prescreen and evaluate containers before they are shipped and, lastly, to use technology to prescreen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. CSI is now operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP's 58 operational CSI ports now prescreen over 80 percent of all maritime containerized cargo imported into the United States (CBP, 2013).

(c) Megaports Initiative (MI)

This regime, led by the US National Nuclear Security Administration (NNSA), detects nuclear and other radioactive materials that might be hidden inside containers or cargo. The MI helps partner countries equip major international seaports with radiation detection equipment and alarm communication systems. In addition, the Megaports Initiative provides comprehensive training for foreign personnel, short-term maintenance coverage, and technical support to ensure the long-term sustainability and viability of installed radiation detection systems.

The goal of the Megaports Initiative is to scan as much container traffic as possible (including imports, exports, and transshipped containers) regardless of destination and with minimal impact to port operations. The Megaports Initiative seeks to equip 100 seaports around the world with radiation detection systems by 2015, scanning approximately 50 percent of global maritime containerized cargo. Since the start of the

Megaports Initiative in fiscal year 2003, NNSA has completed installations at 27 ports around the world to date (NNSA, 2013).

In fact, the US has preemptively introduced a number of initiatives to further address the security of cargo, in particular, containers outside the scope of the ISPS Code. The CSI and MI were launched by the US and there are more regimes in place by the US government. The Korean government actively cooperated with international regimes such as the AEO launched by the WCO and the US-led security regimes such as CSI and MI. Korea concluded that the ISPS Code alone is not enough to guarantee security in the process of the supply chain. The maritime world needs to bear in mind that a stand-alone regime has limitations in terms of effectiveness and actively join the global movement for the enhancement of supply chain security.

6.5 Buildup of the ISPS Code enforceability

6.5.1 The revision of the IMO Member State audit scheme

The inception of Voluntary IMO Member State Audit Scheme (VIMSAS) has motivated the IMO Member States and maritime world to comply with IMO instruments and eventually to mitigate the occurrence of maritime accidents and environmental damage. Despite these positive aspects, it is also true that the VIMSAS has inherent limitations in terms of the possibility of Member States' non-cooperation, and lack of feasibility and effectiveness derived from its voluntariness. This is well evidenced in the number of States accepting IMO audits (IMO, 2013d). To achieve the intrinsic objectives of the audit system, it is necessary to look into the limitations of the current scheme, and look for the ways to improve the VIMSAS.

The Korean Government received an IMO audit successfully on a voluntary basis in

April 2007. As a result, the Korean Government has been benefitted a lot from implementation of the IMO audit because Korea took this opportunity to re-evaluate the state of implementation of the IMO mandatory instruments. In the process of preparing for the audit, Korea took necessary actions ranging from enactment of relevant Acts and lower-level legislations such as Presidential and Ministerial Decrees. However, every Contracting Government is not like the case of Korea because of the diversity of social and financial situations each Contracting Government faces. Therefore, there are definite limitations to VIMSAS in terms of enforceability of the IMO Instruments.

Given the clear distinction of the Member State audit scheme between the IMO and ICAO, the IMO must also pave the way for the mandatory audit regime and the maritime world must prepare for the implementation of a mandatory audit scheme appropriately in the coming years. With regard to the change of the audit scheme, the Secretary-general of the IMO, Mr. Koji Sekimizu, also emphasized the importance of the mandatory audit scheme (IMO, 2012d) and the IMO is also trying to transform the current voluntary regime to mandatory one by 2016 (IMO, 2013c). Consequently, every Member State needs to keep a close eye on the development of the audit scheme and be prepared for drastic changes in the foreseeable future.

6.5.2 Effective implementation of port state control

Current Port State Control (PSC) is predominantly carried out on arriving vessels. It means that PSC does not explicitly focus on the control of vessel departures. However, it is technically more difficult to enforce law at sea than on land. In addition, a vessel moves globally and may therefore travel to States that do not participate in any PSC regime. Just as the departing port control is strictly implemented in the field of aviation, regulated by the International Civil Aviation Organization (ICAO), PSC regimes could integrate additional rules that help to establish an equivalent system (IMO, 2012b).

In addition to the new approach mentioned above, information sharing and cooperation among a number of PSC regimes is significant. Current PSC activities are carried out on an independent basis by 9 regimes around the world; the USCG, Paris MoU, Tokyo MoU and so on. Thus, the IMO needs to standardize the methodology of PSC and reinforce the cooperation and coordination between PSC regimes (IMO, 2012b). Through benchmarking the strongly-enforced PSC system of the USCG, and institutionalization of new methods to enhance the effectiveness of the PSC such as Concentrated Inspection Campaign (CIC) and New Inspection Regime (NIR) which are initiated by the Paris MoU, the enforceability of the IMO Instruments can be improved (Paris MoU, 2009; Paris MoU, 2012).

6.5.3 IMO technical cooperation program

IMO proactively encouraged Contracting Governments to implement the ISPS Code effectively and appropriately from the beginning of its entry into force of the ISPS Code by means of technical cooperation programs such as workshops and training courses (IMO, 2013a; IMO, 2013b). In addition, the MSC introduced a guidance on basic elements of a national oversight program for SOLAS XI-2 and the ISPS Code, and helped Member States to carry out self-assessment effectively.

In addition, regional cooperation programs have been conducive to the implementation of the ISPS Code under the auspices of the IMO. As an example, the fourth regional seminar on Latin American maritime legislation took place in Colombia in March 2006 in the presence of 37 delegations throughout South America. During this seminar, participants discussed how to implement IMO instruments effectively and suggested some recommendations for the ISPS Code, such as necessity of bi- or multilateral agreements on the exchange of information relating to security issues between

Contracting Governments, national legislation on responsibilities of the Recognized Security Organizations (RSOs), coercive actions for substandard port facilities and vessels, and applying the ISPS Code to non-SOLAS vessels internally (IMO, 2006a).

Considering the credibility and expertise of the IMO, each Member State needs to make the best use of the IMO assistance programs, and actively take part in regional programs which are held independently of or in collaboration with the IMO or other international organization such as APEC.

6.5.4 USCG IPS Program

On behalf of the IMO, the USCG has been playing a vital role in enhancing the standards of port facilities around the world by means of its International Port Security (IPS) Program. The USCG is mandated by the US Maritime Transport Security Act (MTSA) to assess security arrangements at non-US ports. As a result of assessment of foreign ports, a Port Security Advisory (PSA) is published.

The PSA clearly shows which port facilities are substandard, not complying with the ISPS Code and what kind of security measures will be imposed on vessels that call at substandard ports, bound for US ports. The PSAs list countries for which there are concerns regarding the ISPS Code compliance at all or some port facilities (Timlen, 2007). PSAs require the country directly concerned and all nations around the world, specifically having the interest of trade with the US, to pay attention to the security issue and take appropriate actions in order for vessels bound for the US to be granted permission to enter the US ports.

The most recent example of the effectiveness of the ISP program is the case of Nigeria in 2013. The Nigerian government has been desperately trying to enhance its security system as a result of the USCG ISP program conducted in May 2013. The Nigerian Maritime Administration and Safety Agency (NIMASA) has begun the process of installing what it called black flags in Nigerian ports that are not complying with the ISPS Code and Nigerian and IMO flags in the ISPS Code-compliant ports. These are part of the measures the agency has put in place to ensure it meets the ultimatum given to the Nigerian government to boost security in its maritime domain by the USCG (Iwori, 2013).

In the absence of strong enforceability of IMO instruments, the IPS Program of the USCG has made a great deal of contributions to the soft-landing of the new maritime security regime, the ISPS Code, since its inception in 2004. Even though IPSP is carried out based on mutual agreement and as a form of visit to foreign port facilities, it has tremendous enforcement power because PSA publishes substandard port facilities and states, and the additional security measures necessary such as raising Security Level onboard the vessels and strict inspection by the USCG at the time of port calls to the US ports.

As well-evidenced in Nigeria, the USCG has been playing a significant role in enhancing the IMO Contracting Governments' compliance with the ISPS Code instead of the IMO. It can be effective in the short term but this practice is not desirable in the long term for the IMO as well as the US. For the US, which is always deeply concerned with threats from anti-American groups around the world, the involvement in other country's administrations based on US domestic legislation, MTSA, can trigger backlash and ultimately attempted and real attacks on the US. The bottom line is to gain substantial enforceability of IMO Instruments by the IMO, not by other international or specific Contracting Governments.

6.6 Addressing the non-ISPS Code vessels

National maritime security systems have to be introduced and amended by introducing measures appropriate for the particular circumstances (Zec, et al., 2009) if the unique security threats exist at the national level in case of non-application of the Code. In this context, it is necessary to address the security aspects of the operation of non-SOLAS ships in a systematic and analytical manner, so as to achieve a tangible enhancement of the global security net which the provisions of SOLAS chapter XI-2 and the ISPS Code seek to establish. As a typical instance, the US Department of Homeland Security introduced regulations to address small vessels not subject to the ISPS Code; Small Vessel Security Strategy (SVSS) and Small Vessel Security Implementation Plan (SVS-IP) (IMO, 2011c).

A number of Contracting Governments have implemented or intend to implement common safety principles and rules for carriage of Automatic Identification System (AIS) equipment for ships which are not included in the requirements of SOLAS chapter V. Similarly, Turkey also mandated the carriage of AIS on certain classes of non-SOLAS Turkish-flagged vessels by issuing a related Directive in 2007 (IMO, 2008a).

The IMO MSC, at its eighty-fifth session, approved the non-mandatory Guidelines on security aspects of the operation of vessels which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code as guidance for Contracting Governments (IMO, 2008c). These guidelines have been formatted in two parts: Part 1 contains information of interest to Contracting Governments and other authorities with responsibilities for administering non-SOLAS vessels (commercial non-passenger, non-SOLAS passenger, fishing and pleasure vessels) and Part 2 contains information pertinent to the owners, operators and users of non-SOLAS vessels and related facilities (marinas, port and harbor facilities) with appendices containing information specific to the four vessels categories and facilities.

These guidelines were created from a series of efforts of Contracting Governments which proposed a number of documents to deal with security issues related to non-SOLAS vessels (IMO, 2006b; IMO, 2007) and, in particular, non-flagged vessels exploited for illegal immigration (IMO, 2010b). In terms of enhancing the level of security around the world, the guidelines of the IMO are not enough. Therefore, there is definitely strong need to introduce more powerful Instruments to mandate Member States to enact legislation and carry out security measures addressing non-SOLAS vessels.

6.7 Buildup of response to incidents

The ISPS Code is not a contingency plan for incidents, but contains preparatory measures for them. Unlike the expectations of the agencies concerned, there is always the possibility that security incidents happen. In this regard, the characteristic of preparedness of the Code must be consolidated with a response system to incidents at national and international levels.

Contracting Governments need to include the response system and procedure to security-related incidents as complementary measures in the process of domestic legislation of the ISPS Code. Likewise, the IMO should also review the current ISPS Code and engage it with response systems and emergency plans with Contracting Governments to improve the effectiveness of its implementation.

As a good example, the Korean government included a contingency plan to address real attacks or security incidents in the National and Regional Port Security Program from the moment when those programs were drawn up in 2008. However, domestic legislation in respect of the ISPS Code can be different nation by nation. In essence, preparedness and response are closely related to each other, so in the mid and long term it is necessary to consolidate a response system into the existing ISPS Code through the amendment of the ISPS Code or guidelines or suggestions for Model Legislation.

Looking into the effectiveness and challenges of the ISPS Code is meaningless unless reasonable recommendations are suggested to the whole maritime world. The primary objective of this paper is to provide recommendations to make the established ISPS Code more well-organized and effective. In order to make recommendations in this chapter come true, strong collaboration and coordination at the national and international level are required.

CHAPTER 7
CONCLUSION

The IMO maritime security regime, the ISPS Code, was introduced in 2002 in the wake of the 9/11 terrorist attacks and entered into force in 2004 to address terrorism. It has achieved substantial success in Korea: building capacity and infrastructure in respect of maritime security, raising security awareness, successful hosting of internationally important events, relevant and fast response to emergency situation, and reduction of security incidents.

Prior to the introduction of the ISPS Code, there was no Act-level legislation to address security issues in Korea, only a Presidential Decree which applies only to the public sector. With the newly-enacted Act-level legislation passed by the National Assembly, now Korea has a robust system regarding maritime security. Act-level legislation can control the public and private sector as well by means of articles in respect of offenses and penalties, so law enforcement in the field of maritime security has become more effective compared to the pre-ISPS Code era. Furthermore, it heightened the security culture inside the public sector in respect of compliance with rules and regulations. In addition, Korea has raised the Security Level stipulated in the ISPS Code and these experiences can be utilized by the IMO as well as by other Contracting Governments when they set up plans to strengthen security.

The beginning of this instrument was on the right track at the right time, but it is also true that it has left something to be desired based on Korean experiences, given the speedy process of the introduction of the ISPS Code and insufficient expertise in Korea. One of the challenges of the ISPS Code, pointed out in the process of implementation, has derived from the unique characteristic of the ISPS Code, recommendatory Part B. In the process of adoption and entry into force, it was agreed to leave Part B non-mandatory unlike Part A in order to give some room to Contracting Governments. It resulted in, to some extent, variations among Contracting Governments. The Korean ISPS Code Act does not have flexibility for implementing security measures under Level 3 unlike the IMO ISPS Code Part B, which prompted the Korean government to think about how to harmonize the balance between security and facilitation of trade.

In addition, the lack of IMO enforceability in the absence of a strong Member State audit scheme is another challenge the maritime world needs to address. Non-existence of a response system to incidents and narrow scope of applicability, ship/port interface, are significant points to be contemplated by the maritime world. Differences in security levels among different security regimes in Korea were also pointed out in this paper.

In order to address challenges found through Korean experiences in the implementation of the ISPS Code, this paper presented recommendations: i) sophisticated legislation at the national and international level such as the introduction of model legislation, 2) coordination with other security regimes in terms of number of security levels, 3) reinforcement of supply chain security through collaboration with other regimes such as AEO, CSI and MI, 4) buildup of the ISPS Code enforceability by means of transition of the IMO Member State audit scheme, from voluntary to mandatory, and active participation by the US and international entities, 5) addressing the threats from non-SOLAS vessels, 6) buildup of response to security incidents.

The most international conventions have evolved with numerous amendments reflecting the valuable experiences and lessons pointed out by the Contracting Governments. The

ISPS Code is not the exception. The fast-adopted ISPS Code has been significantly effective in addressing maritime security threats in Korea, but it has provided some challenges to be overcome. The maritime world can strengthen the enforceability and effectiveness of the ISPS Code through implementation of recommendations in this paper.

Adoption of security regime at the IMO and ratification by Member States must not be regarded as the sufficient measures to obtain security. The most important thing is to maintain security with every possible means including non-ISPS Code regimes which are implemented nationally and internationally. Just ratification of the ISPS Code at the national level can be illusion and self-satisfaction which can be shattered in real situations. At a time when this relatively young regime marks the tenth year of implementation, it is quite meaningful to look back on the past ten years and prepare for another decade with endeavors to enhance the effectiveness of the ISPS Code

REFERENCES

Asia-Pacific Economic Cooperation. (2010). Status Report on Asia-Pacific Economic Cooperation's ISPS Code Implementation Assistance Program (ICIAP).

BBC. (2010, May 20). 'North Korea torpedo' sank South's navy ship – report. Retrieved from http://www.bbc.co.uk/news/10129703

Botelho, R. (2004). Maritime security: Implications and Solutions. *Sea Technology*, 45(3), 16.

Burmester, C. (2006). International Ship and Port Facility Security (ISPS) Code - perceptions and reality of shore-based and sea-going staff.

Charalambous, N. (2003). Issues related to the development and implementation of the ISPS Code. *Contemporary Issues in Maritime Security*, 17-22.

Cho, J. (2004). Reinforcement of security at Busan ports in danger of terrorist attacks. *Yonhapnews*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=101&oid=001&aid=0000701622

Cox, L. (2013). The advent and future of international port security law. *National Security Law Journal* Volume 1, Issue 1 – spring 2013.

Craig, I., Coghlan, T., Evans, M. (2013). British shipping on highest-ever alert over Yemen terror threat. *The Times*. Retrieved from http://www.thetimes.co.uk/tto/news/world/middleeast/article3835122.ece

Customs and Border Protection. (2013). CIS in brief. Retrieved from http://www.cbp.gov/xp/cgov/trade/cargo_security/csi/csi_in_brief.xml

Department of Homeland Security. (2011, April 20). Secretary Napolitano announces implementation of National Terrorism Advisory System. *Press release*. Retrieved from http://www.dhs.gov/news/2011/04/20/secretary-napolitano-announces-implementation-national-terrorism-advisory-system

Euronews. (2010, November 11). Seoul on highest security alert for G20 summit. Retrieved from http://www.euronews.com/2010/11/11/seoul-on-highest-security-alert-for-g20-summit/

Franson, J. (2003). Formulating the ISPS Code: a general background. *Contemporary Issues in Maritime Security*, 9-15

Heathcote, P. (2004). An explanation of the new measures for maritime security aboard ships and in port facilities.

International Maritime Bureau. (2012, July 16). Six months drop in world piracy, IMB report shows. (2012). Relieved from http://www.icc-ccs.org/news/747-six-month-drop-in-world-piracy-imb-report-shows

International Maritime Organization. (2004a, February 25). Voluntary IMO Member State Audit Scheme. (Resolution A.946(23)).

International Maritime Organization. (2004b, June 30). Continued improvement in ISPS Code Implementation. *Press briefing*. Retrieved from http://www.imo.org

International Maritime Organization. (2005a, February 17). Maritime security on agenda as USCG Commandant visits IMO. *Press briefing*. Retrieved from http://www.imo.org

International Maritime Organization. (2005b, May 3). Draft SUA protocols ready for October Conference. *Press briefing*. Retrieved from http://www.imo.org

International Maritime Organization. (2005c, December 19). *Code* for the Implementation of Mandatory IMO Instruments. (Resolution A.973(24)).

International Maritime Organization. (2005d, December 21). Framework and Procedures for the Voluntary IMO Member State Audit Scheme. (Resolution A.974(24)).

International Maritime Organization. (2006a, August 11). Regional seminar on Latin American maritime legislation. (LEG 92/9)

International Maritime Organization. (2006b, September 27). Enhancement of the security of ships other than those already covered by the ISPS Code submitted by Japan. (MSC 82/4/5).

International Maritime Organization. (2007, August 14). Security measures for ships which do not fall within the scope of the ISPS Code submitted by Australia. (MSC 83/4/4)

International Maritime Organization. (2008a, March 4). National supplemental security arrangements submitted by Turkey. (MSC 84/4/2).

International Maritime Organization. (2008b, March 5). Development of model legislation on maritime security. (MSC 84/4/4).

International Maritime Organization. (2008c, December 22). Non-mandatory guidelines on security aspects of the operation of vessels which do not fall within the scope of SOLAS Chapter XI-2 and the ISPS Code. (MSC.1/Circ.1283).

International Maritime Organization. (2009, March 11). A brief report on how the ISPS Code has been implemented – Measures taken to enhance security policies and activities submitted by the Islamic Republic of Iran. (MSC 86/4/1).

International Maritime Organization. (2010a, January 18). Report of the third Latin American Forum on Maritime and Port Security submitted by Colombia. (MSC 87/4/1)

International Maritime Organization. (2010b, September 21). Enhancement to the ISPS Code submitted by Canada. (MSC 88/4/2).

International Maritime Organization. (2011a, March 7). Report of the correspondence group on the maritime security manual. (MSC 89/4/1).

International Maritime Organization. (2011b, March 8). A brief report related application and implementation of the ISPS Code including measures taken to enhance maritime security submitted by the Republic of Korea. (MSC 89/4/3).

International Maritime Organization. (2011c, March 7). Enhancement of the security of ships other than those already covered by SOLAS chapter XI-2 and the ISPS Code submitted by the United States. (MSC 89/4/4).

International Maritime Organization. (2012a, February 22). Australia's implementation of the ISPS Code submitted by Australia. (MSC 90/4/1).

International Maritime Organization. (2012b, April 17). “A new order in maritime security” organized by the Sasakawa Peace Foundation. (Circular letter No. 3267).

International Maritime Organization. (2012c). International Ship and Port Facility Security Code and SOLAS Amendments adopted on 12 December 2002, 2012 Edition, 274-275.

International Maritime Organization. (2012d, January 03). Positional Changes at IMO Secretariat. *Press briefing*. Retrieved from http://www.imo.org

International Maritime Organization. (2013a, March 22). Courses on: Implementation by Flag and Port States of Chapter XI-2 of the SOLAS Convention and the ISPS Code. (Circular letter No. 3354).

International Maritime Organization. (2013b, April 9). Workshops on APEC Manual of Maritime Security Drills and Exercises for Port Facilities submitted by Singapore. (MSC 92/15/2).

International Maritime Organization. (2013c, May 8). Implementation of the global program on Voluntary IMO Member State Audit Scheme note by the Secretariat. (TC 63/7).

International Maritime Organization. (2013d. June 3). Voluntary IMO Member State Audit Scheme - Member States that have volunteered to be audited. (Circular letter No. 3372).

International Maritime Organization. (2013e. July 9). ICAO, IMO and WCO chiefs strengthen ties in promoting global supply chain security. Press briefing. Retrieved from http://www.imo.org

International Maritime Organization. (2013f, July 31). Summary of Status of Conventions. Retrieved fromhttp://www.imo.org/About/Conventions/StatusOfConventions/Pages/Default.aspx

International Maritime Organization. (2013g, September 24). Review of planned outputs and indicators during the 2012-2013 biennium. (CWGSP 13/2).

Iwori, J. (2013, September 6). ISPS Code: US Coast Guard hail NIMASA response. *Thisday Live.* Retrieved from http://www.thisdaylive.com/articles/isps-code-us-coast-guard-hail-nimasa-response/158300/

Ji, S. (2005, October 25). Raising maritime security level in preparation of APEC Summit. *YTN*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=034&aid=0000239253

Kim, S. (2004, July 13). Ports, shippers on alert against terror threat. *The Korea Herald*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=108&oid=044&aid=0000045100

Korea Customs Service. (2013). Introduction of AEO. Retrieved from http://www.customs.go.kr/kcshome/main/content/ContentView.do?contentId=CONTENT_ID_000001325&layoutMenuNo=21042

Lee, Y. (2007. June 1). The result of the IMO VIMSAS on Republic of Korea. *Monthly Maritime Korea*. Vol. 405. Retrieved from http://www.monthlymaritimekorea.com/news/articleView.html?idxno=1337
McDonald, M. (2010, November 23). 'Crisis Status' in South Korea after North shells island. *The New York Times*. Retrieved from http://www.nytimes.com/2010/11/24/world/asia/24korea.html?pagewanted=all

McNaught, F. (2005). Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat.

Mejia, M., Mukherjee, P. (2004). Selected issues of law and ergonomics in maritime security.

Mensah, T. (2003) . The ISPS Code and the international regime to protect maritime security.

Ministry of Government Legislation. (2008) Presidential Decree on National Security. Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=90660&efYd=20081231#0000

Ministry of Government Legislation (MOLEG). (2009). Aviation Safety and Security Act. Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=94102#0000

Ministry of Government Legislation (MOLEG). (2013a). Presidential Decree on National Anti-Terrorism Activities. Retrieved from http://www.law.go.kr/admRulLsInfoP.do?admRulSeq=2000000093162

Ministry of Government Legislation (MOLEG). (2013b). Ministerial Decree on the Security of International Ship and Port Facility. Retrieved from http://www.law.go.kr/lsInfoP.do?lsiSeq=141485#0000

Ministry of Oceans and Fisheries. (2009, April 12). APEC maritime security experts visit Korean ports. *Korean government policy briefing*. Retrieved from http://www.korea.kr/policy/pressReleaseView.do?newsId=155343572&pWise=www2

Ministry of Oceans and Fisheries. (2010, October 19). Carrying out the reinforced security activities pursuant to the ISPS Code in preparation for G20 Summit. *Korean Government Policy Briefing*. Retrieved from http://www.korea.kr/policy/economyView.do?newsId=148700684&pWise=www2

Ministry of Oceans and Fisheries. (2011, December 30). Surveillance camera sharing for improvement of port facility security. *Korean Government Policy Briefing*. Retrieved from http://www.korea.kr/policy/pressReleaseView.do?newsId=155805084&pWise=www2

Ministry of Oceans and Fisheries. (2012, March 20). Reinforcing maritime security in preparation for Nuclear Security Summit. *Korean Government Policy Briefing*. Retrieved from http://www.korea.kr/policy/pressReleaseView.do?newsId=155817637&pWise=www2

Mukherjee, P., Mustafar, A. (2004). The International Ship and Port Facility Security(ISPS) Code and human element issues

Ng, AKY. (2009). Maritime security instrument in practice: a critical review of the implementation of ISPS Code in the port of Hong Kong.

National Nuclear Security Administration. (2013). Protecting the world’s shipping network from dangerous cargo and nuclear materials. Retrieved from http://nnsa.energy.gov/aboutus/ourprograms/nonproliferation/programoffices/internationalmaterialprotectionandcooperation/-5

Office of the Maritime Administrator of Republic of the Marshall Islands. (2013a, June 27). Current Security levels for Indian ports. Ship Security Advisory No. 27-13.

Office of the Maritime Administrator of Republic of the Marshall Islands. (2013b, August 8). Current Security levels for Indian ports. Ship Security Advisory No. 31-13.

Okoroji, L; Ukpere, W. (2011). The effectiveness of the International Ship and Port Facility Security Code (ISPS) in Nigeria. *African Journal of Business Management*. Vol. 5(4), pp. 1426-1430.

Oritse, G. (2013a, May 31). Nigeria yet to properly implement ISPS Code. *Vanguard*. Retrieved from http://www.vanguardngr.com/2013/05/nigeria-yet-to-properly-implement-isps-code-nimasa/

Oritse, G. (2013b, May 31). No accurate data on port facilities in Nigeria *Vanguard*. Retrieved from http://www.vanguardngr.com/2013/07/no-accurate-data-on-port-facilities-in-nigeria-report/

Paris MoU. (2009, May 25). Paris MoU adopts new Port State Control inspection system. *Press release*. Retrieved from http://www.parismou.org/Publications/Press_releases/2010.12.23/Paris_MoU_adopts_new__Port_State_Control_inspection_system.htm

Paris MoU. (2012, June 1). Paris and Tokyo MoUs on PSC will hold joint CIC on Fire Safety Systems. *Press release*. Retrieved from http://www.parismou.org/Publications/Press_releases/2012.06.01/Paris_and_Tokyo_MoUs_on_PSC_will_hold_joint_CIC_on_Fire_Safety_Systems.htm

Park, H. (2011, August 4). Entrance and exit at Pohang Port with the RFID. *Newsis*. Retrieved from http://news.naver.com/main/read.nhn?mode=LSD&mid=sec&sid1=102&oid=003&aid=0004004884

Polner, M. (2010, July). Compendium of Authorized Economic Operator (AEO) Programs. WCO Research Paper No. 8

Raymond, C. (2005). Australia's New Maritime security strategy. *Journal of the Australian Naval Institute*, 115, 14

Robertson, M. (2011). ISPS Code: Opportunities for new technology. *Port Technology International*.

Russia introduces three-level terrorism threat system. (2012, June 16). *Rio Novosti*. Retrieved from http://en.rian.ru/russia/20120616/174076486.html

Russia to adopt three-level terror threat scale. (2010. November 11). *RT News*. Retrieved from http://rt.com/news/prime-time/three-level-terror-threat/

South Korea to heighten airport security ahead of nuclear summit. (2012, March 15). *Yonhapnews*. Retrieved from http://english.yonhapnews.co.kr/national/2012/03/15/60/0301000000AEN20120315002000320F.HTML

Stephen, C. (2013). US consulate attack in Benghazi: a challenge to official version of events. *The Guardian*. Retrieved from http://www.theguardian.com/world/2013/sep/09/us-consulate-benghazi-attack-challenge

Timlen, T. (2007). The ISPS Code: where are we now?. *Cargo Security International*, April/May, 14-15.

United States Coast Guard. (2011, March 11). The U.S. Coast Guard is issuing a Port Security Advisory for Libya. Port Security Advisory (1-11)

United States Coast Guard. (2012a, September 5). Port Security Advisory (1-12)

United States Coast Guard. (2012b, November 27). Port Security Advisory (2-12)

Wright, R. (2005, May 23). World ports. *The Financial Times*. Retrieved from http://www.ft.com

Zec, D., Frančić, V., Šimić-Hlača, M. (2009). Ports security organization and functionality – Implementation of the ISPS Code in medium and small countries.