HÖGSKOLAN I BORÅS
VETENSKAP FÖR PROFESSION

How the ISPS code affects port and port activities

Arsham Mazaheri

The Thesis comprises 30 ECTS credits and is a compulsory part in the Master of Science with a Major in Industrial Engineering with specialisation in Logistics Management, 120 ECTS
Nr 2/2008

How the ISPS code affects port and port activities

Arsham Mazaheri

Master thesis

Subject Category: Technology

Series Number 2/2008

University College of Borås
School of Engineering
SE-501 90 BORÅS
Telephone +46 033 435 4640

Examiner: Farid Rohani

Supervisor: Daniel Ekwall,

University College of Borås
School of Engineering
SE-501 90 BORÅS

Client: Högskolan i Borås, Borås, Sweden

Date: April 2008

Keyword: ISPS code, Port security, Terrorism, Supply chain vulnerability, Risk assessment.

How the ISPS code affects port and port activities

By

ARSHAM MAZAHERI

A thesis submitted to the School of Engineering in conformity with the requirements for the degree of Master of Science

University College of Borås

(Högskolan i Borås)

Borås, Sweden

April 2008

*This thesis is dedicated to my dear parents, **Kambiz** and **Katayoun**, for their endless supports and for all they have done for me.*

این پایان نامه پیشکش شده است به مادر و پدر عزیزم، کتایون و کامبیز، به پاس حمایت بی دریغشان و نیز تمامی زحماتی که برای من کشیده اند.

Abstract

Following terrorist attacks on twin towers in the USA and Limburg oil tanker in Yemen, the IMO has defined a supplementary chapter and an appendix named ISPS code to its SOLAS, to prevent similar events in maritime transportation. The ISPS code forces the ports, ships and all organizations, who work in marine industry, to keep their security gates more tightly. This situation affects involved parties in good and bad ways. Good impacts like increasing in security level, efficiency, effectiveness and competitiveness; and bad effects like increasing in annual costs, administration works and manning.

This thesis is based on a study that was run by preparing an electronic questionnaire and distributing among the Swedish ports to get first hand information about the ISPS code impacts on port and port activities. Through them it was found that the ISPS code achieved its main goal, which it has been described as less smuggling and less theft in Sweden; while actually the ISPS is an anti terrorism regulation by its nature.

On the other hand, the indirect impacts of the code have played an important role in its success; therefore they have been reviewed as well. The ISPS code's indirect impacts on ports can be summarized as its effects on efficiency, effectiveness, administration cost, service price, profit, competitiveness, service level, customer satisfaction, damage occurring, documentation, manning , lead time and checking process.

Keywords: ISPS code, Port security, Terrorism, Supply chain vulnerability, Risk assessment.

Acknowledgment

I would like to express my gratitude towards many people who really helped me to do this thesis. Without them and their supports, I never would have been able to finish this thesis.

First of all, I am grateful to my supervisor, Mr. Daniel Ekwall, for his support, advices and introducing valuable literatures. Also I am thankful to Mr. Timothy Tinney and Mr. Hamed Khademi for their patience to my endless questions about English language.

Especial thanks to Mr. Lars Pålsson and Mr. Johan Ohlsson because of their guidance about security matters at ports and the ISPS code.

I would like to thank all the port administrators and port security officers of Swedish ports, who contributed in this study by answering the questionnaires; especially Mr. Peter Zoné for his friendly manner and also complete and really helpful answers.

I am full of gratitude towards my family for their support and their belief on me and also towards Mr. Kavous Mazaheri for his great help on editing the thesis.

At the end, I have to admit that without understanding and encouragement from my dear girlfriend, I was never able to do this thesis. I am deeply indebted to you, my lovely Bita.

Borås, Sweden
April 2008

Arsham Mazaheri

Table of contents

List of Figures

List of Tables

List of Charts

1. Introduction

In this chapter, the aims of thesis beside the problems that are going to be addressed by this study and the research questions have been discussed. Also the limitations of this research have been argued.

1.1 Purpose

The aim of this thesis is to define the effects of IMO's[1] new regulation, ISPS code, on main part of maritime industry, ports. It has been tried to find if the code was successful in its defined purposes after four years of its implementation. Besides, it has been tried to analyze the vulnerabilities of port activities, as a sub-part of supply and demand networks, to this brand new regulation. The indirect impacts of the ISPS code on maritime industry, which can affect supply chain efficiency, have been studied too.

1.1.1 Problem statement

According to Oxford dictionary, Vulnerable *(adj.)* or Vulnerability *(n.)* are defined as hurt, harmed or attacked easily, especially because of being small or weak. If some thing is vulnerable, it means that it is susceptible to physical injury or attack.

The other word, which is being used regularly alongside vulnerability, is resilience. Oxford dictionary defines Resilient (*adj.*) or Resilience (*n.*) as ability to quickly recover from shock, injury, depression. If some thing is resilient, it means that it is able to recover when it is damaged or injured.

These two words are like twins. Some believes that they are opposite of each other, while they are actually complementary. If a system or a person is vulnerable, it means that some threats or disasters can injure or damage it, even if it is resilient. The truth is that a system or person can be resilient as well as vulnerable. If some thing is resilient, it does not mean that it is safe from being injured or attacked; it just means that it can be recovered from the injury.

By designing and considering security and safety provisions, the vulnerability of a system can somehow be addressed. However, despite all provisions, there is no security and safety system which is 100% trustworthy. Therefore, resilience of a system is another issue, which shall be considered while implementing risk assessment, in addition to vulnerability.

Like every human defined system, the transportation system especially maritime, is vulnerable. When this system locates as a sub-part in a bigger system, like supply chain and supply network, it can make the superior-system vulnerable in same or some other ways as well.

Maritime transportation is vulnerable to some factors like natural disaster, climate change, terrorist attack, piracy, hijacking, insurgency and some other incidents like ship collision or fire. On the other hand, when seaborne transportation is looked as a part of supply network, some other factors, which are not really a risk for maritime transportation, can be interpreted as a threat. In this situation, to find the other possible risks for a maritime transportation as a sub-system, the superior-system's vulnerabilities must be examined.

The supply chain vulnerability is defined as a threat or incident that causes a serious problem in JIT process application (*Kord & Pazirandeh, 2006*); some threats like delay, infected product,

[1] For a complete list of all abbreviations used in this thesis, see Appendix 3: *Abbreviations*

wrong quantity delivery etc. They can happen in production process and warehouse keeping as well as transportation (*Kord & Pazirandeh, 2006)*. In addition to sea transportation's own vulnerabilities, JIT process can be jeopardized through maritime transportation by other factors that can not be sorted as marine threats; like unscheduled delay, unexpected route change, smuggling, and cargo theft.

Therefore, one of the supply chain drivers' main concerns is to address the causes of disruption to avoid them of being happened; whereas the maritime organizations' concern is to protect the shipping industry, sea environment and human lives at sea; which MARPOL 1973, SOLAS 1978, OPRC 1990, ISM 1993, and recently ISPS 2002 are some of these efforts by IMO.[1]

As it will be discussed later in chapter 2, the ISPS code has come to address the maritime problems related to terrorism; although by doing this mission it will be able to address other similar problems like theft and smuggling. Moreover, a mutual concern about shipping industry is to mitigate the maritime transportation vulnerabilities and their consequences, and also to make it resilient against threats, whether from sub-system perspective or superior-system point of view. Therefore, important question which would be asked by supply chain drivers, when a new regulation in maritime industry approves, is that "What and how their business can be affected by the new rule?" and "How the new regulation can make the waterborne transportation, as a part of inter-modal transportation, resilient?"

As it will be mentioned in chapter 3, quite bit efforts like papers and conferences have been done to answer these questions regarding to IMO new rule, the ISPS code.

This study is another attempt to find part of the answers of the above questions.

1.1.2 Research questions

In general, the basic question of this thesis is same as the subject of the thesis:

"How the ISPS code can affect port and port activities?"

This general question has been divided into two more specific questions, which have been tried to answer during the study.

Q1. What are the main impacts of the ISPS code on shipping industry?

Q2. How can they affect port and port activities?

At the end, it has been tried to answer the question about the ISPS code achievement.

Q3. Has the ISPS code accomplished its mission well?

1.2 Delimitations

Countries of the world can be divided into four groups according to their development levels and their foreign policies. (Figure 1)

1- Developed countries with calm foreign policy

2- Developed countries with belligerent foreign policy

3- Developing countries with calm foreign policy

4- Developing countries with belligerent foreign policy

[1] Appendix 3: *Abbreviations*

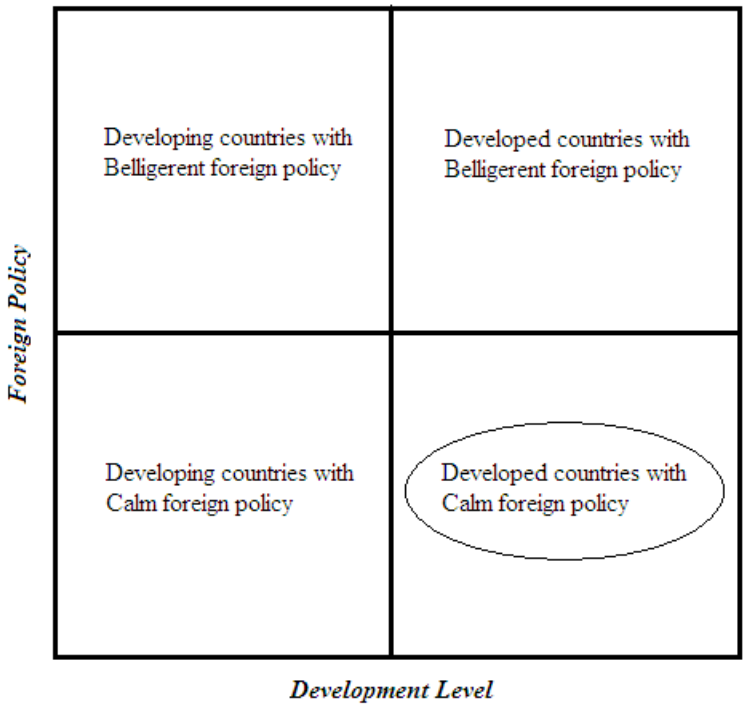


Figure 1, Thesis Scope

In spite of the fact that the research questions of the thesis have been defined to find the impacts of the ISPS code on ports and port activities in general, they have been answered according to the ports located in Sweden, which is one of the most developed[1] and richest[2] countries in the world with really calm foreign policy[3] (countries on right down side of Figure 1). Even though some of the results are applicable for all countries, who have applied the ISPS code, but the most impacts of the code, which have been presented in this study, are highly dependent on where the code is implemented.

Furthermore, the main focus of this thesis is from administrative perspective rather than economical view, although the indirect economical impacts of the ISPS code have been challenged in some ways too.

1.3 Outlines

The outline of the thesis is presented in this chapter to conduct the reader directly to what he/she looks for.

Chapter 1 describes the aim of the thesis and defines the problem that this study has tried to address. Scope of the thesis beside the research questions have been clarified in this part.

---

[1] "Aided by peace and neutrality for the whole of the 20th century, Sweden has achieved an enviable standard of living under a mixed system of high-tech capitalism and extensive welfare benefits. It has a modern distribution system, excellent internal and external communications, and a skilled labor force." *(The World Factbook, 2007c)*

[2] Sweden is 25th country in the world (among 229 countries) according to its GDP per capita with $32,200 PPP *(The World Factbook, 2007c)*

[3] "A military power during the 17th century, Sweden has not participated in any war in almost two centuries. An armed neutrality was preserved in both World Wars." *(The World Factbook, 2007c)*

Chapter 2 includes a brief view and short knowledge about the history of the ISPS code and its objectives as well as some definitions for thesis keywords, like terrorism and security.

Chapter 3 provides a broad view of the previous similar works done by others about the impacts of the ISPS code.

Chapter 4 presents the methods, which have been used for data collection and data analyzing. In addition, the validity and credibility of data sources and results have been discussed.

Chapter 5 presents the outcomes of the distributed questionnaires, beside the author's interpretations from them. Some selected answers from different ports have also been quoted

Chapter 6 concludes the thesis. It also includes answers to the research questions

Chapter 7 presents the complete list of the references which have been used in this study

Chapter 8 contains the appendices to this thesis; like the questionnaire that has been used to collect the primary information, the list of the abbreviations which have been used in thesis beside their definitions and the list of the cooperators companies.

2. Background information

In this chapter, a brief view and short knowledge about the ISPS code and its history has been prepared. The thesis keywords like security, terrorism and supply chain vulnerabilities have been clarified too.

2.1 A brief review of security and safety

Risk and danger are the mothers of both safety and security. But the notion of safety has come to life before security. From the beginning of the world, when human ancestors were fighting with their hands and stony weapons against the wild nature, safety was born. They never slept at a place where they felt danger to be surprised by wild animals, humans or disasters.

On the contrary, security was born when the humans learned to live in societies. Empires, factions, borders and cities were created and thereupon new dangers were discovered. Security was created to protect the communities. Walls were built around the cities to avoid enemy attacks, and spies' tongues were cut to prevent the leak-out of information.

Safety and Security are two words that most of the time come together or are use instead of each other. American Heritage dictionary has described the security as safety. It is a bit complicated (maybe not for native English speakers) to use the right one in right place. As Mark Twain said *"the difference between the almost right word and the right word is really a large matter – it is the difference between the lightning bug and the lightning."*

It is necessary to know where it is meant security and where is safety to avoid misunderstanding.

In general, Safety is reducing the risk or occurrence of loss, injury or death which will be occurred because of some accidental events or natural causes like natural disasters, while Security is reducing the risk or occurrence of loss, injury or death which will be occurred because of deliberate or intentional actions. (*Neal, 1994*)

Security subjects were given heightened attention after 9/11 aviation terrorist attack on world trade center twin towers and Pentagon in New York, U.S. (*Timlen, 2006*) Even though the security was not a new subject (*Timlen, 2006*), but most of the actions to enhance security have started after that catastrophic terrorist attack. [1]

2.2 Maritime security

Security in transportation is more or less similar to security in computer and software. There is no end-line to stop development for anti-virus or anti-hacker software. Every day the hackers and programmers, who want to attack computers of organizations or home-users to abuse them, are increasing their knowledge and abilities. The people, who try to smuggle, steal cargos or use global transportation to achieve their demonic goals, are increasing their capabilities together with technology improvement. It means their powers are growing up and governments, security agencies and organizations have to have continuous research, if they want to cope with. On the other hand, if transport security goes far beyond of what exactly needed, it will convert to a hedge, instead of being a good incentive, for developing in transportation business (*D'Addario, 2006*).

[1] The war on terror with the USA leadership by attacking to Afghanistan; or tight security checking for traveling by plane in the US and the EU airports are some examples of that.

Inter-modal transportation is a term in transportation that recently has been used simultaneously with globalization and growing the world economy[1] *(Donovan, 2004)*. Today the logistics chain in world trade is meaningless without using inter-modal transportation. Meanwhile, the seaborne transportation is not only the main and influential part of this inter-modal logistic chain[2], but also the most vulnerable mean of transportation. Mattias Wengelin (2006) has metaphorically likened the inter-modal transportation to the flow of blood in our body, where the artery flow is the maritime transport system and the capillary flow represents the other means of transportation by air, rail, and on-road-bound systems.

Since the power of each supply chain depends on the power of its weakest link (*Coleman & Jennings, 1998)*, therefore security in maritime logistics is the subject that has a great potential to work and investigate on.

Although there are a fair amount of examples in maritime misdeeds like smuggling, theft, stowaways or illegal immigrants, but the major concern about the maritime security was about piracy, armed rubbery and terrorism; however the terrorism took the most consideration after the 9/11 attack.

2.2.1 Maritime incidents

As it is mentioned earlier, there are quite a bit of examples about maritime offenses before and after 9/11. Here are some of them, which are highlighted in maritime industry, by way of illustration:

1. The *Achille Lauro* was an Egyptian passenger liner, which hijacked on October 7th 1985. Four men, who represented themselves the Palestine Liberation Front, took control of The *Achille Lauro* while she was sailing from Alexandria to Port Said within Egypt. A passenger was murdered in that action.
2. Nine tourists were killed by Palestinian gunmen onboard the *City of Poros*, which was a Greek passenger ferry, in the evening of the July 11th 1988.
3. *Our lady of Mediatrix* was a Philippians' ferry. On 26th February 2000, two bombs that were hidden inside two onboard crowded buses, exploded and killed 45 passengers.
4. An attack by Al-Qaeda terrorist group was against *USS Cole* on October 12th 2000. It was happened by a small explosive boat while the *Cole* was moored in a Yemeni port in Aden. In that action 17 sailors were killed and 39 of them were injured.
5. On 11th December 2001 the Christian ferry, *Kalifornia*, was bombed in Indonesia's Maluku Archipelago. The attack killed 10 and injured 46 passengers.[3]

[1] Inter-modal transportation, itself, goes back to 18th century, predates the railways. The inter-modal notion, which is being used nowadays for freight transportation, goes back to standardization of ISO container by the US department of defense between 1968 and 1970. *(DeBoer, 1992)*

[2] In Sweden, approximately 85% of all goods measured in tons or 60% of the value of the goods are transported via ports (*Sveriges Hamnar, 2006*) and also approximately 80% of world trade measured by volume, transport by ships *(UNCTAD, 2002)*

[3] "Christians tended to believe that a bomb had been placed on the boat but it is possible that the explosion may have been accidental." (*ICG Asia Report N° 31, 2002b*)

6. Another terrorist attack, again by Al-Qaeda, was launched against a French oil tanker named *Limburg* on October 6th 2002 while she was in the Gulf of Aden, Yemen and carrying 397,000 barrels of crude oil. A sailor was killed, 12 other crew members were injured and about 100,000 barrels of oil spilt.[1]
7. The world's deadliest terrorist attack at sea, is the attack that was launched by Abu-Sayyaf terrorist group against the *Supper Ferry 14* on 27th February 2004 in Manila bay, near Corregidor Island, which perished 116 people. The explosion was happened by a television set containing a 4 kilograms TNT time bomb that was hidden onboard.
8. Another Al-Qaeda attack took place in April 2004, against an oil terminal near Basra, Iraq. Two U.S. Navy sailors and one U.S. Coast Guardsman were killed. The attack damaged the terminal and shut it down for two days. This event highlighted the maritime strike capability[2] of Al-Qaeda in the Persian Gulf. (*Köknar, 2005*)

These events, especially *Limburg* incident[3], have shown shipping's potential vulnerability to terrorist attacks and made the shipping society worried about being a target for terrorist groups. Using a ship to smuggle a WMD[4] or as a weapon[5] to attack another vessel or critical infrastructures like bridges, harbors or port facilities, blockade a port or a marine path by immersing a ship, or even an attack upon a passenger ship by exploding a secreted bomb aboard *(BIMCO, 2002a)* or an explosive-laden craft, are events that are dreadful for whoever works in maritime industry. These all are anxieties beside environmental negative impacts that they may cause.

Although all of the mentioned examples and some other similar attacks were inhumane actions, but it should be considered that it will be misjudgment if all of them be categorized as a terrorist attack. In fact, each event has to be matched with some definitions to be named as a terrorist attack.

Most of the countries and organizations have almost same idea about terrorism and terrorist attack, but each one will categorize actions as terrorist according to their own definitions[6]. The definitions are more or less similar. They almost came up with same idea for the main parts and they have just some differences in details.

2.3 Terrorism definition

The United Nation (UN) has described terrorism as *"any action… that is intended to cause death or serious bodily harm to civilians or non-combatants, when the purpose of such an act,*

[1] "The attack on the Limburg did not produce the kind of spectacular explosion conjured by popular imagination, and shipping industry experts said it would be extremely difficult for an attacker to get a tanker to blow up that way; even direct missile hits during the Iran-Iraq war generally resulted only in spills and containable fires. But an attack or accident that crippled even one big oil tanker could have an appreciable effect on the flow of crude." (*Timmons, 2004*)

[2] "Acting as a maritime terrorist group is much harder than a land one; because being a land terrorist group needs less skill. Therefore, it is not possible for every terrorist group to act in maritime field." (*Chew, 2005*)

[3] Limburg incident played the same role for the ISPS code birth as Titanic tragedy played for SOLAS birth

[4] Weapon of Mass Destruction

[5] Ships like gas carriers or oil-tankers (LNG, LPG, VLCC, ULCC, etc). Although it would not be so easy to blow up a crude tanker; but on the other hand, gas carriers due to the high pressure tanks that they have, and tankers which carry flammable products of oil, like petrol, are highly explosive.

[6] Refer to Terrorism Definition by Lord Carlile of Berriew Q.C. (*Carlile, 2007*)

by its nature or context, is to intimidate a population or to compel a government or an international organization to do or to abstain from doing any act".

In addition, the Federal Bureau of Investigation (FBI) in the USA has defined terrorist action as *"the unlawful use of force or 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"*.

Even though almost every country and organizations have its own definition for terrorism *(Carlile, 2007)* but most of their definitions for terrorism are more or less similar to the UN's and the FBI's.

As it is perceptible, one of the conditions that these definitions have indicated that an action must has, to be classifiable as a terrorist attack, is being "against civilians". By considering this fact, the Al-Qaeda attack against the USS Cole can not be described as a terrorist attack as it was launched against a navy. On the other hand, as the Al-Qaeda has been known as an international terrorist group, any action and any attack that this group will or has launched will be categorized as a terrorist attack. Therefore, it will be sensed that, although there is a nearly unique definition for terrorism, but in some cases the public sensation of terrorism has more effect on classification of an act as a terrorist one, which can differ from one point of view to another.

In this situation the terrorism concept beside the public fear and abhorrence from this inhumane action, can give an opportunity to some governments or organizations, to cover their personal goals within it.[1] There are no differences between these governments and the ones, who are hiding their personal purposes behind the religion.[2] Both are abusing a notion (one from terrorism, another religion) to repress their adversaries.[3]

If an action has been done in a non-violent manner, it can not be described as a terrorist action, like a peaceful protest or strike; even if it is forced to be an aggressive aggregation by repressive units. But it would be so easy to ascribe them to a terrorist group and then easily wipe them out. Therefore, it should be wakeful when we are using the term terrorism to avoid abusing it. In this survey, the definition, which will be used for terrorism, is a combination of the UN's and the FBI's definitions by reserving their copyrights.

The "unlawful use of force or violence" phrase in the FBI's should be eliminated as it has great potential to be misused. On the other hand, the "property" term in the FBI's is the word that has been neglected from the UN's definition. The term "non-combatant" also is the word that has not been mentioned in the FBI's definition, which it should be. As a result, the definition of terrorism that is going to be used in this survey is:

> Any action that is intended to cause death or serious bodily harm to civilians or non-combatants or destruct a property, when the purpose of such an act, by its nature or context, is to intimidate the civilian population or any segment thereof or coerce a government or an international organization, to compel to do or to abstain from doing any act in furtherance of political, social or economic objectives. *(The FBI& the UN)*

[1] War against Iraq, which has been launched by the USA and the UK intractable and without the UN permission, is an example.

[2] People discontents from most of religious governments in the world, like Wahhabis in Saudi Arabia, Islamic Republic in Iran or Taliban in Afghanistan, are the witnesses.

[3] Of course, the religious terrorist groups, like Al-Qaeda, are abusing religion to reach to their goals as well.

However this definition is almost acceptable for this study, but it should be attended that this definition has some potential to be misused as well. For example, hijacking, kidnapping and armed rubbery could be included in that. But it must be considered that these actions must not be categorized as a terrorist attack without considering their intentions. Always should be aware that although terrorist actions and other violent actions are the actions which normal citizens hate them, but they have differences in their intentions by far.

2.4 The ISPS code

In November 2001, following the 9/11 tragic event, which showed no country in the world is safe from terrorist attacks[1], the International Maritime Organization (IMO) agreed to develop new measures relating to the security of ships and port facilities. Thereafter, in December 2002, a new rule for security issue in ships and port facilities was defined by a week-long Diplomatic Conference (December 9 to 13, 2002) at the London headquarter of IMO and was entered into force on July 1st, 2004, to reinforce maritime security and prevent similar terrorist acts against shipping.

The new rule is in the form of amendment to the 1974 Safety of Life at Sea (SOLAS) Convention. The complete name of this new regulation is the International Code for the Security of Ships and of Port Facilities with the abbreviated name of the **I**nternational **S**hip and **P**ort Facility **S**ecurity Code or the ISPS Code.

As it is mentioned previously, safety and security are two different issues which IMO considered this fact as well to define new regulation. Before adopting the ISPS code, the SOLAS had a chapter (Chapter XI) that contained special measures to enhance maritime safety. In December 2002, the chapter XI was re-named to chapter XI-1 and a new chapter (Chapter XI-2) was added on special measures to enhance maritime security. The ISPS code has been added as a supplement for this new chapter.

Chapter XI-2 applies to passenger ships and cargo ships of 500 gross tonnages (GT) and upwards, including high speed craft, mobile offshore drilling units and port facilities, which serving such ships engaged on international voyages.

The code contains two parts, A and B. The former part (A) is compulsory while the latter part (B) is not; and it is just a guideline when implementing security provisions in part A. However, it is recognized that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and cargo. In spite of this, following the adoption of the code, the USA declared that compliance with Part B would be mandatory for US flag ships and all foreign flag ships visiting the US. Also, they attempted to persuade Maritime Safety Committee (MSC) to adopt an amendment to the ISSC[2] template which would indicate whether the Ship Security Plan (SSP) was so compliant. This was defeated at 77th session of MSC in May 2003 and was recorded in circular 1097, which clearly states that Part B is recommendatory. (*Lloyd's Register, 2007a*)

Besides, the European Union parliament, in its new regulation to enhance ship and port facility security[3], made some sections of part B of the code mandatory, but just for its member states; and also made part A of the code mandatory for their domestic class A passenger ships.

---

[1] The bombing in Bali (Indonesia, October 12th, 2002), Madrid (Spain, March 11th, 2004), London (England, July, 7th, 2005) and in Sharm el-Sheikh (Egypt, July 23rd, 2005) are some proofs for this reality.

2 International Ship Security Certificate

3 Regulation (EC) No 725/2004 of the European Parliament and of the Council of March 31st, 2004 on enhancing ship and port facility security *(2004b)*. (Came into force on July 15th 2007)

In addition, the definition for port area that must be protected has been changed in EU directive. According to EU directive, the properties and infrastructures like oil tanks or power plants, which are located in port area and are important to be protected and also the areas nearby them, must be included in the protected area as well.[1]

2.4.1 Objectives

Basically, the ISPS code has been applied to ensure that the security of ships and port facilities, onboard the ships and at the port/ship interfaces, will always be in place. Since the core of the ISPS code has been based on risk management activities, continuous risk assessments must be done at regular time intervals, to be sure that the security of seaborne transportation will be provided. Therefore, the main goal of the ISPS code is to establish a uniform and international framework for the risk evaluations in maritime transportation industry.

The general objectives of the ISPS code, as IMO has mentioned, are:

1- To establish an international framework, involving co-operation between Contracting Governments[2], Government agencies[3], local administrations and the shipping and port industries to detect and assess security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;

2- To establish the respective roles and responsibilities of all these parties concerned, at the national and international level, for ensuring maritime security;

3- To ensure the early and efficient collation and exchange of security related information;

4- To provide a methodology for security assessment so as to have in place plans and procedures to react to changing security levels;

5- To ensure confidence that adequate and proportionate maritime security measures are in place.

2.4.2 Contents

The ISPS code contains two parts, A and B. The former part (A) is compulsory while the latter part (B) is not; and it is just a guideline when implementing security provisions in part A.

Part A

Part A of the ISPS code contains 19 sections and 2 appendixes. The sections contain definitions, applications, responsibilities of in charged parties and technical information about the requirements of the Code.

It defines:

1- The obligations of the company, ship, port facility and of the contracting government,

[1] According to part A of the ISPS code, the port facility should relate solely to the ship/port interface. On the other hand, in part B (15.5), identification and evaluation of important assets and infrastructures in port facility, which are important to protect but are not covered by ship/port interface term, is recommended.

[2] The government of countries, who are the members of IMO

[3] The agencies, which are in contract with the Contracting Government to do particular delegated job

2- The necessary requirements which risk assessments and security plans must have,

3- The way that the records must be provided and be kept,

4- The information about training and exercising of the crew and staff

5- The requirements about the certification and verification for ships

The appendices of part A contain two sample forms for *ISSC* (International Ship Security Certificate) and *Interim-ISSC*. Through these forms, the requirements to issue the certificates can be understood.

Part B

Like part A of the ISPS code, part B of the code contains 19 sections[1] and 2 appendices as well. More details and guidelines about the mentioned subjects in part A are included in part B. In some ways, applying part A without taking part B into account seems a vain effort. Also the different interpretation of the code, which is one of the main weaknesses of the ISPS code, could be ineffective in many ways, if all the parties bear part B in mind while implementing part A of the code.

In the appendices of part B, the *Declaration of Security* (DOS) form and *Statement of Compliance* form for port facility have been provided.

2.4.3 How ISPS code works [2]

Since the ISPS code is based on risk assessment, the first step to carry out the code is risk and security assessment. A security assessment is a process that identifies weaknesses in infrastructures and physical structures, databases and information systems, communication systems, personnel protection systems, processes, or other areas that may lead to a security breach, which can pose a risk to persons or properties. It also suggests options to eliminate or mitigate the risks and their consequences that would be identified.

Two security assessments have been considered in the code; Ship Security Assessment (SSA) and Port Facility Security Assessment (PFSA). After implementing the SSA and PFSA, the Ship Security Plan (SSP) and Port Facility Security Plan (PFSP) shall be prepared according to them. It means that the security assessments are essential and integral part of the process of developing and updating the security plans. For each security plan, there is a security officer who is in charge for implementation of the security plan.

Ship Security Assessment (SSA)

The Ship Security Assessment (SSA) is an assessment that defines the vulnerable parts in ship structure or operation. According to part A of the ISPS code, a SSA shall include an on-scene security survey. It should consider the persons, activities, services and operations that it is important to protect. Also it should mull over all possible threats and vulnerabilities that may occur for the ship whilst she is at berth, anchor or at sea. The threats that may also happen while she is at ship/port interface shall be considered as well. Moreover, the conflicts between safety and security measures shall be well thought-out. The ship security assessment is an

[1] Sections no. 7, 11, 12, 14 and 19 do not have any additional information. Relevant guidance is provided under sections 8, 9 and 13 for sections 7, 11, 12, and under sections 15, 16, 18 for section 14. Section 19 does not have any further guidance.

[2] The ISPS code, version 2003, is the main reference of this part. Most of the definitions and sentences (but not the figures) have been taken in from there. This is to avoid too much citation in the text.

essential and integral part of the process of developing and updating the ship security plan, therefore it shall be reviewed periodically.

Company Security Officer (CSO) is the responsible person for SSA in all ships belonging to the company. She/he should ensure a ship security assessment is carried out for each of the ships in the company's fleet which is required to comply with the provisions of the ISPS code. When SSA has been done, Interim- ISSC can be issued. What's more, SSA can be done by a Recognized Security Organization (RSO), which is an organization that is certified to work in security issues and Contracting Governments may delegate some security related duties to it.

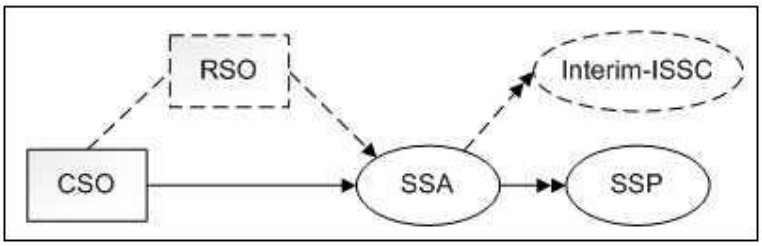


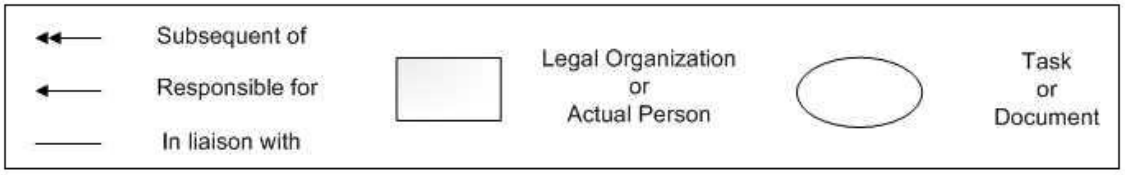
Figure 2, Ship Security Assessment according to the ISPS code[1]

Ship Security Plan (SSP)

When the SSA has been done, the Ship Security Plan (SSP) will be prepared according to SSA. A ship security plan is a plan to ensure that all measures on board have been properly designed to protect the ship, persons on board, cargo, cargo transport units and ship's stores from the risks of a security incident. For preparing the SSP, all the scenarios that might be happened must be considered and proper actions according to specific threat has to be thought over. The SSP shall be reviewed and updated periodically according to the SSA. Like SSA, the SSP can be done by a RSO. In this case, the RSO shall not be same as the RSO who have prepared the SSA.

When the SSP was prepared and approved, the International Ship Security Certificate (ISSC) can be issued.

[1] The legends which have been used in Figure 2 till Figure 11



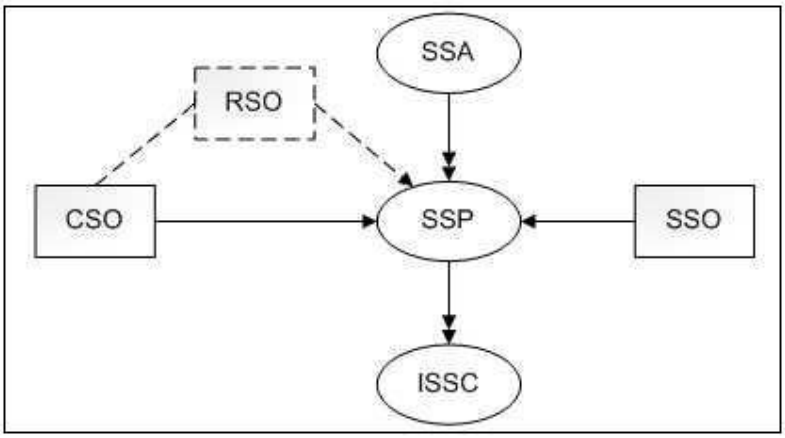


Figure 3, Ship Security Plan according to the ISPS code

Ship Security Officer (SSO)

The Ship Security Officer (SSO) is the person on board the ship accountable to the master, for security of the ship; including implementation and maintenance of the SSP. The SSO is in liaison with the CSO and the Port Facility Security Officers (PFSO). The SSO could be also the master of the ship, which this should be defined by ship administrator.

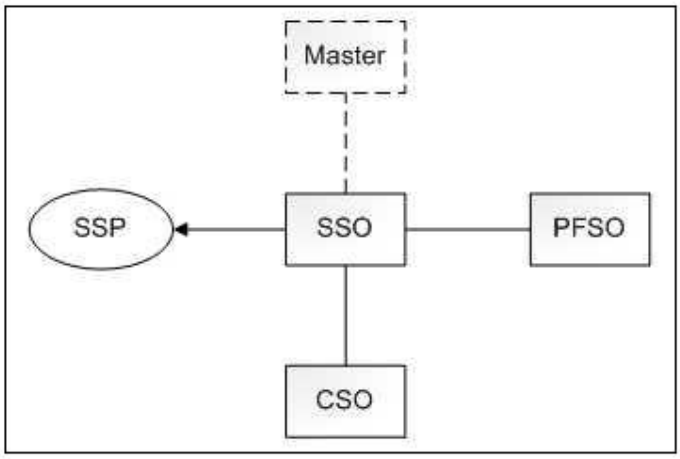


Figure 4, Ship Security Officer according to the ISPS code

Figure 5 concluded the ship security procedure according to the ISPS code. The ship/port interface has not been considered in the Ship Security Diagram.

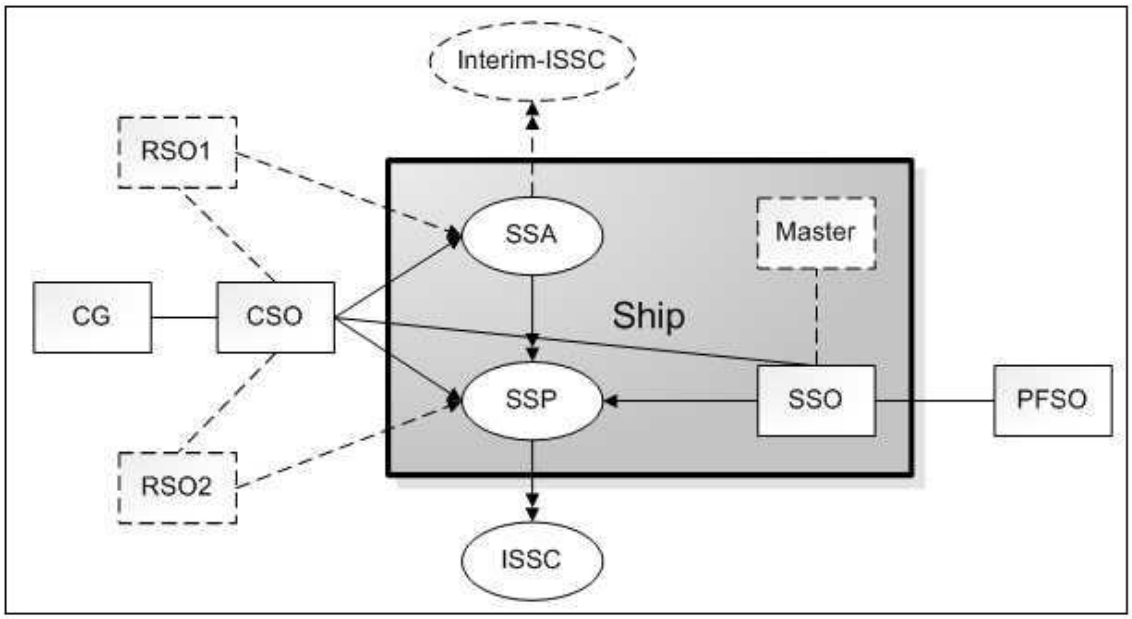


Figure 5, Ship Security diagram according to the ISPS code

Port Facility Security Assessment (PFSA)

The PFSA is a risk analysis of all aspects of a port facility's operation in order to determine which parts of it are more susceptible to be the subject of attack. All possible threats should be considered. The vulnerability of each target and the consequences of each attack shall be considered as well, while the PFSA is carrying out.

The assessment shall include, at least, the following elements:

1. Identification and evaluation of important assets and infrastructures that are important to protect
2. Identification of possible threats to the assets and infrastructures and the likelihood of their occurrence along with their consequences, in order to establish and prioritize security measures
3. Identification, selection and prioritization of counter measures and procedural changes and their level of effectiveness in reducing vulnerability
4. Identification of weaknesses, including human factors in the infrastructures, policies and procedures

The Contracting Government (CG) is responsible for implementation of PFSA in the ports that are located within its territory, which also may delegate it to a RSO to carry out.

Like SSA, the PFSA shall be reviewed and updated periodically; specifically when major changes to the port facility take place. When the PFSA was done, the Port Facility Security Plan (PFSP) shall be prepared according to it.

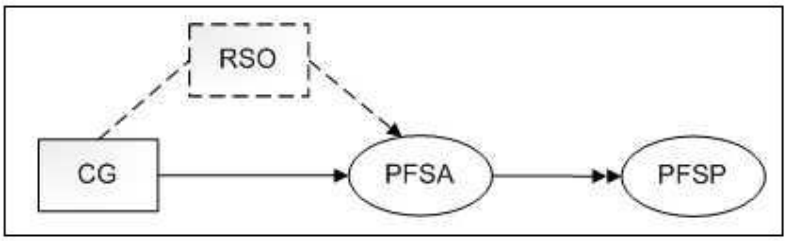


Figure 6, Port Facility Security Assessment according to the ISPS code

Port Facility Security Plan (PFSP)

When the PFSA has been prepared, the Port Facility Security Plan (PFSP) shall be designed according to it. PFSP is a plan to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident. The Port Facility Security Officer (PFSO) is responsible for development, implementation, revision and maintenance of the PFSP.

PFSP approval is the responsibility of the Contracting Government which can be delegated to a RSO. Same as what has been remarked for ship security, the RSO who have prepared the PFSA can not contribute in the PFSP approving process.

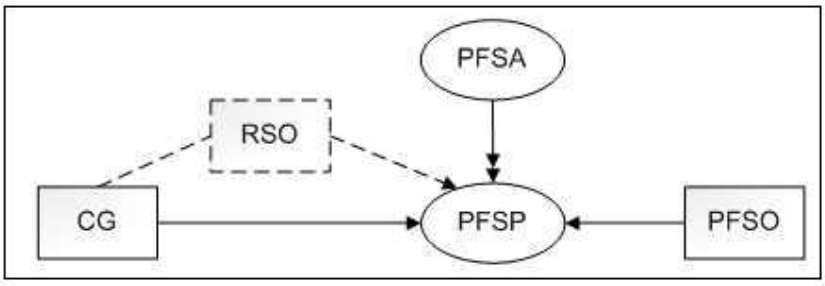


Figure 7, Port Facility Security Plan according to the ISPS code

Port Facility Security Officer (PFSO)

Port Facility Security Officer (PFSO) is the person who appointed as responsible for the development, implementation, revision and maintenance of the PFSP and for liaison with the SSO and the CSO.

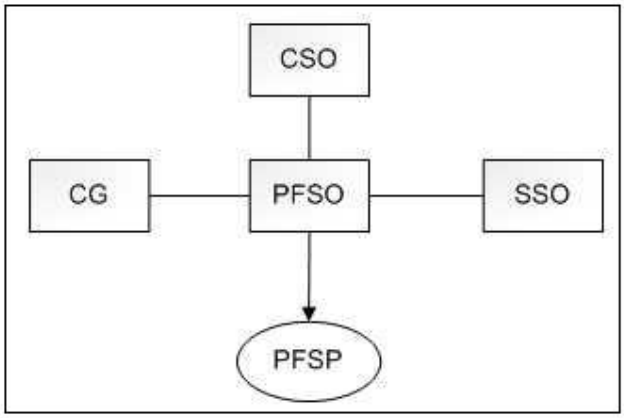


Figure 8, Port Facility Security Officer according to the ISPS code

Figure 9 concluded the port facility security procedure according to the ISPS code. The ship/port interface has not been considered in the Port Facility Security Diagram.

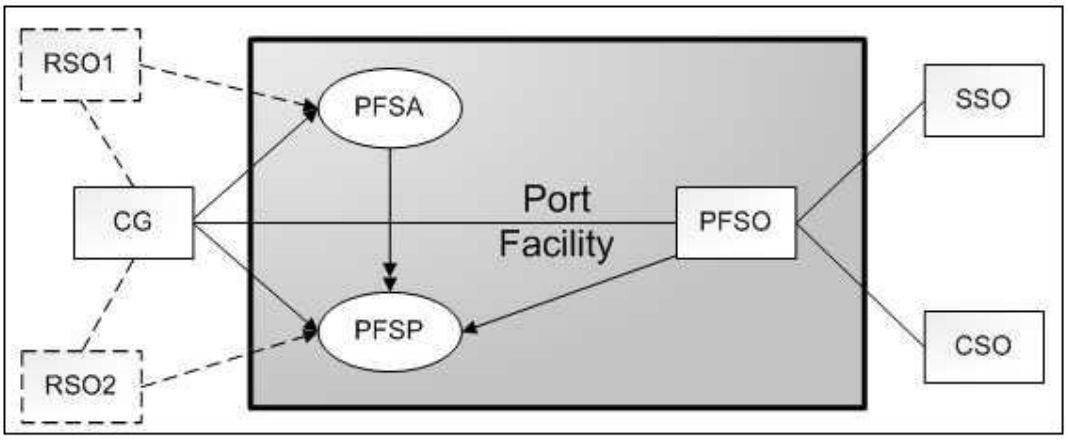


Figure 9, Port Facility Security diagram according to the ISPS code

Company Security Officer (CSO)

The person ashore, designated by the ship owner company, for ensuring that a SSA is carried out, the SSP is developed and submitted for approval, and thereafter implemented and maintained. She/he also appointed for liaison with the PFSO and the SSO.

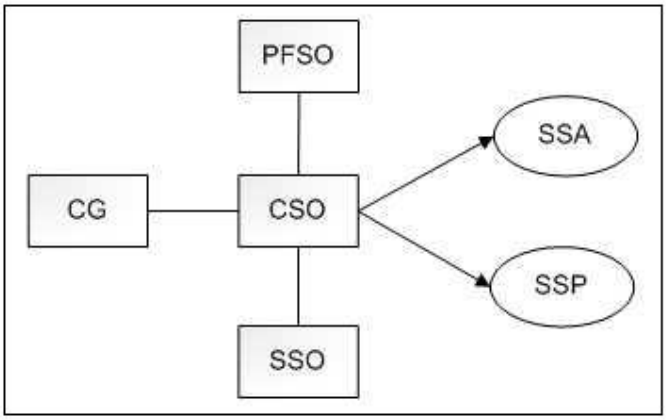


Figure 10, Company Security Officer according to the ISPS code

Security levels

Three security levels, for ship and port facility, have been defined to work in it; level 1 to 3. The Contracting Governments is responsible to set security level for port facility and also for the ship at all times.

Each level has its own specific meaning:

- Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

- Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.
- Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

When a ship wants to berth near a port facility, both the ship and the port facility must have the same level of security. Therefore, if one of them has the level of security lower than what the other has, the party who has the lower level, has to increase its level of security; otherwise the ship does not have permission to berth. The level of security of the ship will be reported to the port facility by a Declaration of Security (DOS) before entering to the port territory.

The ISPS code procedure is concluded in Figure 11 as a diagram.

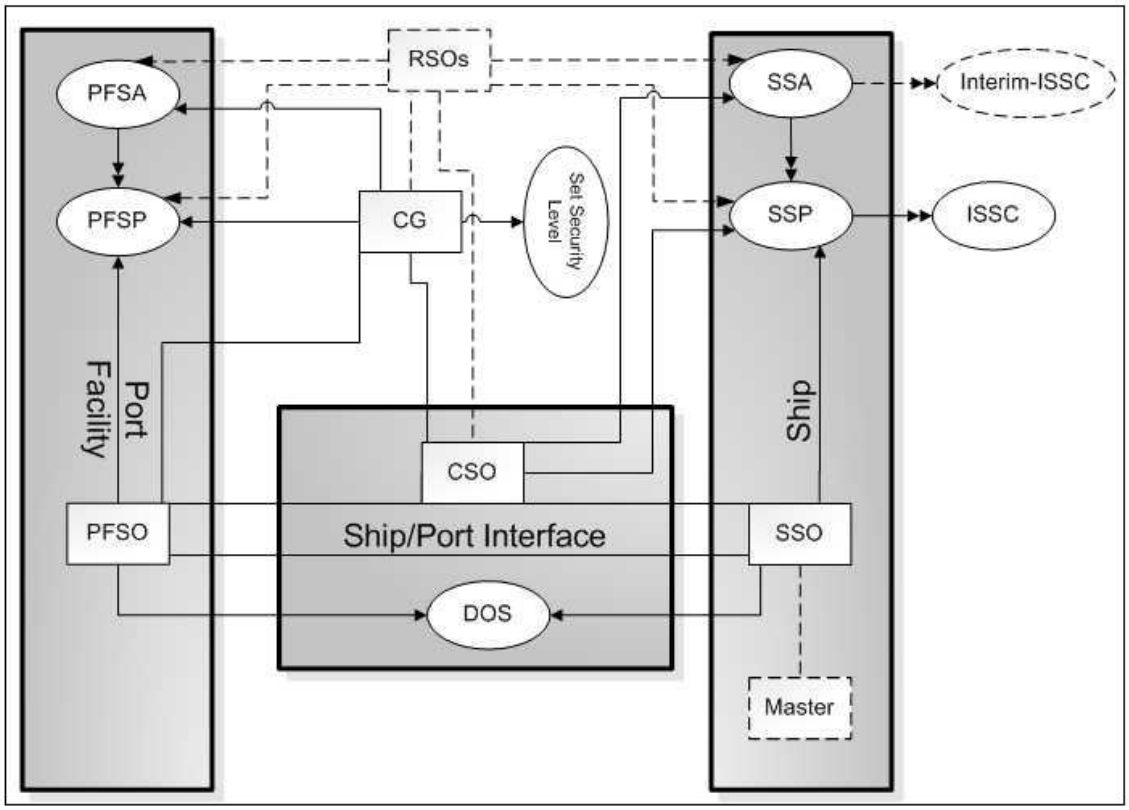


Figure 11, The ISPS code procedure diagram

2.5 Supply chain vulnerabilities

As it is mentioned in Chapter 1 (Problem statement), to have a proper survey about maritime transportation vulnerabilities, as a sub-system for supply networks, the superior-system's vulnerabilities have to be investigated as well.

According to a survey, which was done by CLSCM[1], supply chain vulnerability can be defined as "*an exposure to serious disturbance, arising from risks within the supply chain as*

[1] Center for Logistics and Supply Chain Management, School of Management, Cranfield University, UK

well as risks external to the supply chain" *(CLSCM, 2002c)*. In complementary, supply chain risk can be defined as "*any threat of interruption to the working of the supply chain*" *(CLSCM, 2003).*

The vulnerabilities of supply chain are divided into two major groups of Internal and External risks. Aftermath each is divided into sub-groups (Figure 12).

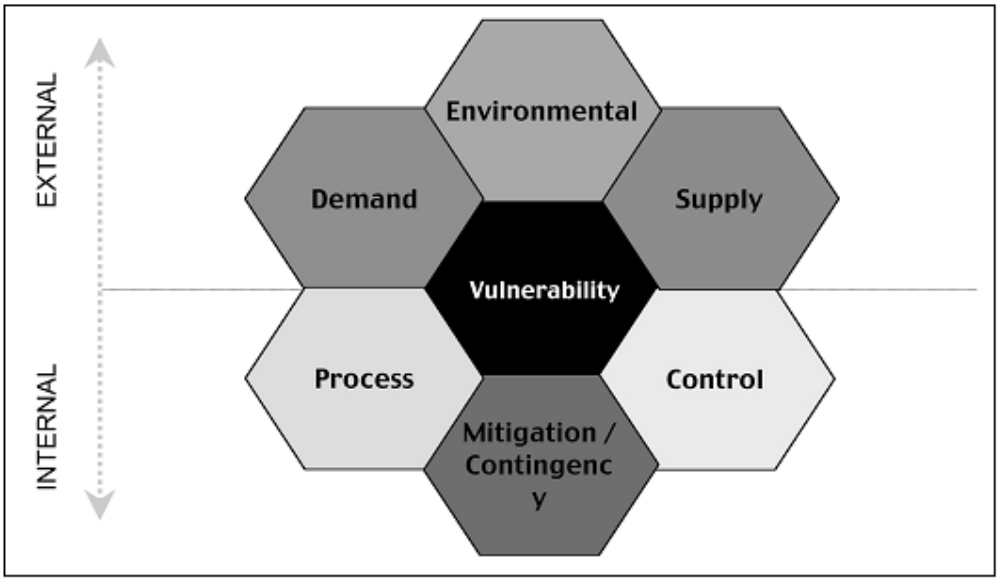


Figure 12, Supply Chain Vulnerabilities *(CLSCM, 2003)*

The external risks are those that can not be managed by the company, like any unpredictable fluctuations in demands from downstream, or any sudden disruptions in supplies from upstream. However they are categorized as external risk, they are also classified as environmental risk. "*Environmental risk is the risk associated with external and, from the company's perspective, uncontrollable events. The risks can impact the company directly or through its suppliers and customers."* (*CLSCM, 2003)*

The environmental risks are more critical for companies to consider, even as they are uncontrollable events, they comprise large variety of risk's types. They can be classified into eight groups according to their origins and from supply perspective:

1. Vehicle and route subjects like traffic, congestion, blockade and accident, which can make unexpected delay or cargo and infrastructure damages,
2. Cargo related issues like perishable or sensitive cargos in cold supply chains (medicines, food etc), or incidents related to dangerous cargos like chemicals and explosives, which lead up to cargo or infrastructure damages,
3. Human factors like strike *(CLSCM, 2003)* or unauthorized access *(Kord & Pazirandeh, 2006)*, which eventuate unexpected delay or sometimes cargo and infrastructure damages,
4. Errors *(Kord & Pazirandeh, 2006)*, including humans' or machines', which can cause unexpected delay or damage either to cargos or infrastructures,
5. Natural factors like natural disasters (earthquake, cyclone, volcanic eruption, flood etc) *(CLSCM, 2003)*, or sudden climate changes, which can make unexpected delay or cargo and infrastructure damages,

6. Communication risks as unintentional disruptions (*Kord & Pazirandeh, 2006*), which can lead up to unexpected delay or even lost,
7. Criminal threats *(CLSCM, 2003)* like theft, hijacking, sabotage, smuggling and terrorism, which can eventuate damages to cargo and infrastructure or cause unexpected delay or lost,
8. Governmental actions like taxation and regulation *(CLSCM, 2003)* that can create unsmooth business or prolongation of processes and routines, which can lead up to longer lead time and, consequently, cause delay,

Nowadays, technologies and product markets are changing rapidly and also customer expectations in terms of better products, lower prices and quicker response times are increasing (*Hallikas et al., 2002; Handfield & Nichols, 1999*). As a result, failure to manage risks efficiently has wider effects on supply chains as financial losses, reduction in product quality, damage to property and equipment, loss of reputation in the eyes of customers and suppliers, and delays in delivery time. (*Cousins et al., 2004*)

In recent decades, dependencies between companies and their suppliers have been increased *(CLSCM, 2002c)*. Some notions like Zero-Inventory[1] and Outsourcing[2] made the companies to be more dependent on their suppliers, and as a result, more vulnerable. In addition, increasing globalization and complexity of supply chains lead the companies to greater exposure to risk from political and economic events *(Harland et al., 2003).* Any disruption to supplies (or even consumes) in a country can quickly effect on entire global supply chain and global trade *(Khan & Burnes, 2007)*. An example for disruption to supply is the sharp increase in world oil prices caused by the disruption of US oil production because of hurricane Katrina *(Khan & Burnes, 2007)*; or for disruption to consume, the recent downturn in the USA housing market, which coupled with oil high price and lead to less consuming in the USA markets and spread fear of pervasive downturn in global trade.

Transportation networks are indivisible parts of supply networks and they are, metaphorically, vital limbs for supply chains' bodies. As Sheikh Saadi[3] said "*One limb impacted is sufficient for all others to feel the Mace"*, therefore every disruption in transportation would be interpreted as a vulnerability for supply chain.

Mainly the supply chain's vulnerabilities, which come from transportation side, are classified as environmental risks. In supply chain drivers' point of view, the ISPS code has come to address the threats come from environmental risks' group 7 (criminal actions) or even group 3 (human factors: unauthorized access). But, on the other hand, there is a possibility that the

[1] Zero-Inventory is a term used to describe a Just-In-Time Inventory Control system where emphasis is placed on reducing inventory to minimal levels to reduce costs and promote organizational effectiveness. This can result in sizable profit increases. (www.answers.com)

[2] Outsourcing is the transferring of the management and/or day-to-day execution of a business function to an external service provider, mainly to cut costs. If the service provider located in a country other than the one in which the client company is based, it also be called offshoring or offshore outsourcing. (Overby, 2007)

[3] Sheikh Saadi (1184 – 1283 CE) is one of the major Persian poets of the medieval period. He is recognized not only for the quality of his writing, but also for the depth of his social thought. His poem is used to grace the entrance to the *Hall of Nations* of the UN building in New York: (Translated by Iraj Bashiri)

"*Of one essence is the human race,* *thusly has creation put the base;*
One Limb impacted is sufficient, *for all others to feel the Mace.*"

ISPS code, itself, converts to other kinds of environmental risks for supply chains by its implementation in maritime transportation; like the threats that come from environmental risks' group 1 (vehicle and route issues: blockade or congestion), group 8 (governmental action: regulations) or even group 3 (human factors: strike). Therefore, the ISPS code and its implementation need to be in control to prevent of converting to potential threat. This fact proofs that "*risk and security concerns are not a one-time issue but require a continuous risk management process*." *(Harrison & Hoek, 2005)*

2.6 Port activities

The activities that a port normally does are highly dependent on port's specialty and its size. For instance, the activities that a container port will do are different from the activities of an oil port; or a small harbor might not offer some services that larger ones do. Therefore it is quite hard to say what exactly port activities are. However, in general, most of the ports normally offer some of the following services:

1- Handling, which previously were being done by porters and stevedores and nowadays they are being done mostly by cranes and forklift trucks,
2- Storing and warehousing, which are done for goods that are not immediately needed; or for some companies, who do not own enough space to store their received cargos,
3- Value adding, which mostly are done by distribution centers. They can be categorized as stuffing and stripping, assembling, packaging, labeling, testing, consolidation and deconsolidation,
4- Hinterland transportation (inter-modal), which is done by pipelines, trucks, trains, or even vessels for short sea distances,
5- Maritime services like pilots, tugboats, boatmen, vessel traffic control,
6- Other services like foodstuff preparation, power supplying, ship repairing, recycling and oil refinery,

The ISPS code might have positive or negative impacts on these services in ports by its implementation. However these services were quite detailed activities and studying the code's impacts on them were out of the scope of the thesis. Instead, the impacts of the code on some other more general aspects, which also are affected by mentioned activities, are studied. These general factors that have been the subject of analysis in this thesis include manning, lead time, service level, checking process, effectiveness and efficiency. These factors have been chosen by considering supply chain's key factors too. It means that the factors that this thesis will try to find the impacts of the code on them, have been chosen from both port's activities' and supply chain's perspectives.

3. Review of the state of the art

Since the ISPS code is a fairly new rule and less than four years has passed from the date that it came into force (July 2004), only a few surveys about its impact have been conducted. Although there have been some efforts to find the effects of the code on different segments of industry and global business, but there are almost no exact similar works which had been done on the impacts of the ISPS code on port and port activities. Most of the works have been done to find if the ISPS code was effective to address maritime security threats or not. Other studies in this area are about the impacts of the code on ship owners, seafarers, stakeholders, cargo owners and other parties who are working in seaborne transportation.

Two significant similar studies, which have been done to reveal the impacts of the code in port's area, are UNCTAD's (United Nations Conference on Trade and Development) report about the cost and related financing of the implementation of the ISPS code over all regions; and a survey by Mattias Wengelin about the ISPS code performance in Swedish ports.

3.1 UNCTAD study

UNCTAD's survey is a global study to find the ISPS code financing impacts and level of compliance on all affected parties. It was published on March 14th, 2007 but the survey included the ISPS Code related expenditures made from 2003 through 2005.

In spite of UNCTAD's expectation to have a global collaboration, the number of received responses was limited to ports and governments only. The UNCTAD's work is comparable with this study not only because it has been done on ports (though it is limited to financial effects), but also because they have used similar way to this survey's to collect the first hand information and have used same method to analyze data.

They prepared questionnaires and distributed them. They have received 55 completed questionnaires from the ports located in 28 countries which their majority (62%) located in developed countries, while 82% of respondent ports located in Asia and Europe. The respondent ports handle about 16% of the global port cargo throughput (MT)[1] based on 2004 world seaborne trade figures, and approximately 24% of the global container port throughput (TEU)[2]. The size variations of respondent ports are 46% large, 11% average sized and 43% small.[3]

According to their study, the financial effect of the code was substantially higher for smaller ports in point of related average cost view (*UNCTAD, 2007*). It seems that the bigger ports were more compatible with the ISPS code requirements, therefore their initial cost for equipments, infrastructures and etc were less in comparison with smaller ports'. In addition, calculations of the estimated global port-related cost for implementation of the ISPS code are equivalent to increases in international maritime freight payments of about 1% with respect to the initial expenditure and 0.5% with respect to the annual expenditure (*UNCTAD, 2007*).

The impacts of the ISPS code on different factors in a port, according to UNCTAD's (2007) report, are illustrated in Chart 1.

[1] Metric Tonne

[2] Twenty-Feet Equivalent Units

[3] "A small port authority handles few million tonnes, an average sized authority handles between 10 and 20 million tonnes and larger ports handle over 20 million tonnes." (Fourgeau, 2000)

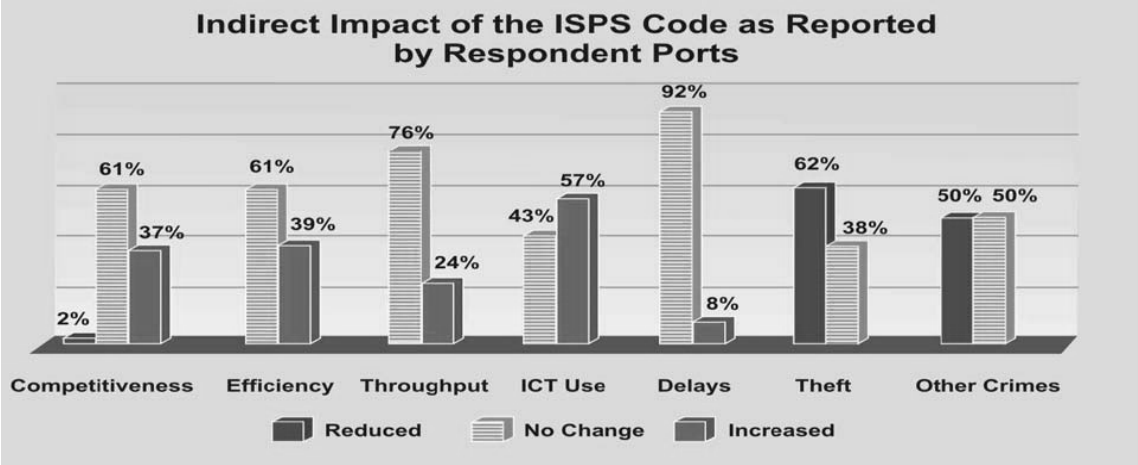


Chart 1, Indirect impact of the ISPS code *(UNCTAD, 2007)*

As seen, except in theft and ICT (Information and Communication Technology) usage, the majority of the respondent ports came up with this opinion that the ISPS code has had no specific indirect impact in their activities. But the overall impact of the ISPS code on ports has another story (Chart 2). The common idea (64%) about the overall impact of the code shows that it has had positive impact on ports and port activities; 24% of respondent ports have believed that the ISPS code has had negative impacts on their activities, while only 12% of the participants have told that it has had limited effect on their activities.

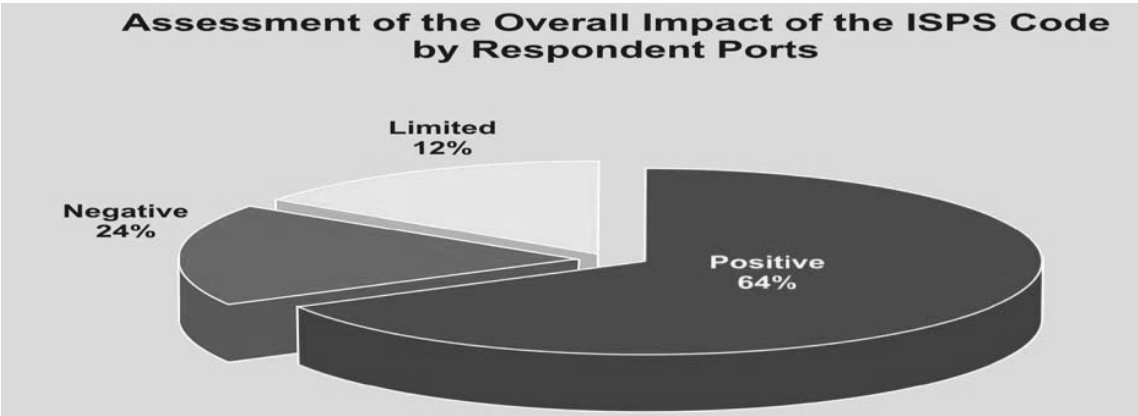


Chart 2, Assessment of the Overall Impact of the ISPS code *(UNCTAD, 2007)*

The UNCTAD secretary reports that *"the ports seem to have accepted the ISPS code objectives as legitimate and reported an overall positive impression of the new security regime, especially in terms of increasing awareness, streamlining processes, standardizing risk assessment and improving business practices"*. (*UNCTAD, 2007*)

3.2 Wengelin study

Wengelin's assessment is based on interviews with PFSOs from six different Swedish ports varying in size and geographical location and participatory observations in a port during two weeks. He also used the official sights and opinions of the Swedish Maritime Authority, the Swedish Customs, the Swedish Coast Guard and of the police department of Skåne province.

His work is comparable with this study because, except the size, they both used similar sample population. It was done according to Swedish ports' experiences with the ISPS code.

The original work was published in Swedish language by Lund University namely "Fångad i Nätet" (Catch in the Net) on May 2005. Wengelin has used the results to write an English paper by the title of "The Swedish Port Security Network – An Illusion or a Fact?" which was published by Journal of Homeland Security and Emergency Management on 2006. This specific paper was the source, in this thesis, to cognize the results of the original report.

The main goal of the paper was to find if the parties, who are in charge of security for Swedish ports, are working together properly as a network or not. Even though, the code's impacts on Swedish ports have been outlined briefly, but it has not been discussed deeply to find the direct and exact impacts of the code in Swedish ports.

Wengelin has described a typical Swedish port before and after ISPS code implementation. As most of the Swedish ports are part of urban areas, previously they were a place for entertainment beside a place for trade. Before the ISPS code execution, the port areas in Sweden were open to the public. There were no fences and gates; people could pass through it easily, use the shore for fishing and flying kites and maybe buy something from the seafarers. After the code implementation they all vanished. Now fences, gates and CCTVs are telling that the previous free atmosphere is a history.

He mentioned that the ISPS code has come to protect some parts of the world from the effects of their own foreign policies. Even though, he has not directly mentioned which parts of the world he has meant, it is clear that the US and the UK are some of them. Then he raised this idea that as a result the Sweden is protecting the US from the effects of its foreign policies by implementing ISPS code in Swedish territories.

In other part of the paper, while he was citing from a PFSO, it has been said that the ISPS code could not be a protection against terrorist attacks. "*It's pretty easy to break through a fence, or by using weapons as they do in other places in the world, then we don't have much to say…*" (*Wengelin, 2006*)

Since the Swedish mentality is quite unfamiliar with terrorism (because of Sweden's foreign policies during the past couple of centuries), the interviews lead Wengelin to find that the ISPS code are accepted by Swedish actors in some ways that have nothing in common with its initial objectives, which was related to security; like decreasing in the number of petty thefts and in the number of people walking around the port equipments.

At the end, Wengelin has concluded his work by posing a question.

> "*What effect does this attitude have on the actual risk for the port or the risk of being used as an entrance point for transiting an antagonistic threat through the maritime transportation system? It is definitely a weakness not being able to effectively gather the efforts for securing maritime transports if viewed from the perspective that initiated the development of the code. It could also be a sufficient adaptation to local preconditions and a logical construction of rationality, creating meaning for actions to be taken. Rules and regulations do not travel well over time and space. The original triggering event loses its strength and importance the further you get in time and in space. What is left is to construct local reasons available to create meaning, whatever they are. Another approach is to question the globalization of rules and regulations to suit one actor on the global arena. Now, having defined the problem, the questions still remain largely unanswered.*" (*Wengelin, 2006*)

3.3 Some other studies

There are some other surveys on the impacts of the ISPS code in seaborne parties, which are not closely related to this survey; as they are focused mostly on other parties in maritime transportation than ports or their studies were just a brief discussion about the ISPS code impacts and not a full research on it. Some of them have been cited here by way of illustration.

1- A short survey has been done by *International Transport Intermediaries Club* (ITIC) as an organizational circular for their members' information to find the impacts of ISPS code on members of ITIC. This circular has just talked about the duties of the involved parties for applying the ISPS code. It seems that they wanted to define the responsibilities of their customers to clarify that the ITIC will not be in charge in case of any failure from mentioned duties. At the end, it is mentioned that further effects of the ISPS code are unknown and it is impossible to find the impacts of ISPS code at this stage. The exact date of this circular was unknown but it seems that it has been done shortly after or before July 2004.

2- The other work, which is a newsletter, has been written by the *Charterers P&I Club (2004a)* on November 2004 and described the possible effects of the ISPS code on the Charterers. It has been indicated that the ISPS code brings more responsibility for involved parties and also more works that have to be done by them. It is cleared that all of these jobs need more time and more administration works to be managed. It has been said that the ISPS code forces Charterers to carry out additional documentation, advance informing of arrival, manifest of cargos and passenger list etc, all of which waste time and money for the Charterers. The Charterers will indemnify by applying higher cost on their services, which results in the customer paying extra fees. Overall, it has been said that the most significant impact of the ISPS code on the Charterers is the effect on financial part, and the Charterers are suffering from this part more than increasing in their responsibilities.

3- An article about the impact of the ISPS code on Australian ship-owners has been written by *Trever Griffett*, for a meeting for the Australian Ship-owner association on April 2005. He mentioned that the new wave of action, which was started after 9/11, has root in shipping history. It means the war on terror in shape of new security rules for maritime is not new and more or less existed previously. Its name was anti-theft or anti-piracy. He has mentioned that the ship-owner's concerns about security matter are slightly different from governments' perceptive. The ship-owners, want to protect the ship and its crews as well as the cargo, which is located in the ship for the time being. The governments want to protect the environment and the area where the ship is located and defend against any dangers that might occur because of the ship's location. Griffett categorized the impacts of the ISPS code in four categories: 1- Duplication of documentation 2- Additional layer of bureaucracy 3- Disruption of treatment between crews and 4- Unjustified panic by media and academia

4- The next article is about the impacts of the ISPS code, which was written in the 48th IFSMA (International Federation of Shipmasters' Associations) newsletter in December 2005, which is a report from Canadian Ship Master's conference in Halifax in September 2005. In this report, the impacts of the ISPS code on ships, ports, seafarers and shipping companies was discussed briefly. Mostly, it talked about the impacts on seafarers and the effect of the new rule on their sea lives. The article uses evidence found in a paper by *Douglas B. Stevenson* named "*Effects of ISPS Code on Seafarers*". Stevenson mentioned two major negative effects that the Center for

Seafarers' Rights (CSR) has founded regarding the security rules in maritime. They are seafarers' denial of shore leaves and chaplain's access to the vessel. The article hints the most of the problems for seafarers are caused by some ports that are following the words of the ISPS and not its spirit (*Stevenson, 2005*). Take into consideration that most of these similar problems are happening because of the different interpretation of the ISPS code. Each port or security agency perceives the code in its own ways. The paper's author believes that a source of these kinds of problems is a misinterpretation of the code. In addition, he believes that the cost of the ISPS code implementation is a major source of problems. The question always remains who is going to pay the cost of this or that?

5- The other one is an article by *Fiona McNaught*, on the ISPS code effectiveness in addressing maritime threats which is published on GEDDES papers, 2005. She emphasized on this point that the ISPS provisions relating to port facilities relate only to the ship/port interface; and part B of the code has just addressed the security issues for ships while she is alongside the port and it has not considered the threats which may be posed by ships to port facilities. She has also mentioned that one of the ISPS weaknesses is its limitations for some sorts of vessels, which can be used by terrorist groups for their goals; like pleasure boats. According to her, the different interpretation of the code in different countries is one of the ISPS code weaknesses. In addition, she believes that the other barrier for ISPS code to be an effective regulation is the Seafarers Identity Documentation (SID) or Maritime Security Identification Card (MSIC), which have not come into force yet and they will not in the near future; because of some differing opinions that are existed in this matter. Furthermore, McNaught believes that there is still problem for providing the cost to apply the code, but she thinks that the saving which can come from avoiding of cargo stealing can retrieve those costs.

6- The last one is an impact assessment of the ISPS code, by *Alexandros M. Goulielmos* and *Agisilaos A. Anastasakos*, which has been written as a paper namely "Worldwide security measures for shipping, seafarers and ports"; and has been published on Journal of Disaster Prevention and Management on 2005. Two main concerns of this paper are about the ISPS code standpoint in relation to seafarers with its consequences and about local regulations, which have been come into force contemporaneous with the ISPS. The regional rules, like the EU regulations to enhance maritime security or the US requirements for ship calling in the US ports, have been defined to reinforce effectiveness of the code at specific regions. It is indicated that a vessel operator, who followed a fixed schedule, needs to know the expected extent delays and added operating procedures and costs in advance to plan accordingly. However, these local rules can have negative effects for the global fleet working by those areas, mainly the US ports.

4. Methodological framework

In this chapter the methods which have been used to get results for the thesis, have been discussed. Also the methods to gain the primary and secondary information beside the analyzing method have been clarified. The data validation and its reliability have been challenged as well.

4.1 Research procedure

The results, which have been presented in this thesis, were gained by both theoretical and empirical works. In addition, in terms of theory of sciences, the research procedure used in this thesis is both inductive and deductive. It could be argued that the research question, which has been defined by the thesis supervisor, has come out in a deductive perspective and the answer was obtained in an inductive view.

It is supposed that all regulations, because of their inherent limitations, will affect the parties who are obeying the rules, in many ways. Therefore it is premised, as the ISPS code is a regulation that its implementation is mandatory for all ports, which their governments are IMO members, it should affects port activities in some ways. To find the answer of the thesis questions and also the proofs or denials of the above hypothesize, the literatures studies were done. The ISPS code and its related parts at SOLAS were fully read to find the possible problematic parts, which could affect the maritime transportation, especially ports. The similar surveys about the impacts of the ISPS code in all involved parties were reviewed thereafter. Besides, three interviews with experts in maritime security were done to confirm the author's findings. Afterwards, a questionnaire[1] was prepared, which comprised questions about the possible effects that the ISPS code may had.

4.1.1 Data collection method

A common way to divide the sources of information is to divide them into two groups of data, primary and secondary (*Ekwall, 2007*). The primary data is that one which will be collected directly by the researcher (Interview, questionnaire, observation etc), and the secondary one will be gained by reviewing others' works (Book, paper, report etc). (*Ekwall, 2007*)

Primary data, in this study, was collected by electronic questionnaires which had been distributed among the involved parties in implementation of the ISPS code. The secondary data, which was used to prepare the questionnaire and also to compare and validate the thesis results, was gained by reviewing the books, reports, papers and also by browsing internet, in related subjects.

4.1.2 Analysis method

The most common analytical method to analyze data, is to convert the raw data to quantitative data and then compare them to each other by drawing charts, figures etc. Thereafter, by an analytical vision, the drawn charts show (by its own or by comparing with other similar results from much the same studies) what the raw data indicated. It is the method which has been used for analyzing in this thesis.

[1] Appendix 1: *Questionnaire*

4.2 Survey and interviews

After preparing the questionnaire and confirming it with supervisor and some other experts in port security, the electronic questionnaires were sent to email address of persons, who were in charge of the ISPS code in their ports; like PFSOs or security managers. Before sending the questionnaires, they were informed, via phone, about the survey and its objectives and also were asked to give permission to the interviewer to send the questionnaire to their email addresses. The persons that did not like to answer the questions never received the questionnaire.

They had been requested to answer the questionnaires within two weeks. Where the answer would not be received within the given time, the interviewee would be re-emailed or re-called to be asked again to answer. If the answer would not be received despite of all these efforts, aftermath the port would be deleted from the study's sample population.

Three interviews with experts in port security were done by the author, directly in meetings, before the questionnaire were prepared. These interviews helped the author to well prepare the questionnaire and also to get better result from the questionnaires. The interviewees were not asked by the questions in the questionnaire. The topics of the conversations were the ISPS code, the EU regulation 2004/725/EC *(2004b)*, the EU directive 2005/65/EC *(2005a)* and their impacts on ports, especially EU ports with focus on Swedish ports.

4.3 Profile of respondent ports

The respondent ports[1] were varying in both sizes and their geographical locations.

4.3.1 Geographical locations

The locations of the respondent ports are shown in the figure below (Figure 13). They were mostly from southern regions of Sweden. It is noteworthy to mention most of the Swedish ports are located on south of Sweden.

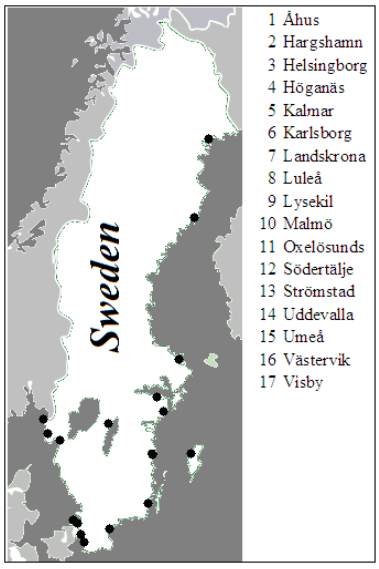


Figure 13, Respondent Ports Dispersion

[1] Appendix 2: *The cooperator companies*

4.3.2 Size variations

The smallest respondent port had the size of less than 300,000 MT cargo handled in 2006, and the biggest respondent port had the size of more than 9,000,000 MT cargo handled in 2006.[1]

It should be mentioned that all the respondent ports would be categorized as small ports, according to Fourgeau[2]. However it should be borne in mind that Sweden does have only one large sized port and just two average sized ports.

4.4 Data sources and their reliabilities

The validity and reliability of each research depends on how much the sources, which have been used to gain information, are reliable (*Ekwall, 2007*).

The secondary data in this thesis was used to define the probable problems that the code may cause and then preparing a questionnaire according to them. All of the sources to gain secondary data were published-materials like international rules or research papers, which surely have been checked before publication by experts. They have been sorted in "References".

The primary data has been collected by a quite long questionnaire[3] with more than 40 single questions (more than 60 nested questions). Because of the number of questions, the questionnaire was prepared in multiple-choice form to make the interviewees' work easy to answer. Besides, an opportunity was considered for some interviewees who want to add more information by considering a *Comment* part. At the end, the questions that were hard to ask in multiple-choice way were added as normal questions; but answering them was not emphasized, though it was requested. Since few answers were collected from those questions, they did not analyze; although they were used to get clear ideas during the analyzing process and concluding the results.

The reliability of the primary data could not be questioned as the interviewees had an option to do not answer each question that they did not want to. In addition, they were promised to remain anonymous. Thus they answered questions willingly while they felt safe, which is an important factor to have a reliable data collection (*Ekwall, 2007*). Besides, they had quite long time (no actual time limit) to answer the questionnaire, which is another factor to have reliable data collection process (*Ekwall, 2007*). Furthermore, all of the interviewees were the expert persons in maritime transportation, who also were in charge about the ISPS code in their ports. Thereupon, they had broad view about implementation of the code. It should be of course borne in mind that the ISPS code is being carried out since July 1st 2004, so nobody has more than 4 years experience to deal with.

4.5 Verification and validation of results

After calling more than 50 ports to talk about the study and get permission to send the questionnaire, 42 of them agreed to receive the questionnaire. Despite of all efforts and correspondence, just 18 ports[4] (43% of called ports) replied to the request and sent the

[1] Refer to table 2 of statistics (Cargo statistics of Swedish ports) in www.transportgruppen.se

[2] "A small port authority handles few million tonnes, an average sized authority handles between 10 and 20 million tonnes and larger ports handle over 20 million tonnes." (Fourgeau, 2000)

[3] Appendix 1: *Questionnaire*

[4] Appendix 2: *The cooperator companies*

completed questionnaires, however the accuracy of the study has been defined as 25%. This number came from the port weighting according to their sizes, which were defined regarding their cargo handled tonnage in 2006.

The total number of Swedish ports with commercial traffic is 52 harbors (*Sveriges Hamnar, 2007*). The total value for these ports, according to their sizes, is 96. Since 4 ports from among the 10 biggest Swedish ports (*Sveriges Hamnar, 2007)* were part of our sample population and answered our questionnaire (although all of them were called), so the total value of respondent ports was 24. Hence, the accuracy of 25% has been gained by this study.

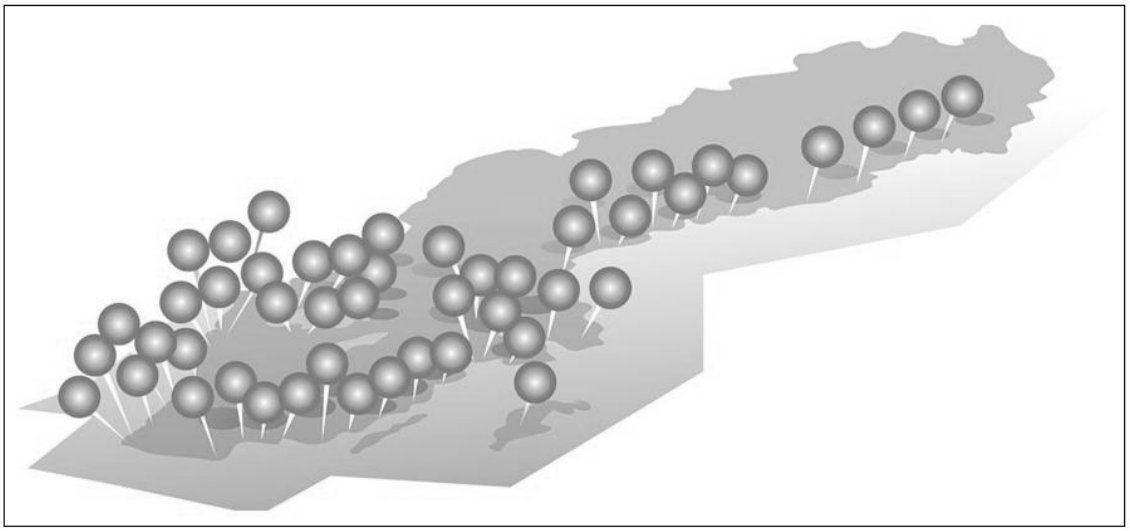


Figure 14, Dispersion of Swedish ports with commercial traffic (*Sveriges Hamnar, 2007*)

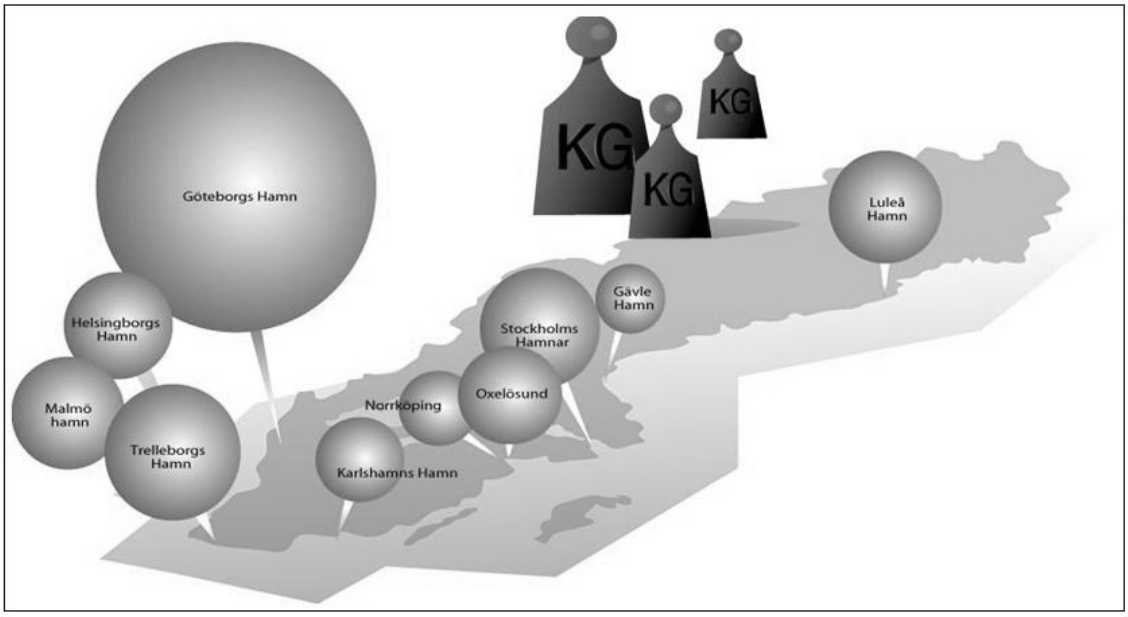


Figure 15, Largest Swedish ports (*Sveriges Hamnar, 2007)*

It is assumed that the size of the port would affect the port experience about the ISPS code, which is not wrong either. As each port which has bigger size, has handled more cargo and

served more ships in an equal time interval, then it has challenged the code more. Therefore, the author's assumption is acceptable.

The results have been analyzed in two ways, one with consideration of the port's values and the other without them. These results have been compared with each other in case of noticeable differences.

5. Results

In this part, the data has been analyzed according to the quantification of the answers. The answers have been analyzed in two ways; one with consideration of the value of the ports and one without it. In the case of significant differences, the results are compared to find the reasons; otherwise the shown results are represented without considering the ports' values. It is proper to mention that all the indicated percentages in this chapter, which are based on our study, are percentages of respondent ports (any exception would be noted).

5.1 Implementation difficulties

The ISPS code implementation had and has some difficulties for the parties who are engaged; some problems like expenditures, time, different perspectives etc. In this part the viewpoint of respondent ports about these subject matters have been expressed and discussed.

5.1.1 Initial costs

In question 3, the cooperator ports were asked about their level of compatibility with the ISPS code before its implementation, to find out how much work they needed to do to meet the code's requirements. As it is shown in Chart 3, the compatibility level is dependent on the port's size. The result, without weighting the answers, shows that 38% of the respondent ports were 30-50% prepared with the code's requirements. But when the ports' values were considered, the result has been changed. About 52% of the respondent ports were 50-70% matched with the code's requirements before its implementation.

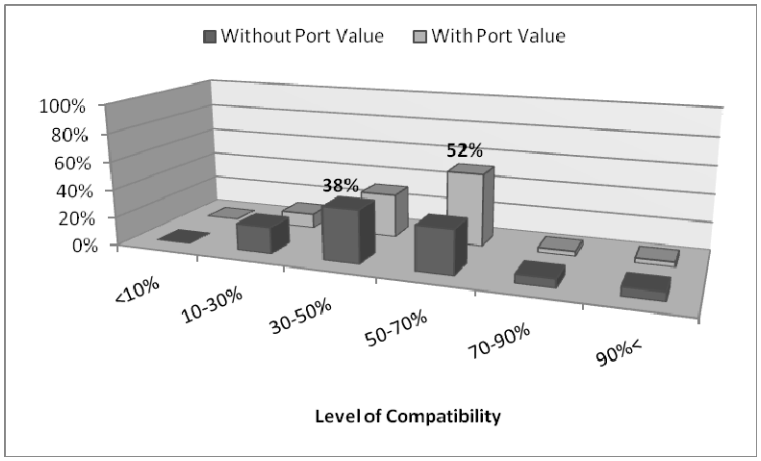


Chart 3, The percentages of ports' compatibility with the ISPS code

It comes from this fact that the larger ports had previously more problem about the security matters, as they handle more cargos and deal with more ships. Therefore, they prepared more security equipments and trained more personnel regarding to security matters, to cope with possible problems. Consequently, they were more compatible with the code requirements before its adopting. On the other hand *"the ISPS code is, in many ways, a structured summary of many routines and instructions in force on a daily basis from other authorities…" (An interviewee)*

It also shows that the smaller ports had to investigate and do more to apply the code, while they serve fewer ships and handle fewer cargos than what the larger ports do. Therefore, their unit cost (cost per cargo unit) would be higher than what the larger ports would have. As a result, the smaller ports will suffer more to cope with the initial cost of the code. This is similar to the result that UNCTAD (2007) has mentioned in its report (Chart 4&Chart 6):

> *"The unit cost analysis revealed the presence of important cost differentials between respondent ports, especially between larger and smaller ports. In other words, relative costs appear to be substantially higher for smaller respondent ports." (UNCTAD, 2007)*

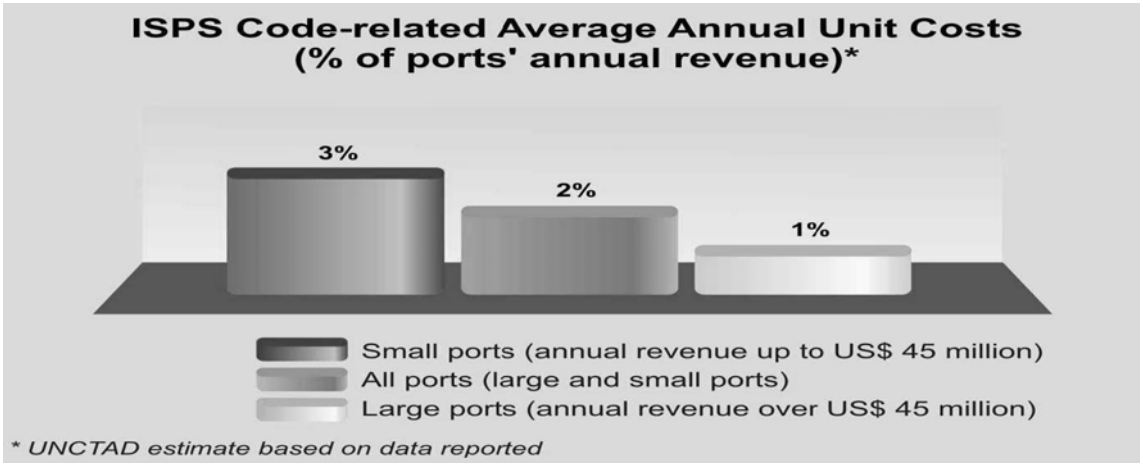


Chart 4, ISPS code-related average unit costs based on ports' annual revenue *(UNCTAD, 2007)*

> *"The above results suggest that the ISPS code-related financial impact is more pronounced in the case of smaller ports." (UNCTAD, 2007)*

This is the result that has been replicated while UNCTAD (2007) uses different reference points like *tonne of cargo throughput*, *TEU throughput*, *ISPS port facility* or *even ship calls.*

Furthermore, this fact that applying the ISPS code had more financial impacts on smaller ports rather than larger ones would be highlighted if the ports be compared in point of break even situation based on port's size.

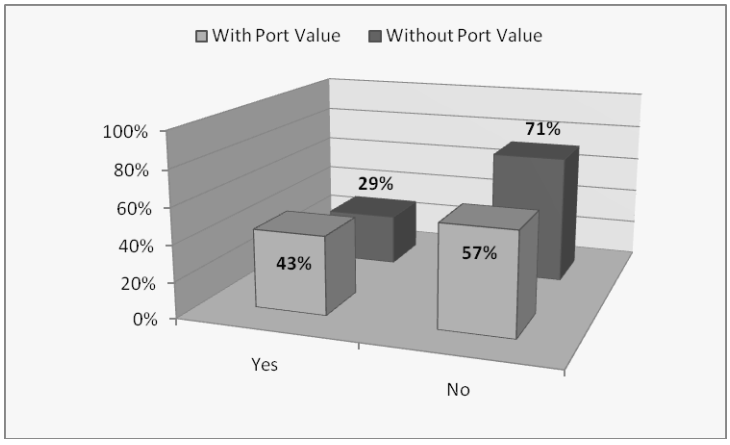


Chart 5, Reach to break even point

As it is seen (Chart 5), an important majority of respondent ports (71%) have not broken even yet. This number will change if the port size takes into account. In this condition, an important minority of the respondent ports (43%) have reached to the break even point. It shows that larger ports were more successful to break even than the smaller ones. As the break even point is the comparison between investment and payback, it could be understood that either larger ports invested less than what the smaller ports did (regarding their annual revenue), which is supported by UNCTAD (2007) result (Chart 6); or larger ports had more cargo turnover then it was easier for them to compensate their initial costs.

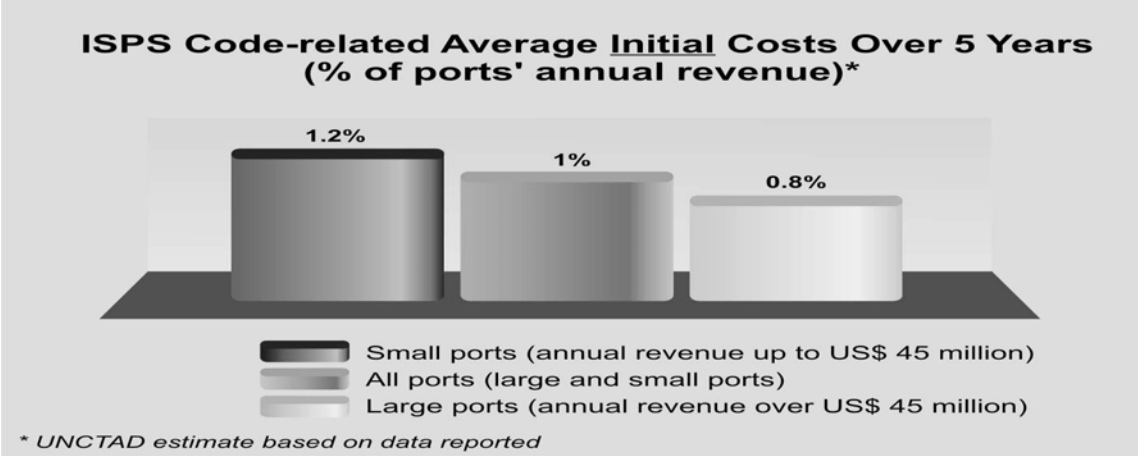


Chart 6, ISPS code average initial costs regarding to % of their annual revenues *(UNCTAD, 2007)*

The main initial costs for implementing the code were invested to provide the security equipments (Chart 7) like fences, gates and security systems; which in some cases were nearly tens million SEK.

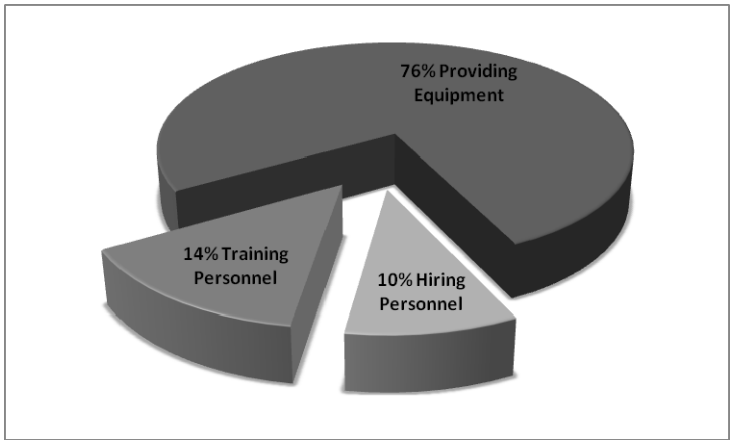


Chart 7, Main cost for applying the ISPS code

To put this result in perspective, once more it can be compared with UNCTAD's (2007) report. According to its report (Chart 8), expenditures on equipment and infrastructure absorb the largest share of the initial costs in the ISPS port facilities.

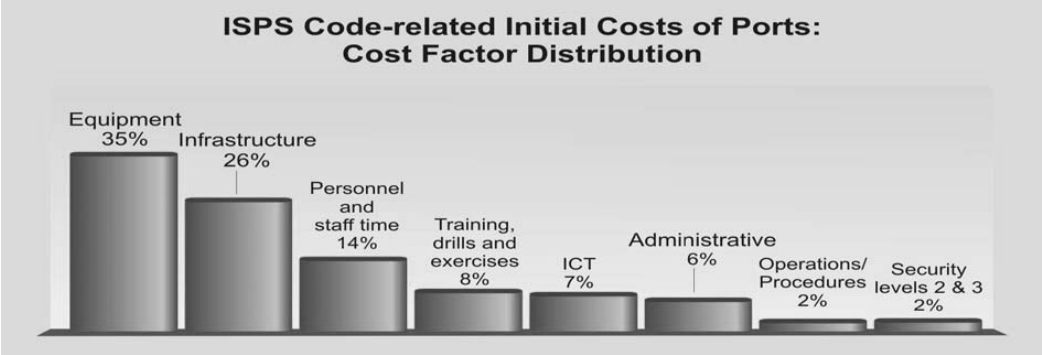


Chart 8, Main cost for applying the ISPS code based on UNCTAD report *(UNCTAD, 2007)*

It should be mentioned that in all asked ports, all the cost were provided by port authority and they did not get any addition subsidization. It is very clear that it will take quite long time for some small ports to break even initial investment without any further subsidization. It should also be brought up that some small ports can not offset their investments by saving that might be gained from raising security in their territories[1]. As one of the interviewees has answered to the question about reaching to the break even point:

> *"Will never do, since we are only a … [small] port" (An interviewee)*

5.1.2 Other costs

As it is mentioned earlier, the security level of a ship and port facility shall be at the same level while she wants to moor in a port. If the security level of either the ship or port facility be higher than what the other has, the party who has the lower level of security must increase its level. Since increasing security level is costly for ports[2] then responsibilities for its costs are really a matter for port facilities. According to the results (Chart 9), seems there is no predefined rule to impel a party to pay these costs. Therefore, it is negotiable or depends on who are more interested to conduct business with whom; if the ship is really eager to moor in specific port then the port facility holds the aces or vice versa. Thereupon, it can be a winning factor for port facilities in global commercial competition; bearing in mind it is not a situation that occurs frequently.

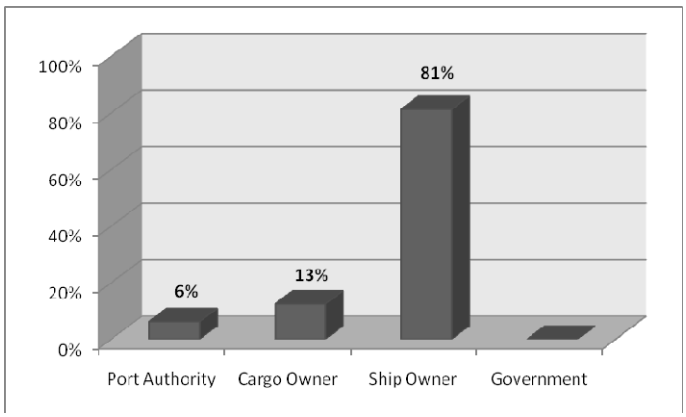


Chart 9, Cost payer of increasing security in a ship when its level is lower than what the port has

[1] Refer to McNaught's opinion (Review of the state of the art, p.25)

[2] Increasing security level in a ship imposes extra works, rather than cost, to seafarers and it could not be a cost matter in a ship

5.1.3 Time window

The other possible problem that the ports were asked regarding to the ISPS code implementation was about time that they had, to meet the code requirements. Chart 10 shows how much the ports had problems to apply the code in their territories from time point of view. The overwhelming majority of the respondent ports (89%) had problems, as the time gap between adopting the code and its implementing was not quite enough.

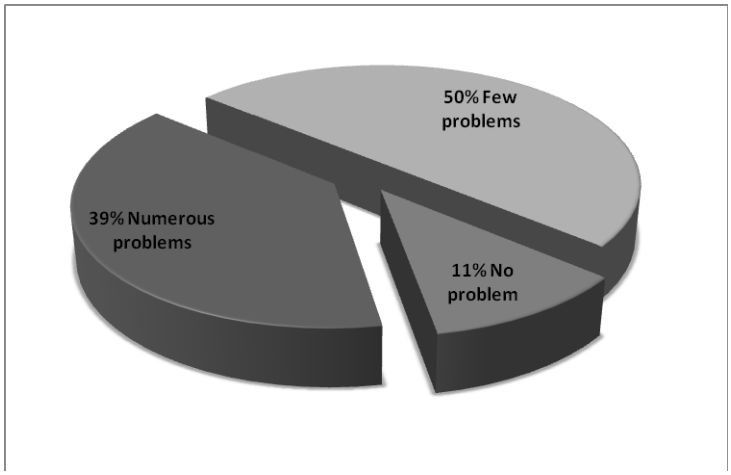


Chart 10, Time problem to apply the ISPS code

Some ports were also disappointed from in charge authorities who did not give clear directives and information about the code implementation. It could have happened because the responsible authorities themselves were not fully aware about the code requirements; which is another consequence of being in haste to apply the code.

5.1.4 Human rights

One of the main concerns about the ISPS code is about its effects on seafarers' life and some acts against human rights, such as preventing shore leave. However, it seems that this concern is not underlined in Sweden, which can be rooted in Swedish culture.

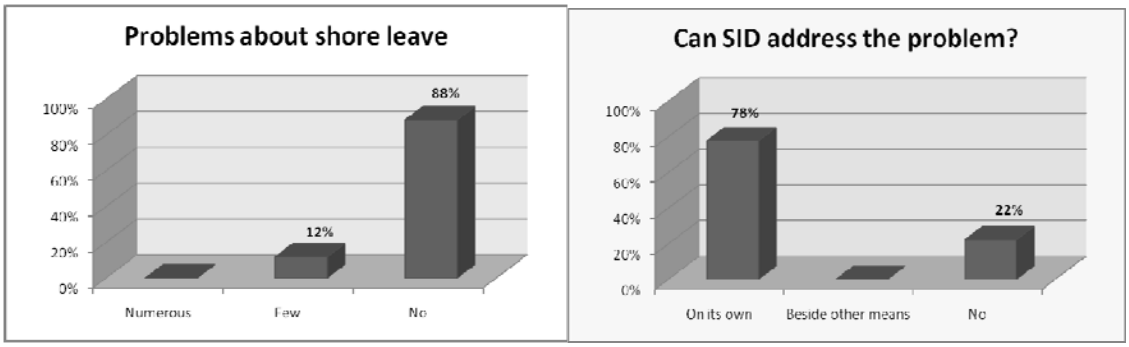


Chart 11, Shore leave problem and its solution

As it is shown in Chart 11 and Chart 12, most of the respondent ports have proclaimed that they did not have any problem about such matters. Moreover, nearly 80% of them believe that

issuing an international identity document like SID can address any possible problems related to seafarers. It should be stated that all of the ports that reported some problems about this matter declared that SID could solve it.

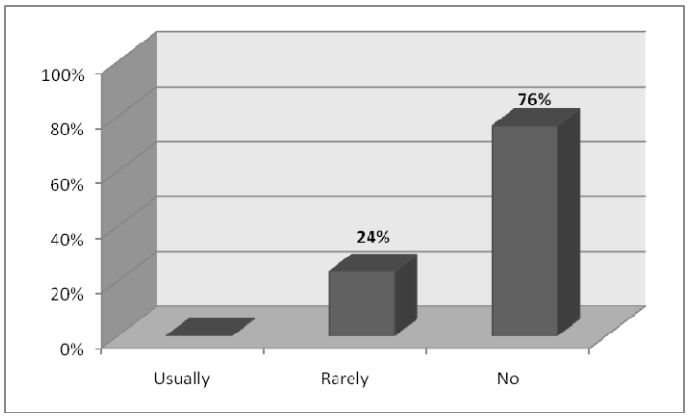


Chart 12, Problem about security checking which may cause an action against human rights

Furthermore, it could be possible that ports charge seafarers or chaplains for shore leave or ship access. Even though all the respondent ports declare that they do not charge mariners extra to give them such permission, it is possible that some of them included its fee on their tariffs; since 31% of the ports have increased their service prices (Chart 18). Albeit it is not a major issue in Swedish ports and it can also be used as another winning factor for them in global commercial competition.

5.1.5 Different interpretation

According to one of the interviewed security experts, different interpretation of the ISPS code in different regions of the world could be a major problem of implementation of the code[1]. For instance, in Denmark the border of the protected area by the code is defined by just yellow lines, while in its neighbor, Sweden, it is defined by fences. It has been tried to address these problems in EU states by delegating it to security professionals from different EU countries, who are designated to inspect port facilities in EU regions to have a concordant ISPS code region. However, this problem still remains in other sections of the world. Chart 13 shows that the Swedish ports are not really involved with this problem.

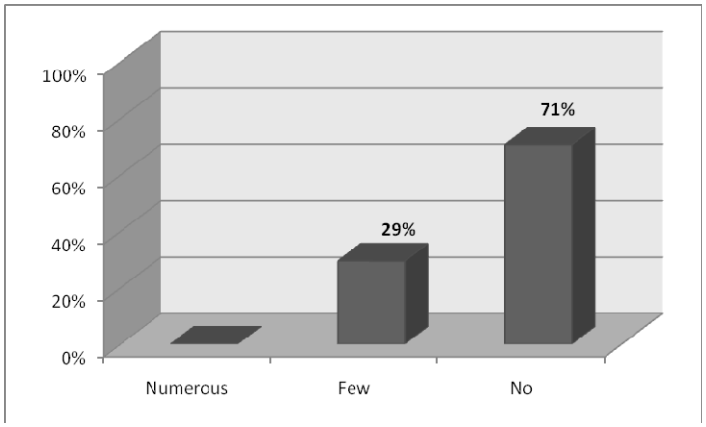


Chart 13, Problem because of different interpretation of the ISPS code

[1] Fiona McNaught (2005) has same idea in this matter. (Refer to 3.3Some other studies, p.25)

5.1.6 Bad-trained officers

The other problem, which might be existed within the ISPS code implementation, is the security officers (SSO, PFSO or CSO) who have not been trained well. According to the ISPS code, the security officers must be trained to be able to handle all the duties that would be delegated to them[1]. Therefore, logically, such problems about bad-trained officers should not be existed at all. However, if we want to have a rational judge, we have to admit that there are some companies that are not too enthusiastic to control these matters seriously. Consequently, these may cause some problems due to untrained security officers, who do not know much about the ISPS code and its implementation. Therefore, it was asked from the collaborator ports to find if there were any problems in Sweden with this regard.

According to Chart 14, again, it is not a really important hitch in Swedish harbors; even though, an interviewee was really disappointed about untrained SSOs, who visited their port:

> *"I have most experience with untrained SSOs. Some do not know much about the rules. Depends largely on the attitude of the Flag State and also of the company…"*

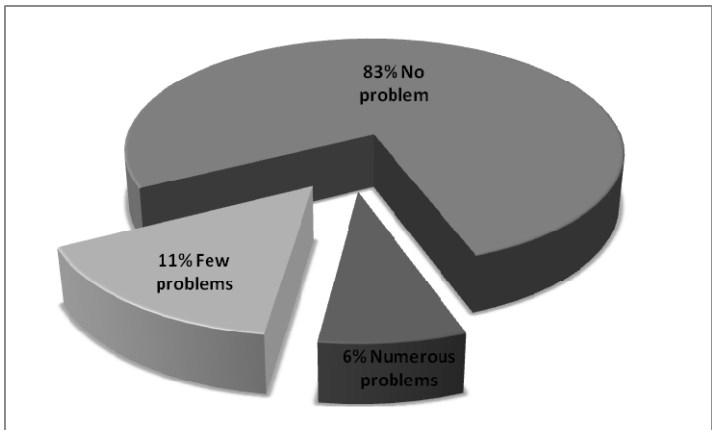


Chart 14, Problems due to insufficient training of PFSO or SSO

On the other hand, the ports were asked regarding to any possible arguments or problems that they had with ship or cargo owners about the ISPS code. The results show, same as previous, that it could not be a major issue in Sweden.

It is noteworthy to mention that most of those few cases regarding to either untrained officers or cargo and ship owners, happened at the beginning of the code implementation; and it seems that the situation is getting better as time goes by, since every one has become more familiar with the ISPS and its intricacies.

5.2 Impacts on activities

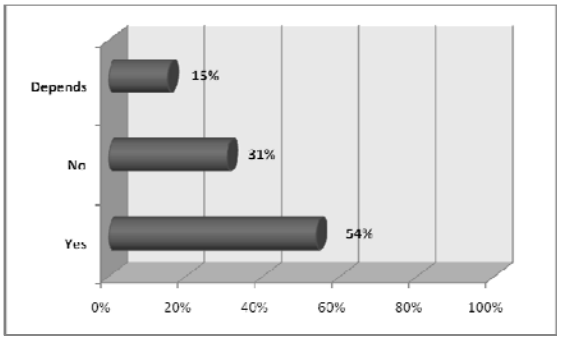
The next stage in this study is to find the impacts of the code on port's activities. Although the issues that were mentioned lately can affect port's activities in some ways, but the more effects would come from the matters that will be mentioned in this part.

[1] ISPS code, Part A, Sections 13&18

5.2.1 Working situation on security level 3

One of the situations that might happen, while the ISPS code rules in ports, is when the security level would be set on highest level. In this level, as an imminent attack is possible, then the security preparation and checking process would be applied in their highest level. For instance 100% of the cargos would be checked at this level, while this amount is 20% and 5% for level 2 and 1 respectively *(A security expert).* As a result, working in these circumstances would be extremely time-consuming and costly. It is possible that some ports would not be so eager to work and prefer to remain idle until the threat vanishes. On the other hand, if a port decides to stop working in security level 3, it could be interpreted that the intruders were successful to disrupt the port's activities and global business *(A security expert)*. Therefore, the ports were asked regarding to work in this condition or not. The result was truly favorable (Chart 15, Figure 1); 54% of the respondent ports will work in security level 3 and 15% of them have answered that it will depend on cause of the alert. Nonetheless the result could be disenchanted, if the answers of the ports, which preferred not to answer this question, be comprehended as "No". As it is seen (Chart 15, Figure 2) the outcome has almost shifted; 50% of the ports will not work in security level 3, which is not desirable for Contracting Governments.

The ports, which preferred not to answer the question, are ignored.



The answers of the ports, which preferred not to answer the question, are comprehended as "No".

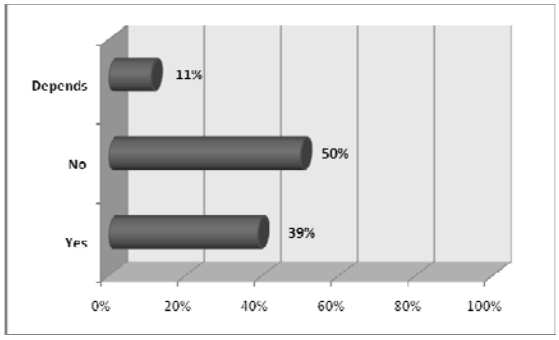


Chart 15, Working in security level 3

5.2.2 Serving time

The other concern of the author about the ISPS code was to know if the ISPS code has changed the serving time for ships or not. According to results (Chart 16), since all the security checking and customs formalities must be checked before the ship arrives, the loading and unloading time have not changed noticeably. Therefore, it could be understood that the serving time has remained unchanged. In view of the fact, by applying the code the level of security is increased and at the same time the serving time has not changed; therefore some advantages are gained without loosing other benefits. On the other hand, due to closing of the port for exterior people, the working environments have been increased and as a result, the effectiveness of cranes, lift trucks and other equipments at port facility have been increased too *(An interviewee)*. Then it could be apperceived as one of the main advantages of the ISPS code.

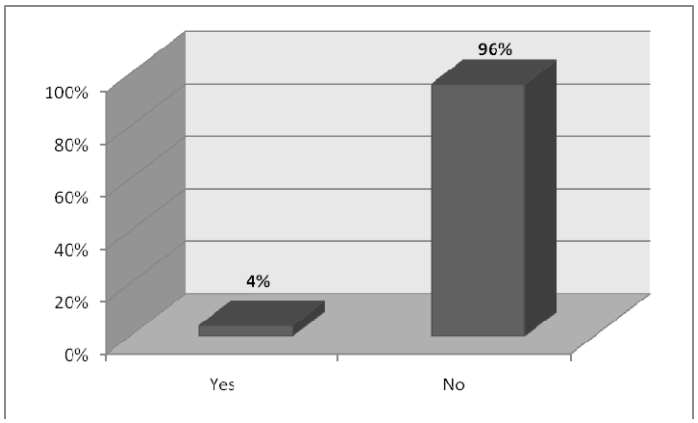


Chart 16, Change in serving time

5.2.3 Part B of the code and related concerns

One of the other possible problems, which might be occurred because of existing discordant views, is about the part B of the code. As it is mentioned in previous parts, the USA made part B of the code mandatory for all the US flag ships and also for foreign ships that want to conduct business with the United States' ports. Besides, the EU parliament made it obligatory too, but just for its own ship flag states. However, the other countries in the world have not made such decision for their territories. Therefore it is possible that these decisions put some businesses in trouble. Thus the ports were asked to know their ideas regarding this matter. It should be borne in mind, even though their opinions can reveal some facts about this issue, it would be noteworthy if this question would be asked from some other parties and companies who are more involved in business conduction and also are located outside the EU and the US borders.

The respondent ports' major ideas impart that this decision did not have any undesirable impacts on global trade and business. As it is shown in Chart 17, 70% of the respondent ports believe that it has had no impacts, while just 30% of them have accepted that it might cause some problems. It should be mentioned that 45% of the respondent ports preferred not to answer this question. One of them has mentioned its own reason as:

> *"I don't agree that part B is [mandatory] only for US and European countries. It is in the SOLAS that is global for ships over 500 tonnes. That's the reason to set the regulation under SOLAS to make it mandatory for all ships"*

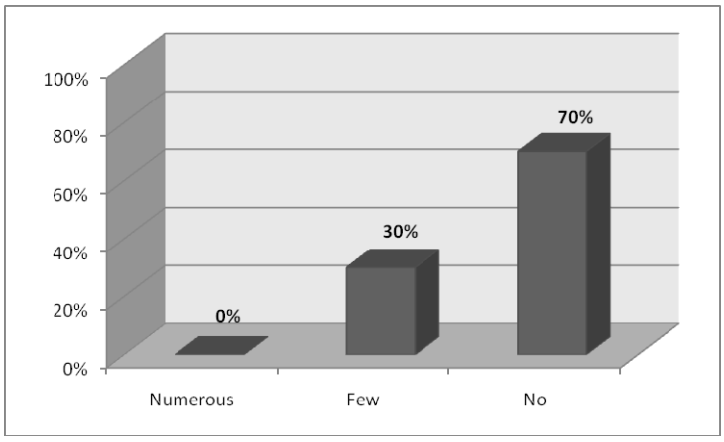


Chart 17, Possible effect of making the part B of the code mandatory

5.2.4 Indirect impacts

In questionnaire, the ports were asked about the indirect impacts of the ISPS code on their activities in addition to the security level. The factors, which were questioned, had been defined according to supply chain essential elements like lead time, administration cost, service level, customer satisfaction etc, to find how the ISPS code has affected supply chain's vulnerabilities as a mean to mitigate supply chain's environmental risks. (Chart 18)

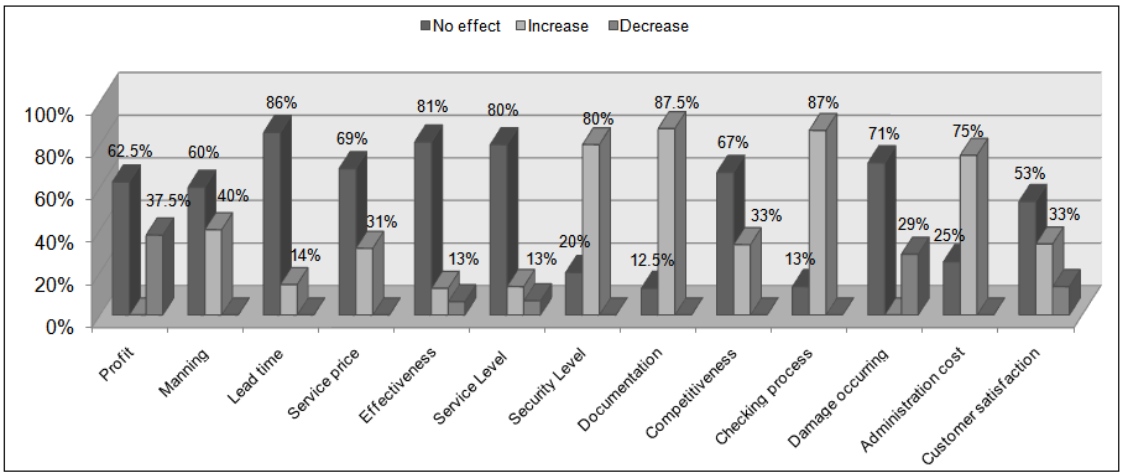


Chart 18, Indirect impacts of the ISPS code beside the impact on security level

An important majority of the respondent ports (80%) noted an increase in security level, which is the main goal of the ISPS code. Although it is estimated as 60% increase in security level, but it seems that the code was mainly successful to fulfill its major purpose. It must be considered, as Swedish ports are not really related to terrorism, increasing in security level in Swedish ports could be meant less smuggling and theft or better control in port area. As some interviewees said:

> *"We do not think our port is of great interest for terrorist…"*
>
> *"Do not think we are a subject to any substantial risk whatsoever"*

In comparison, the other factors like documentation, checking process and administration cost were reported as increase in their levels by majority of the respondent ports; whereas other factors like lead time, effectiveness, service level and damage occurring have not been affected significantly by the ISPS code. On the other hand there are some other factors like profit, manning, customer satisfaction, service price and competitiveness that the respondent ports have not had quite similar idea about the ISPS code's impact on them.

To have an overall analysis about the above mentioned factors, they have been divided into two groups; *Group 1* consists those factors that increasing in their level will increase the efficiency of the port, and *Group 2* includes those factors that decreasing in their level will affect the port efficiency in good way.

Group 1	No effect	Increase	Decrease
Profit	63%	0%	38%
Service Level	80%	13%	7%
Effectiveness	81%	13%	6%
Security Level	20%	80%	0%
Competitiveness	67%	33%	0%
Customer satisfaction	53%	33%	13%

Table 1, Positive factors in port efficiency

Group 2	No effect	Increase	Decrease
Manning	60%	40%	0%
Lead time	86%	14%	0%
Documentation	13%	88%	0%
Checking process	13%	87%	0%
Damage occurring	71%	0%	29%
Administration cost	25%	75%	0%
Service price	69%	31%	0%

Table 2, Negative factors in port efficiency

By considering the positive impact from group 1 and negative impact from group 2 on port efficiency in case of increasing and vice versa, the total efficiency of the respondent ports have been affected by the ISPS code according to Chart 19. Again, it should be borne in mind that the records are showing the total number of ports which agree to the specific effect.

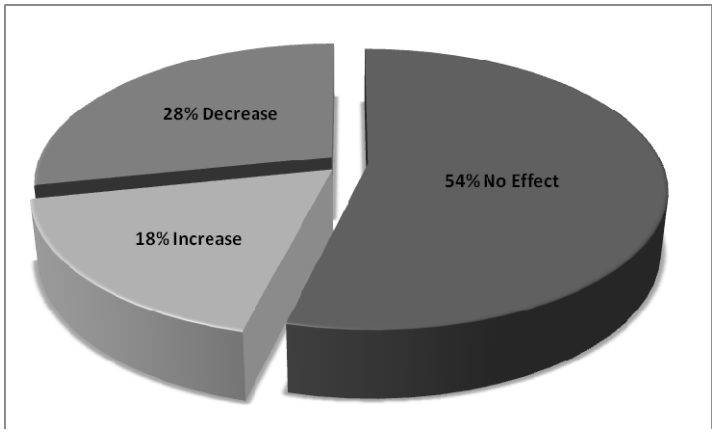


Chart 19, Impact of the ISPS code on ports' efficiencies according to separated factors

As it is seen, about half of the respondent ports believe that the ISPS code has had no significant effect on their activities, although more than quarter of the ports accepts that the ISPS code has decreased their efficiencies.

This is quite interesting result. However it will be more interesting if it is compared with Chart 20, which is the outcome of the direct question about the impact of the ISPS code on port efficiency. The number of the interviewees, who believe the ISPS code has had neither positive nor negative impacts on their ports' efficiency, will be remained without considerable change. But when the comparison is done on the ports, who believe that the ISPS code had either positive or negative effect on port efficiency, the result would be ponderable. The number of the interviewees, who believed that the code had positive effect on their ports'

efficiencies, increases dramatically 294% from 18 to 53 percent; while this number for the interviewees, who believed in opposite, shows 100% decrease from 28 to 0 percent.

This considerable result expresses this fact that the port efficiency is being affected noticeably by other factors than what have been mentioned above. These factors, according to UNCTAD's (2007) report could be additional security personnel, new access control measures at gates, screening measures, the introduction of port worker passes, better internal organization and better planning of container yards and ships.

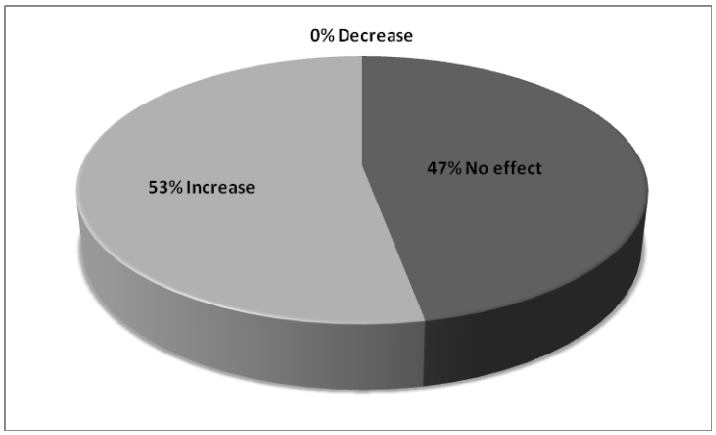


Chart 20, Impact of the ISPS code on ports' efficiencies according to direct question

It is proper to mention that Chart 1 and Chart 2 from UNCTAD's (2007) report are comparable with together Chart 18 and Chart 20 from this report.

From supply chain vulnerability's perspective, it seems that the ISPS code has mitigated the environmental risks' group 7 (criminal actions)[1] by increasing security level in maritime sectors. On the other hand, if the code's extra costs be ignored, since most of the extra works that the ISPS code imposed to parties can be done during idle time, the ISPS code has not created any new environmental risk for supply chains because of its extra manning and documentations.

5.2.5 Port satisfaction

Ports' level of satisfaction for applying the ISPS code can be another factor to evaluate the code's degree of success. Even though the results are dependent on ports' values, level of satisfaction will not change significantly if the value of the ports would not be taken into consideration. The satisfaction level of biggest population of the respondent ports (32%) is set to more than 90 percent satisfaction, if the value of the ports be taken into account. This level would be lain down between 70 and 90 percent without considering the ports' values. This conclusion, in some ways, is another proof for this fact that the ISPS code is working better for larger ports rather than smaller ones. (Chart 21)

[1] Refer to 2.5 Supply chain vulnerabilities

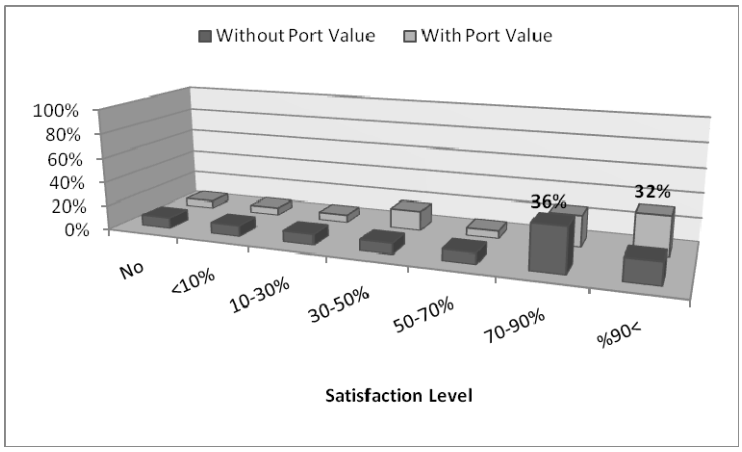


Chart 21, Satisfaction level of the ports from the ISPS code by considering port value

As it is perceptible, the value of the port does not have any important effect on the level of satisfaction. Thus, the overall level of satisfaction of the ISPS code implementation can be summarized in Chart 22. High level of satisfaction represents those ports that were more than 50% satisfied with implementing the ISPS code. Consequently, low level of satisfaction acts for those ports, which were less than 50% satisfied with applying the code.

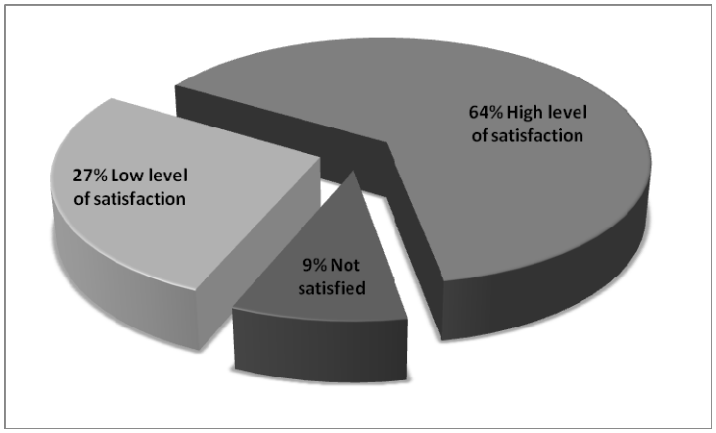


Chart 22, Satisfaction level of ports from the ISPS code by an overall view

As it is seen, the overwhelming majority of the respondent ports (91%) are satisfied with implementing the ISPS code on their port areas, which is another winning point for the ISPS code. Of course the unsatisfied ports have also some thing to say:

> *"We have no choice [!]"*
>
> *"Who can stay outside and still operate on international business?"*

Although the relation between satisfaction level from implementing the ISPS code, and improving percentage in port's activities due to the code, is not clear; but comparison between the ports' answers about satisfaction level and improving percentages in their activities, can reveal this possible actuality that their satisfactions do not relate too much to improving level

of their activities. As it is shown in Chart 23, nearly 90% of the respondent ports have reported low level (lower than 50%) or even no improvement in their activities. Even though this quite odd outcome could be because nearly 50% of the ports preferred not to answer this question, but the other explanation is that improvement in their activities is not really an important factor in satisfaction of the ports' administrators. For instance, the other factors like security level could be more powerful parameter in satisfying the ports. It should be mentioned that improving level and effectiveness in port activities are two comparable factors, which in this study are showing, more or less, similar results.

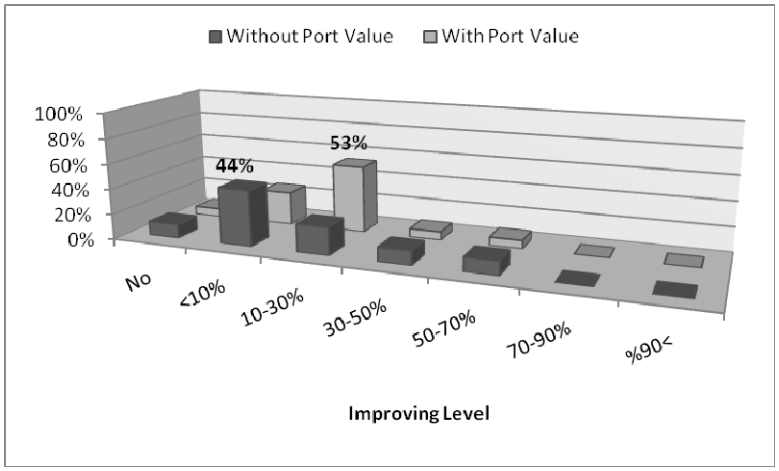


Chart 23, Improving level in ports' activities due to the ISPS code

The question is "why did half of the respondent ports prefer not to answer this question?". It is possible that they did not have a detailed and exact view about the improvement in their activities, and consequently they preferred not to answer the question. It is the reason that is supported by one of the interviewee's comment:

"Hard to give firm answer, think in the long run the port activities have improved."

In this case, it could be expected to have more improvement in port activities by time lapse.

5.3 Nature of the ISPS code

On question 34, the ports were requested to express their opinions about the ISPS code. The options that they had to choose were three; 1- Preventive, which means the code is more useful to stop threats to happen, 2- Protective, which means the ISPS code is more fitted to protect the ship or port facility against a thereat while it is happening, 3- Consequence reducer, which means the code can be used after the threat passed, to make a port resilient and reduce the consequences of happened threat. As it was expected, the majority of the respondent ports did agree with this idea that the ISPS code is more practical before a threat happens; means it has a preventive essence rather than protective or consequence reducer.

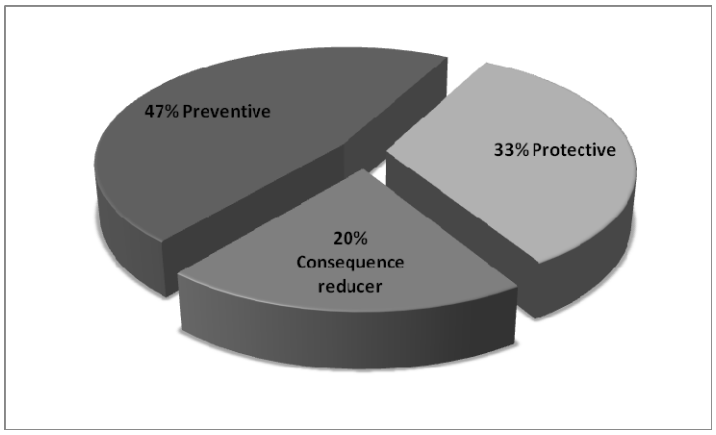


Chart 24, The ISPS code description

In addition, one of our interviewees has described the ISPS code smartly:

> *"The ISPS code rules used with common sense in a proper way; is good for increasing the awareness and competence of all workers in the port. Best way to improve correct action before, during a threat, and making the consequences lower after a threat."*

5.4 Pros and cons

The respondent ports had different ideas about the advantages and disadvantages of the code. However the overall points that had been mentioned by the ports were similar to those which were pointed out in previous parts, the opinions about them differed from port to port.

In general, the advantages of the ISPS code can be summarized as:

- Higher safety and security and lower risk
- Better control on port's area, goods flow and personnel
- Better documentation (Having unified standard for documents)
- Better working environment

While its disadvantages are:

- Slow work progress
- More paper works
- More costs
- More administration works

Also 17% of the respondent ports believed that the ISPS code did not have any disadvantages, while only 7% of them mentioned that it had no advantages.

5.5 Additional questions

In this part, few answers that have been received for additional questions, beside the general comment from an interviewee, have been quoted. The additional questions are some few subjects that have been asked at the end of the questionnaire. Answer to those questions was not emphasized while it was requested; therefore most of the respondent ports preferred not to answer those questions. However, the few received answers can illustrate more facts about the

ISPS code implementation. It should be hinted that the duplicated answers have not been cited.

5.5.1 Which parts of the port or port facilities are more susceptible, and/or more likely to be subject of a terrorist attack, in your point of view?

- *"The container and roro port facility"*
- *"We do not think our Port is of great intrest for terrorist, accept the possible use of the Port or people connected to the port to use as " base" for attacks to other facilties. Such as the nuclear power plant nearby."*
- *"Probably the cafeteria because of the quality of the coffee!"*
- *"Oil harbour and the area around the factory for animal feedstuff in the port"*
- *"Containers"*
- *"Don´t think we are a subject to any substansial risks whatsoever"*
- *"None"*
- *"Our container handling"*
- *"The terminal building."*

5.5.2 How much the mariners, workers, seafarers, fishermen etc have contributed to adopting the ISPS code in your port?

- *"Nothing"*
- *"A lot. Without the support and understand of the code rules by the mentioned groups, the rules are worthless"*
- *"Litle"*
- *"less than 5%"*
- *"Most people have done their best"*
- *" Workers and customers are in the process of implementing ISPS"*

5.5.3 Which opportunities do you think that you have gained or missed by applying the ISPS code?

- *" Nothing"*
- *"We have gained better working environment"*
- *"We had lost a lot of interest from present and new clients"*
- *"The harbour is in better order. Betterr safety and security, less losses and damages"*
- *"We have a closed port and nobody can visit the area"*

5.5.4 Any comment:

- *"Before ISPS was implemented, Sjöfartsverket and companies like Securitas built up a vision that ISPS was a job in war against terrorist and showed pictures of Bin Ladin. ISPS have nothing to do with war against terrorists. The aim must be to fight criminal acts like smuggle of people, weapons, drugs etc"*

6. Conclusions

In this chapter, the results, which have been gained by this study, have been concluded. Besides, the research questions have been answered.

6.1 General conclusion

Terrorism is the phenomena that the Sweden and Swedes were unfamiliar with until recent years. After Olof Palme[1] and Anna Lindh[2] assassinations, the Swedish citizens gradually understood that the terrorism is converting to an industry, which some ones use it to extort their wants. However, this is a situation which is really rare in Sweden, but as Sweden's security service[3] has warned, "*there is a risk of Sweden becoming a recruiting base for terrorists, and a base for the financing and planning of attacks in other countries*." *(Thornberg, 2007b)* [4] As a result, Sweden, as well as other countries, has to be aware about terrorism and its consequences.

The ISPS code, which has designed to make terrorists' work as hard as possible, came into force in all regions as well as Sweden. The ISPS code main mission is to address the security issues in maritime transportation. Although the birth reason for the ISPS code was terrorism, the other security related issues like smuggling, theft and piracy can be addressed by its implementation.

By an overall view, the ISPS code was successful in its main goal. The security level has increased in maritime sectors. Of course the main issue, threats, could not be wiped out totally, however the ISPS was an outstanding step to mitigate their effects on seaborne transportation.

In addition to what the ISPS has as its advantages, there are some disadvantages, which of course could not fade its benefits, but should be considered to make its impacts as effectual as possible. Some disadvantages like extra costs and extra works.

Moreover, it seems that the ISPS code is well designed for large ports rather than smaller ones. It could be argued as the large ports are the ones who define the key factors of the market and affect international rules, the small ports would be the loser players without external helps. As a proof, the USA as one of the biggest players in global trade, has its own unique maritime rules in international trade, like making the part B of the code mandatory for foreign flag ships that want to conduct business with the US ports, or asking for 4 days in-advance declaration for every ships that want to enter into the US sea borders, and also CSI (Container Security Initiative) and C-TPAT (Customs-Trade Partnership Against Terrorism) programs. Although joining to the last two programs is not mandatory, it is quite impossible for others to neglect them. They had to obey it, since the USA is one of the key factor definers in international maritime trade.

[1] Former prime minister of Sweden, who was shot and murdered on February 28th , 1986

[2] Former foreign minister of Sweden, who was stabbed and murdered on September 10th , 2003

[3] Säpo

[4] Anders Thornberg, Säpo's information director, *(The local, 2007b)*

6.2 Impacts on supply chain vulnerabilities

From supply chain vulnerability's point of view[1], the ISPS code has alleviated the environmental risks' group 7 (criminal actions) and group 3 (human factors: unauthorized access) by increasing security level in maritime sectors. On the other hand, it is possible that the ISPS code make supply chains more vulnerable by its implementation. For instance some issues like human rights, which have not been risen for consideration yet, might make supply chains vulnerable via maritime sectors by increasing risk of mariners strike (Environmental risks' group 3, human factors); or some irrational and tight security checking, supplementary to the ISPS code, could make supply chains more vulnerable by causing congestion in ports and making the global business unsmooth (Environmental risks' groups 1 and 8).

6.3 Answers to the research questions

Q1. What are the main impacts of the ISPS code on shipping industry?

They can be summarized into two factors, security level and expenditures. The security level has really increased in maritime transportation. Secure fleet, secure flow of goods and secure environments at ports and their areas show this fact. But, the extra costs and extra works that the ISPS code has imposed on maritime parties due to its implication, is the bad side of this new regulation.

Q2. How they can affect port and port activities?

On the one hand, increasing security level in harbors, as a main part of the shipping industry, has an important role in their effectiveness. Better control of the port area, restriction of unauthorized access and better work environment are the main and good influences of the ISPS code on port and port activities. On the other hand, the extra costs and extra works, due to the ISPS code, cause some difficulties for ports and their activities. One of the main problems about the code's implication is that the cost payers have not been defined well. In every case, the main question is "who must pay the costs?" which can result in some hitches. In addition, some factors like more documentation, more administration, extra checking and extra manning make it really difficult to judge about the code. It highly depends on the price that everyone likes to pay to feel secure.

Q3. Has the ISPS code accomplished its mission well?

Let's say, with some leniencies, yes it has. The security level has increased in ports. Although it is hard to talk about its impacts on terrorist events presently, but certainly it had really clear influences on smuggling and theft.

Overall, the ISPS code is like a train which is moving while railroad tracks are being laid. There were many issues that needed more consideration before its execution; some matters like human rights or cost payers. Now, after its implementation, there is more need for high attention, and all in charge parties must keep a sharp lookout for its implementation, otherwise it might be derailed!

[1] Refer to 2.5 Supply chain vulnerabilities

7. References

[1] 9/11 by the Numbers. New York Magazine Holdings LLC. Available online at: http://nymag.com/news/articles/wtc/1year/numbers.htm (accessed 2007/11/01)

[2] Impact of the ISPS Code on Members of ITIC. International Transport Intermediaries Club Ltd. Available online at: http://www.itic-insure.com/publications/isps_code/impact_isps_code.php (accessed 2007/06/27)

[3] (2002a) Is shipping vulnerable to the terrorist? , Baltic and International Maritime Council (BIMCO). Available online at: http://www.bimco.org/Corporate%20Area/Seascapes/Questions_of_shipping/Is_shipping_vulnerable_to_the_terrorist.aspx (accessed 2007/10/15)

[4] (2002b) Indonesia: The search for peace in Maluku. Jakarta/Brussels, ICG (International Crisis Group). Available online at: http://www.reliefweb.int/library/documents/2002/icg-maluku-08feb.pdf (accessed 2007/06/27)

[5] (2002c) Supply Chain Vulnerability: Final report on behalf of DTLR, DTI and Home Office, Cranfield University, School of Management.

[6] (2003) *Understanding Supply Chain Risk: A Self-Assessment Workbook*, Cranfield School of Management, Centre for Logistics and Supply Chain Management. Available online at: http://www.som.cranfield.ac.uk/som/research/centres/lscm/risk.asp (accessed 2008/01/28)

[7] (2004a) ISPS code-Legal Implications for Charterparties. Sounding Archive. 4 ed., The UK Defense Club (UKDC). Available online at: http://www.ukdefence.com/ukdc_publications/soundings/2004_i4_soundings.php (accessed 2007/07/07)

[8] (2004b) REGULATION (EC) No 725/2004 on enhancing ship and port facility security. 2004 ed., The European parliament and the council of the European Union.

[9] (2005a) DIRECTIVE 2005/65/EC on enhancing port security. 2005 ed., The European parliament and the council of the European Union.

[10] (2005b) Military Law Review, Protecting U.S. ports. U.S. Armed Forces journal of military legal scholarship, 185.

[11] (2006) Sveriges Hamnar. TransportGruppen. Available online at: http://www.transportgruppen.se/templates/MultiMaster.aspx?id=31763

[12] (2007a) ISPS Code, Advisory and certification services. Lloyd's Register. Available online at: http://www.lr.org/Standards/Codes/ISPS+faq.htm (accessed 2007/10/10)

[13] (2007b) Sweden 'risks becoming terror base'. The local. Available online at: http://www.thelocal.se/8106/20070806/ (accessed 2007/12/29)

[14] (2007c) *The World Factbook*, CIA. Available online at: https://www.cia.gov/library/publications/the-world-factbook/ (accessed: 2007/12/29)

[15] ASBJØRNSLETT, B. E. (2006) Coping with risk in maritime logistics. Trondheim, NTNU.

[16] ASBJØRNSLETT, B. E. & RAUSAND, M. (1999) Assess the vulnerability of your production system. Production Planning & Control, 10, 219-229.

[17] BANOMYONG, R. (2005) The impact of port and trade security initiatives on maritime supply-chain management. Maritime Policy & Management, 32, 3-13.

[18] BARNES, P. & OLORUNTOBA, R. (2005) Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management. Journal of International Management, 11, 519-540.

[19] CARLILE, A. (2007) The Definition of Terrorism. London, U.K. Parliament.

[20] CAVINATO, J. L. (2004) Supply Chain Logistics Risks, From the back room to the board room. International Journal of Physical Distribution & Logistics Management, 34, 383-387.

[21] CHAUVEL, A.-M. What is ISPS code? Bureau Veritas- DNS/DCO.

[22] CHEW, F. (2005) Piracy, maritime terrorism and regional interests. Geddes Papers 2005. The Australian Command and Staff College.

[23] COLEMAN, B. J. & JENNINGS, K. M. (1998) The UPS strike: lessons for just-in-timers. Production and Inventory Management Journal, 63-7.

[24] COMPTON, M. (2006) Cargo handling in the global marketplace. ISO Focus, 3, 41-43.

[25] COUSINS, P., LAMMING, R. C. & BOWEN, F. (2004) The role of risk in environment-related initiatives. *International Journal of Operations & Production Management,* 24**,** 554-565.

[26] D'ADDARIO, F. (2006) ISO/PAS 28001 enables Starbucks Coffe Company's supply chain strategy. ISO Focus, 3, 12-17.

[27] DEBOER, D. (1992) *Piggyback and Containers: A History of Rail Intermodal on America's Steel Highway,* San Marino, CA, Golden West Books.

[28] DONOVAN, A. (2004) Intermodal Transportation in Historical Perspective. NCIT (National Center for Intermodal Transportation).

[29] EKWALL, D. (2007) Antagonistic Gateways in the Transport Network in a Supply Chain Perspective. Department of Technology Management and Economics-Division of Logistics and Transportation. Göteborg, Chalmers.

[30] ELLIOTT, L. (2005) US trade deficit hits record after Boeing strike and hurricanes. *The Guardian.*

[31] FOURGEAUD, P. (2000) Measuring port performance. The World Bank.

[32] GOULIELMOS, A. M. & ANASTASAKOS, A. A. (2005) Worldwide security measures for shipping, seafarers and ports- An impact assessment of ISPS code. Disaster Prevention and Management, 14, 462-478.

[33] GRIFFETT, T. (2005) The impact of ISPS Compliance on Ship owners. Melbourne, Australian Ship owners Association.

[34] HALLIKAS, J., VIROLAINEN, V.-M. & TUOMINEN, M. (2002) Risk analysis and assessment in network environments: a dyadic case study. *International Journal of Production Economics,* 78**,** 45-55.

[35] HANDFIELD, R. B. & NICHOLS, E. L. (1999) *Introduction to Supply Chain Management,* Prentice-Hall, Upper Saddle River, NJ.

[36] HARLAND, C., BRENCHLEY, R. & WALKER, H. (2003) Risk in Supply Networks. *Journal of Purchasing and Supply Management,* 9**,** 51-62.

[37] HARRISON, A. & HOEK, R. V. (2005) *Logistics Management and Strategy,* Prentice Hall, Financial Times.

[38] HOEK, J. V. D. (2006) ISO/PAS 28000: A security oddity? ISO Focus, 3, 23-25.

[39] IMO (1974) SOLAS. in IMO (Ed. 2002 ed.

[40] IMO (2002) ISPS code. in IMO (Ed. 2003 ed.

[41] KHAN, O. & BURNES, B. (2007) Risk and Supply Chain Management: Creating a Research Agenda. *The International Journal of Logistics Management,* 18**,** 197-216.

[42] KÖKNAR, A. M. (2005) Maritime terrorism: a new challenge for NATO. IAGS Energy Security. Available online at: http://www.iags.org/n0124051.htm#12 (accessed 2007/10/16)

[43] KORD, H. K. & PAZIRANDEH, A. (2006) What is vulnerability? Borås, University College of Borås.

[44] LEAVITT, F. & WASSERSUG, S. R. (2006) US ports set sail for ISO/PAS 28000. ISO Focus, 3, 18-22.

[45] MACKENBACH, P. & LIGHTBURN, P. (2006) Regulating towards more secure supply chains. ISO Focus, 3, 31-37.

[46] MCNAUGHT, F. (2005) Effectiveness of the International Ship and Port Facility Security (ISPS) Code in addressing the maritime security threat. Geddes Papers.

[47] NEAL, M. (1994) Security Films vs. Safety Films, Understanding the Misunderstood Differences. Pinnacle Armor. Available online at : http://www.pinnaclearmor.com/technical-papers.php

[48] O'MALLEY, S. (2006) Best practice in custody for security of the supply chain. ISO Focus, 3, 8-12.

[49] OSNIN, N. A. (2003) Maritime Security and The ISPS Code. Center for Ocean Law and Policy. Maritime Institute of Malaysia.

[50] OVERBY, S. (2007) ABC: An Introduction to Outsourcing

[51] PECK, H. (2005) rivers of supply chain vulnerability: an integrated framework. International Journal of Physical Distribution & Logistics Management, 35, 210-232.

[52] RØDSETH, Ø. J. (2006) Electronic port clearance: Extensive ship reporting for port calls. ISO Focus, 3, 38-40.

[53] SARATHY, R. (2006) Security and the Global Supply Chain. Transportation Journal, 29-51.

[54] STEVENSON, D. B. (2005) The Impact of ISPS Code on Seafarers. International Conference Security of ships, ports and coasts. Halifax, Nova Scotia, Canada.

[55] SVENSSON, G. (1999) A conceptual framework for the analysis of vulnerability in supply chains. International Journal of Physical Distribution & Logistics Management, 30, 731-749.

[56] SVENSSON, G. (2001) A conceptual framework of vulnerability in firms' inbound and outbound logistics flow. International Journal of Physical Distribution & Logistics Management, 32, 110-134.

[57] TIMLEN, T. (2006) Approaching security cohesion. ISO Focus, 3, 29-30.

[58] TIMMONS, H. (2004) Got Oil? Now, Try to Find Tankers to Carry It. The New York Times. Available online at: http://query.nytimes.com/gst/fullpage.html?res=9B01E4D71630F93AA35755C0A9629C8B63 (accessed 2007/10/16)

[59] TRELAWNY, C. (2006) Containerized cargo security- A case for international standards. ISO Focus, 3, 25-28.

[60] TZANNATOS, E. S. (2003) A decision support system for the promotion of security in shipping. Disaster Prevention and Management, 12, 222-229.

[61] UNCTAD (2002) Review of Maritime Transport. United Nations Conference on Trade And Development.

[62] UNCTAD (2007) ISPS Code implementation, costs and related financing. United Nations Conference on Trade And Development.

[63] WENGELIN, M. (2006) The Swedish Port Security Network – An Illusion or a Fact? Journal of Homeland Security and Emergency Management, 3, Article 8.

8. Appendices

8.1 Appendix 1: *Questionnaire*

How the ISPS code affects port and port activities

Questionnaire

September 2007

Borås-Sweden

This survey is running within secure flow project, which is a VINNOVA sponsored project. VINNOVA sponsored project tasked with improving the safety and security of goods transportation within the supply chain in Sweden. VINNOVA is Swedish Governmental Agency for Innovation Systems. (www.vinnova.se)

Government of Sweden assigned VINNOVA to:

- promote sustainable growth
- support research and development
- stimulate Swedish participation in EU & international R&D collaboration

The aim of this survey is to find the impacts of ISPS code on port and port activities. Your answers will be completely anonymous. Therefore, the interviewee's name will be mentioned no where. The name of the company will just be mentioned at the end of the report, in alphabetic order, at the topic of "The Cooperator Companies". There will be no way to find who answers what. In addition, you can skip each question that you do not like to answer by filling in the square next to "☐ *Prefer not to answer this question*"

We would really appreciate it if you can send back your answers within 2 weeks. In case of any questions, please do not hesitate to contact us.

Yours very sincerely,

September 2007

Arsham Mazaheri

Contact Details:

Interviewer:

Arsham Mazaheri

Master Student at University College of Borås (Högskolan i Borås)
Email: X050048@utb.hb.se
Cell phone: 0704 810 715

Project Leader:

Håkan Torstensson

Professor at Engineering School of University College of Borås

Email: hakan.torstensson@hb.se

Tel: 033-4355971

Supervisor:

Daniel Ekwall

Ph.D. at University College of Borås

Email: daniel.ekwall@hb.se

Tel: 033-4355972

Advisor:
Timothy Tinney
Researcher at University College of Borås
Email: timothy.tinney@hb.se
Tel: 033-4354256

Attention:

1. Please kindly use TAB button or Mouse to switch between fields, instead of ENTER.
2. Please kindly use Ctrl+S regularly to save your answers to avoid to lose them accidentally
3. Every where that the word "*you*" has been mentioned, it has been meant "*your organization*" or "*your port*".
4. You should answer some questions by filling in the blank square beside each answer or by writing your idea below each question. In case of multiple-choice questions, if you have additional information, we would appreciate if you kindly add your comments also. In other questions, please use the space in front of the word "Comment" to write your answer.
5. If you want to choose more than one answer in some questions, feel free, do it!
6. Except questions no. 4 and 5, the other questions have been asked regarding to the ISPS code. Please leave your comments in case of any differences between the ISPS code and "Regulation 2004/725/EC" and "Directive 2005/65/EC", in those questions.
7. If it is possible, please kindly attach your port's statistics or a link to your website, which contains information about numbers and kinds of ships that have visited your port annually from 2000 or later (but before 2004) up to now. Otherwise, please answer below questions:
    a. Your answer will be according to which year?
    b. How many ships (in general) have visited your port in that year?
    c. What was the total tonnage of the ships that you have served in that year?

Questions:

1. Name of the company:
2. Position of the interviewee:
3. For applying the ISPS code, each port had to implement some security measures before July 1st 2004. In this way, some ports, which were more close to terms of the ISPS code, had to do less than the others, who were far from the ISPS code's requirements. How much have you been matched with the requirements of the ISPS code before adopting it?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Less than 10% ☐ 10-30 % ☐ 30-50% ☐ 50-70%
☐ 70-90% ☐ More than 90%

Comment:

4. Would you please answer question no.1 for "Regulation 2004/725/EC of the European parliament and of the council of 31 March 2004 on enhancing ship and port facility security"?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Less than 10% ☐ 10-30 % ☐ 30-50% ☐ 50-70%
☐ 70-90% ☐ More than 90%

Comment:

5. Would you please answer question no.1 for "Directive 2005/65/EC of the European parliament and of the council of 26 October 2005 on enhancing port security", which made the part B of the ISPS code compulsory?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Less than 10% ☐ 10-30 % ☐ 30-50% ☐ 50-70%
☐ 70-90% ☐ More than 90%

Comment:

6. Did you have any problem (in the time point of view) to apply all the ISPS code requirements before its deadline? As it is published in late 2002 and came into force on July 1st 2004.

☐ The question is unclear
☐ Prefer not to answer this question

☐ Yes, lots of problems ☐ Yes, but not to much ☐ No, not at all

Comment:

7. Would you please answer question no.6 for "Directive 2005/65/EC of the European parliament and of the council on enhancing port security"? As it is published in October 26th 2005 and came into force on June 15th 2007.

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, lots of problems ☐Yes, but not to much ☐No, not at all

Comment:

8. How much did it cost for you (Approximately) to apply the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

SEK or % of our annual income

Comment:

9. Have you reached to break even point yet?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Yes ☐ No

Comment:

10. Will you work in security level 3 or do you prefer to stop the business? (Because, working in security level 3 could be really costly)

☐ The question is unclear
☐ Prefer not to answer this question

☐ Will work ☐ Will not work ☐ Depends (Please specify)

Comment:

a. How much does it cost (approximately) if you stop your businesses (for any reason) for one hour?

☐ The question is unclear
☐ Prefer not to answer this question

SEK or % of our annual income

Comment:

11. Who will pay the cost of the increasing security level in a ship (who wants to moor in your port), when its security level is lower than what the port's is?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Port Authority ☐ Cargo Owner ☐Ship Owner ☐Government ☐ Other

Comment:

12. In past 2 years, how many times have you raised your security level because of requesting a ship?

☐ The question is unclear
☐ Prefer not to answer this question

time(s) or % of our total acceptance in this time interval

Comment:

a. Did you charge them because of that (if there was any)?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No

Comment:

13. Do you charge extra to give permission to seafarers or chaplains to have shore leave or access to the ship?

☐ The question is unclear
☐ Prefer not to answer this question

☐No ☐Yes

Comment:

14. What were the main costs for applying the ISPS code in your point of view?

☐ The question is unclear
☐ Prefer not to answer this question

☐Providing equipments ☐Hiring personnel ☐Training personnel

Comment:

a. Who has paid these costs?

☐ The question is unclear
☐ Prefer not to answer this question

☐Port authority ☐Government ☐Companies at the port

Comment:

15. How many ships have been expelled annually from your port or denied to entry (if there was any) in general, ***before*** applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

% of our total acceptance

Comment:

a. What were the main reasons for them?

☐ The question is unclear
☐ Prefer not to answer this question

Comment:

16. How many ships have been expelled annually from your port or denied to entry (if there was any) in general, after applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

% of our total acceptance

Comment:

a. How many of them were expelled because they did not meet the ISPS code requirements?

☐ The question is unclear
☐ Prefer not to answer this question

% of total number of expelled ships or % of our total acceptance

Comment:

b. How many of them were unduly expelled?

☐ The question is unclear
☐ Prefer not to answer this question

% of total number of expelled ships or % of our total acceptance

Comment:

i. How many of them have charged you because of unduly expelling?

☐ The question is unclear
☐ Prefer not to answer this question

% of total number of unduly expelled ships

Comment:

ii. How much did they charge you totally?

☐ The question is unclear
☐ Prefer not to answer this question

SEK or % of annual income

Comment:

17. Do you accept a ship who has not applied the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No ☐Depends (Please specify)

Comment:

18. How many cargo ships, which are below the Convention size (500 GT), visit your port annually?

☐ The question is unclear
☐ Prefer not to answer this question

Ships or % of your annual acceptance

Comment:

a. Do you serve them as previous (before the ISPS code) or you do apply the ISPS code requirements on them as well?

☐ The question is unclear
☐ Prefer not to answer this question

☐Serve them as previous ☐Apply the ISPS code on them

Comment:

19. Does the serving time for ships, who does not apply the code and the ones, who does apply, differ from each other?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No ☐Depends (Please specify)

Comment:

a. If yes, which one is shorter?

☐ The question is unclear
☐ Prefer not to answer this question

☐Who does apply the code ☐Who does not apply the code

Comment:

20. Do you have some regular customers, like companies or ships, who use your port facility regularly?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No

Comment:

a. If yes; do you apply some exception for them because they are known for you?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No

Comment:

i. If yes; in what security level do you apply those exceptions?

☐ The question is unclear
☐ Prefer not to answer this question

☐Just in level 1 ☐Level 1&2 ☐Level 1&2&3

Comment:

ii. Do you charge them for these exceptions?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No

Comment:

iii. Do these exceptions make big differences, in time point of view, for them?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, always ☐Yes, some times ☐No

Comment:

21. Have you ever had any problem by arguing with the ship's crew or other personnel or passengers in the ship or port, because of doing the security checking, which may cause an action against human rights; like preventing the crew from shore leave?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, usually ☐Yes, rarely ☐No, not at all

Comment:

22. As you know, the part B of the ISPS code has been mandatory for EU member states and the USA. Do you think that this decision creates problems for ports located within these countries, to conduct business with ships from other countries, where the ISPS part B is not compulsory?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, it leads to lots of problems ☐Yes, it leads to some problems
☐No, it makes the business better ☐No, it has no effect

Comment:

23. Do you apply the ISPS code requirements for the ships, which are in domestic voyages?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No ☐Depends (Please specify)

Comment:

24. How many times have you raised your security level to level 2 or 3 after applying the ISPS code (July 1st 2004)?

☐ The question is unclear
☐ Prefer not to answer this question

times to security level 2
times to security level 3

Comment:

a. Have they happened because of real dangerous situation or just because of fake report?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Less than 10% were fake report
☐10-30 % ☐30-50% ☐50-70% ☐70-90%
☐ More than 90% were fake report

Comment:

25. Do the ships, who want to anchor in your port, have to submit the required documents (according to ISPS code) electronically or in printed forms?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Just electronically
☐ Just printed form
☐ Electronically ***and*** printed form
☐ Electronically ***or*** printed form

Comment:

26. Has the ISPS code affected these factors in your port? If yes, how much? (*please specify the percentage, in case of any change*)

☐ The question is unclear
☐ Prefer not to answer this question

Profit:	☐No	☐Increase	☐Decrease	%
Manning:	☐No	☐Increase	☐Decrease	%
Lead time:	☐No	☐Increase	☐Decrease	%
Service level:	☐No	☐Increase	☐Decrease	%
Effectiveness:	☐No	☐Increase	☐Decrease	%
Security level:	☐No	☐Increase	☐Decrease	%
Documentation:	☐No	☐Increase	☐Decrease	%
Checking process:	☐No	☐Increase	☐Decrease	%
Damage occurring:	☐No	☐Increase	☐Decrease	%
Administration cost:	☐No	☐Increase	☐Decrease	%
Customer satisfaction:	☐No	☐Increase	☐Decrease	%

Comment:

27. Has the ISPS code affected your service price?

☐ The question is unclear
☐ Prefer not to answer this question

☐No ☐Yes, Decrease, % ☐Yes, Increase, %

Comment:

a. In case of increase, was it acceptable for your customers? Do they pay your higher costs willingly because of increasing security level?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes ☐No

Comment:

b. How many ships have denied to entry (if there was any) <u>because of the extra security cost</u> that they had to pay?

☐ The question is unclear
☐ Prefer not to answer this question

Ships or % of your total acceptance

Comment:

28. Has the ***loading*** time of ships changed after applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

☐Decrease ☐Increase ☐Remain without change

Comment:

a. In case of change, in which security level has it changed?

☐ The question is unclear
☐ Prefer not to answer this question

☐Level 1 ☐Level 2 ☐Level 3

Comment:

29. Has the ***unloading*** time of ships changed after applying the ISPS code?

☐ The question is unclear

☐ Prefer not to answer this question

☐Decrease ☐Increase ☐Remain without change

Comment:

a. In case of change, in which security level has it changed?

☐ The question is unclear
☐ Prefer not to answer this question

☐Level 1 ☐Level 2 ☐Level 3

Comment:

30. Do you believe that the implementation of the ISPS code has had negative or positive impact on your port's efficiency in general?

☐ The question is unclear
☐ Prefer not to answer this question

☐Positive impact ☐Negative Impact ☐It has had no impact

Comment:

31. Do you think that applying the ISPS code has established an unfair competition between the ports, who have not applied the ISPS code, and the ones, who have applied it? If yes, who will be the winner?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, The parties, who have not applied the ISPS code
☐Yes, The parties, who have applied the ISPS code
☐No

Comment:

32. Are you satisfied by applying the ISPS code in your port (company)?

☐ The question is unclear
☐ Prefer not to answer this question

☐No, not at all
☐ Yes:
☐Less than 10% ☐10-30 % ☐30-50% ☐50-70%
☐70-90% ☐ More than 90%

Comment:

33. What is the improving percentage in your activities (totally) after applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

☐ Less than 10% ☐10-30 % ☐30-50% ☐50-70% ☐70-90%
☐ More than 90%
☐ There is no improvement, some times could be even worse

Comment:

34. Which below sentences can describe the ISPS code (against a threat) better? (*You can choose more than one*)

☐ The question is unclear
☐ Prefer not to answer this question

☐ Preventive (before a threat happens)
☐ Protective (while a threat is happening)
☐ Consequence reducer (which make your port resilient, after a threat happened)

Comment:

35. Have you ever faced with some problems, which they have happened because of different interpretation of the code from different perspectives? For instance, between your port and the ships from other Flag States.

☐ The question is unclear
☐ Prefer not to answer this question

☐ Yes, many times ☐Yes, but rarely ☐No

Comment:

36. Have you ever had any problem or argument between your workers and ships' crew for refusing the security plan? For example, if you want to carry out PFSP and it has some conflicts with SSP; then the ship's crews do not allow you to do or vice versa?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, lots of problems ☐Yes, but not too much ☐No, not at all

Comment:

a. If you had, do the tensions, decrease or increase after implementing "Directive 2005/65/EC on enhancing port security"?

☐ The question is unclear

☐ Prefer not to answer this question

☐Increased ☐Decreased ☐had no impacts

Comment:

37. Is the training of PFSO sufficient to handle all cases? How many cases has been there that any problem occurred, which have been related to insufficient training of the PFSO or SSO?

☐ The question is unclear
☐ Prefer not to answer this question

☐Insufficient, lots of cases ☐ Insufficient, not to much
☐Sufficient, not at all

Comment:

38. How many cases has been there that arguing with ships' crew or officers occurred because of preventing them to shore leave?

☐ The question is unclear
☐ Prefer not to answer this question

☐Lots of cases ☐Not too much ☐Not at all

Comment:

a. Do you think that the SID (Seafarers Identity Document) can prevent of these kinds of happenings?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes it can address it on its own
☐Yes it can, but needs some other methods beside (*Please specify if you think about any*)
☐No it can not

Comment:

39. Have your workers ever had any problem or any argument with ships' crew or SSO after applying the ISPS code, except about Shore leave or Different interpretation? What were the reasons?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, lots of problems ☐Yes, but not too much ☐No, not at all

Comment:

40. Have you ever had any problem with ship owners or cargo owners about security manner; ***before*** applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, lots of problems ☐Yes, but not too much ☐No, not at all

Comment:

41. Have you ever had any problem with ship owners or cargo owners about security manner; ***after*** applying the ISPS code?

☐ The question is unclear
☐ Prefer not to answer this question

☐Yes, lots of problems, more than before
☐Yes, lots of problems, but less than before
☐Yes, not too much, but more than before
☐Yes, not too much, less than before
☐No, not at all

Comment:

Additional Questions:

The survey is finished now, but at the end, we would really appreciate if you answer the following questions as well; if you would like and also if you have time.

By answering these questions, you will help us more to have reliable and accurate analysis.

42. Which parts of the port or port facilities are more susceptible, and/or more likely to be subject of a terrorist attack, in your point of view?
43. How much the mariners, workers, seafarers, fishermen etc have contributed to adopting the ISPS code in your port?
44. How much the Police, Coast Guard and other security agencies have contributed to adopting the ISPS code in your port?
45. Which opportunities do you think that you have gained or missed by applying the ISPS code?
46. What are the advantages and disadvantages of the ISPS code in your point of view?

Any comment:

8.2 Appendix 2: *The cooperator companies*

The list below shows organizations and ports, which had collaboration in this study by answering the questionnaires and other questions regarding the ISPS code and port security. The list is sorted alphabetically.

1- Åhus Hamn
2- ConocoPhillips Company
3- Copenhagen-Malmö Port (CMP)
4- Hargs Hamn AB
5- Helsinborgs Hamn
6- Höganäs Hamn
7- Kalmar Hamn
8- Karlsborg Hamn (Billerud AB)
9- Landskrona
10- Luleå Hamn
11- Lysekil Hamn
12- Oxelösunds Hamn AB
13- Securitas
14- Stena Line
15- Strömstad Hamn
16- Södertälje Hamn
17- Uddevalla Hamnterminal AB
18- Umeå Hamn AB
19- Vastervik (Swe-Dan Seafood AB)
20- Visby Hamn

8.3 Appendix 3: *Abbreviations*

The abbreviations which have been used in this thesis are sorted below:

CCTV:	Closed Circuit Television
CG:	Contracting Government
CLSCM:	Center for Logistics and Supply Chain Management at Cranfield University, UK
CSI:	Container Security Initiative
CSO:	Company Security Officer
CSR:	Center for Seafarers' Rights
C-TPAT:	Customs-Trade Partnership Against Terrorism
DOS:	Declaration Of Security
EC:	European Community
EU:	European Union
FBI:	Federal Bureau of Investigation
GDP:	Gross Domestic Product
GT:	Gross Tonnage
ICG:	International Crisis Group
ICT:	Information and Communication Technology
IFSMA:	International Federation of Shipmasters' Associations
IMO:	International Maritime Organization
ISM:	International Safety Management
ISO:	International Standards Organization
ISPS:	International Ship and Port facility Security
ISSC:	International Ship Security Certificate
ITIC:	International Transport Intermediaries Club
JIT:	Just In Time
LNG:	Liquefied Natural Gas carrier
LPG:	Liquefied Petroleum Gas carrier
MARPOL:	International convention for the prevention of (Marine) Pollution from ships
MSC:	Maritime Safety Committee
MSIC:	Maritime Security Identification Card
MT:	Metric Tonne
OILPOL:	International convention for the prevention of Pollution of the sea by Oil
OPRC:	International convention on Oil pollution Preparedness, Response and Co-operation
PFSA:	Port Facility Security Assessment

PFSO:	Port Facility Security Officer
PFSP:	Port Facility Security Plan
PPP:	Purchasing Power Parity
RSO:	Recognized Security Organization
SEK:	Swedish Krona
SID:	Seafarers Identity Document
SOLAS:	Safety Of Life At Sea
SSA:	Ship Security Assessment
SSO:	Ship Security Officer
SSP:	Ship Security Plan
TEU:	Twenty feet Equivalent Unit
TNT:	Tri Nitro Toluene
UK:	United Kingdom
ULCC:	Ultra Large Crude Carrier
UN:	United Nations
UNCTAD:	United Nations Conference on Trade And Development
US:	United States
USA:	United States of America
VLCC:	Very Large Crude Carrier
WMD:	Weapon of Mass Destructions