2006

Intermodal shipping : an examination of the security framework with emphasis on container security

Maged Mohamed Abdou
World Maritime University

WORLD MARITIME UNIVERSITY
Malmö, Sweden

THE INTERMODAL SHIPPING: AN EXAMINATION OF THE SECURITY FRAMEWORK WITH EMPHASIS ON CONTAINER SECURITY

By

Maged Mohamed Abdou
Egypt

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

MASTER OF SCIENCE
IN
MARITIME AFFAIRS

(MARITIME SAFETY AND ENVERONMENTAL PROTECTION)

2006

DECLARATION

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

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

(Signature):……

(Date): ……..

Supervised by: Dr. **Jens-Uwe Schröder**
Assistant Professor
World Maritime University

Assessor: **Maximo Q. Mejia Jr.**
Lecturer
Institution: **World Maritime University**

ACKNOWLEDGMENTS

No words could express my honest gratefulness to all the staff of World Maritime University and for their assistance to me during my studies here at this unique educational institute.

I sincerely would like to express my appreciation to Dr. Gamal El Din Mokhtar the President of the Arab Academy for Science & Technology and Maritime Transport (AASTMT), to grant me this unique opportunity to study at WMU. I would also like to thank Captain Samy Abu Samra, the Dean of the Up Grading Studies at the College of Maritime Transport and Technology in AASTMT. Many thanks to Captain Mohy El-Ashmaouy and Dr. Nagy Khayralaa in AASTMT for there continuously supports to me at all times.

I would like to thank the MSEP Faculty of World Maritime University for providing valuable knowledge, which will really progress the safety standards in the maritime field. A special merit to Professor Dr. Proshanto K Mukherjee, for all his magnificent knowledge and support during this study, I would like to tell him that I am really proud to be one of his students at the WMU. Great thanks should be also to Professor Jan Åke Jönsson for all his efforts and brilliant technical knowledge provided during the third semester. Warm thanks to Professor Maximo Q Mejia Jr for his interesting knowledge, especially those related to maritime security issues.

I express genuine thanks to my dissertation supervisor, Professor Dr. Jens-Uwe Schröder, for his extreme support with my research and his proficient in sharing knowledge and supportive materials. I would like to thank him also about his efforts and kindness. Thanks should be to the library staff at WMU, Susan and Cecilia and English lecturers, especially Ms. Inger Battista for their assistance with the research materials and their support to my dissertation.

Finally, I would like to express my deepest warm thanks to my family; my parents, my wife, and my lovely children Ahmed and Jana, for their great motivation of keeping up with me. Thanks to all of you for your efforts, encouragement, and great support.

Title of Dissertation: **The Intermodal Shipping: An Examination of the Security Framework with Emphasis on Container security.**

Degree: **MSc**

Abstract

The dissertation is a study of the current international security regime in the intermodal transportation system. The new trend of the terrorist action by using the transportation unit, gives red warning to address the security weaknesses in the transportation system. Container shipping is very essential intermodal transport for the world economy. The container will pass through different modes of transportation and different security control measures, some of which under the international regime represented in ISPS Code in the maritime transport sector and others under the national security transport regulation for each country.

The main objectives of this study is first to identify the historical background of maritime criminals and national/international assessment of specific risks caused by terrorists using the transportation chain as well as the security weaknesses in the transport system from the point of origin to the final destination; secondly, to examine the effectiveness of the current security measures under the international umbrella to provide ship and port facilities security and the development of the security framework between countries with mutual commercial interests as additional measures to the (ISPS) Code. Then to the benefits and impact of increasing levels of security on a state's economy, shipping actors are examined. The final objective is to provide transport authorities by proper information to make meaningful decisions on the establishment of a proper security framework.

A brief look is taken at current maritime crimes, including the vulnerability of possible terrorist attacks using intermodal transportation facilities or the container itself for

that purposes. The role of transportation authorities´, stakeholders´, decision makers´, and security experts' opinions in the container shipping is discussed.
The concluding chapters provide a decision maker with clear view of current security problems in order to be able to take careful decisions that may improve security and management control through the container transport chain.

KEYWORDS: Intermodal transportation; Assessment; ISPS Compliance; Economic Impacts; Shipping Actors; Container Security; Terrorist; Transportation Authorities.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

AAPA	American Association of Port Authorities
AIS	Automatic Identification system
BIC	Bureau International des Containers
CRS	Congressional Research service
CBP	Customs and Border Protection
CBRN	Chemical, Biological, Radiological and Nuclear
CSI	Container Security Initiative
C-TPAT	Custom Trade Partnership Against Terrorism
ECMT	European Conference of Ministers of Transport
ESC	European Shipper Council
FEU	Forty foot Equivalent Unite
FOCS	Flags of Convenience ships
GDP	Gross Domestic Product
GPS	Global Positioning System
ILO	International Labour Organization
IMB	International Maritime Bureau
IMDG	International Maritime Dangerous Goods
IMO	International Maritime Organization
INTERTANKO	International Association of Independent tankers Owners
ISO	International Standards Organization
ISPS	International Ship and Port Facilities Security
ISS	International Ship Security Certificate
ITF	International Transport Workers' Federation
ITU-R	International Telecommunication Union – Radio-communication
MSC	Maritime Safety Committee
OCR	Optical Character Recognition
OECD	Organization for Economic Development and Development
P&I	Protection and Indemnity
PSC	Port State Control
PSO	Port Security Officer

ROV	Remotely Operated Vehicle
RFID	Radio Frequency Identification Tag
SOLAS	Safety of Life at Sea
STCW	Convention on Standards of Training, Certificates and Watch-keeping for Seafarers, 1978, as amended in 1995
TEU	Twenty-foot Equivalent Unit
UNCTAD	United Nations Conference on Trade and Development
USCG	United States Coast Guard
VTS	Vessel Traffic System
WCO	World Custom Organization

Chapter 1

Introduction

1.1. Scope and objectives

Trade is the lifeblood of every nation and it is the most important medium for the transfer of technology and transportation of goods from one country to another. At the present time, the world is facing a new kind of terrorism and the security of global trade is indispensable to prevent terrorism. The systems and processes involved in the intermodal transport chain, which includes ocean shipping, should be reviewed and analysed in terms of the emerging security regime, particularly in the international maritime field and every effort should be expended to ensure that the shipping and related industries are protected from any kind of terrorist attack.

The events of 11 September 2001 signalled a red warning light pointing to the formidable dangers facing the maritime transportation system, especially the weaknesses in various stages of the transport chain. Since time immemorial, different types of maritime criminal acts have prevailed including theft of goods, drugs and smuggling of cargo, latent targeting of dangerous cargo, piracy and other illegal activities. The shipping industry now faces new types of attacks through the use of transport facilities as weapons against other countries. Millions of packages of hazardous and radioactive materials for the purpose of agriculture, medicine, research and manufacturing are transported annually by ships, especially container vessels, in addition to the huge amount of oil transported by sea. The methodologies used previously in different types of crimes show that the possibility of terrorist acts against shipping and countries by the use of materials described above as well as other kinds of materials also exists.

The reactions of countries have differed widely. The most important response of the international community was the adoption by the International Maritime Organization (IMO) in December 2002 of the International Ship and Port Facility Security (ISPS)

Code to establish a new mechanism for developing minimum standards of security requirements with a strong communication system that has been incorporated as chapter XI-2 to the Safety Of Life At Sea convention (SOLAS). The ISPS Code came into force on 1 July 2004. For State parties to SOLAS, this represents a major defensive tool for their ships, territories and ports.

Some countries such as the USA and certain European countries have enhanced their defensive positions in addition to the ISPS Code to ensure maximum security for their territories. This new strategy implemented in their domestic rules is designed to ensure the safety of cargo from its point and port of origin. The container security initiative proposed by the USA to promote scanning and tracking of containers is a good example of a sound national security framework. However, this framework cannot achieve its aims without the acceptance and cooperation of other countries with mutual commercial interests. Therefore, the World Custom Organization (WCO) is pushing to internationalize this program. It has been accepted by most of the countries that are members of this organization through the signing of a cooperation agreement to implement the framework in their domestic rules.

This agreement gives an indication of further improvement in the maritime security system that may become the international security strategy for ships and port facilities, especially in the container-shipping arena. It is considered to be a vital process for the transportation of dangerous, nuclear and radioactive materials.

Decision makers in each country should be aware of all the aspects of the new security framework in order to deal with it and to make appropriate decisions. They should be able to set a National Security Maritime Transportation Plan for each country by managing the different types of risks to prevent any illegal transportation of weapons or use of ships as vehicles of mass destruction against target countries.

In conclusion, to ensure maximum security for the shipping transportation system a global agreements is needed to the international security frame work by effective implementation of the ISPS Code and providing advanced security measures by

studying the national framework that may help the decision-maker to improve the security standards for each country which help improve international maritime security against any kind of terrorism attacks.

The objectives of this study are:

- to identify the historical background of maritime criminal and national/international assessment of specific risks caused by terrorists using the transportation chain,
- to identify security weaknesses in the transport system from the point of origin to the final destination,
- to examine the effectiveness of the current security measures under the international umbrella to provide ship and port facilities security,
- to examine the development of the security framework between countries with mutual commercial interests as additional measures to the (ISPS) Code,
- to examine the benefits and impact of increasing levels of security on a state's economy, shipping companies and the customer,
- to facilitate transport authorities to make meaningful decisions on the establishment of a proper security framework.

The research focuses on these objectives and is based on analysing the status of the international transport framework. It highlights container security issues and their potential impact, and seeks to determine the appropriate methodology to ensure maximum security for the shipping transport chain, as well as the possibility to introduce this framework in the current regime. The findings of the research will provide a comprehensive overview of security for the transport authorities and decision-makers, which will help them, take sound decisions.

1.2. Intermodal transportation and terrorist threats

Intermodal transportation is a system using two or more transport modes during a single journey and container transportation is a typical example for that system. The system covers all transportation requirements from the point of origin to the final destination. This requirement includes documentation process, transportation

facilities, customs procedures, safety standards, and security measures. However, security of the intermodal transportation chain is extremely difficult because the system is complex and not covered by a single transport framework. In case of container transport, while the outer edges (land or inland water way) are cover by domestic rules of both the export and import countries, the maritime sector (ports, ships, shippers, shipping companies) is covered by international regime through IMO codes and conventions. Therefore, a discussion through this study will be carried out to examine the availability to cover the intermodal transportation system in terms of container transportation against terrorist attacks.

Transport systems have become a potential target of terrorist attacks. This was shown on September 11, 2001 in the USA and further highlighted by the rail and public transport bombing in Moscow and Madrid. Then it tremendously increased in July 7, 2005 in another public transport bombing in London during the rush hour (Sweet, 2006). According to latest news form Scotland Yard that 21 persons are arrested at Heathrow Airport in London, on August 10, 2006, were planning to blow up as many as 10 jets leaving Britain to the U.S (Scotland Yard, 2006). Considering these crises against the industrialized world, ensuring that supply chain is not used to transport terrorist goods, as weapon of mass destruction is a matter of security measures.

Some incidents give red warning for the vulnerability of terrorist attacks against the shipping industry. In Panguil Bay 2000, the bombing on board the Ro-Ro ferry *Our Lady of Mediatrix* caused death of 40 and injury of 50 people. The same year, another 19 people died and 37 were hurt in the bombing of the American warship *Cole.* In October 2002 a new attack in the Gulf of Aden by bombing the oil tanker *Limburg* resulted in the death of one person on board and 90,000 barrels polluting the sea. The aim of terrorists is to cause death and destruction of the human lives, the environment, and commerce (Mukherjee & Mejia, 2003). This crisis gives an indication of the great challenges facing governments, particularly the transportation authority to protect their territories against those criminals. Actions should be taken to design a security framework and ensure maximum protection to the transport modes.

In the maritime sector “What September 11 has done is to intensity focus on this issue and present the IMO with the challenge of deterring perceived threat to maritime security through proactive measures and new instruments” (Mejia, 2002, p.27). However, intermodal system is not only maritime transport, but also include other modes of transport inside the countries´ territories. Therefore, another proactive measure should be taken by the United Nations to cover the gaps of the intermodal transportation system that may appear in the outer edges of the system.

1.3. The role of the transportation authorities

Intermodal transportation is a hybrid system connecting different modes of freight transport. Transportation authorities´ role inflate from their responsibility for providing a safety environment to those people living in the country or using the entire public transport system. Further, the authorities’ responsibilities extend to promoting the nation’s benefit, enhancing national security, and protecting public interests. While governmental authorities are involved in setting the rules and regulations, some sectors within the transportation modes are operate by private entities (Sweet, 2005. p.9).

For example, the private industry owns and operates a huge portion of the transportation system, such as pipeline companies, railroad companies, passenger air carriers, and motor carriers for freight and passenger. Moreover, the local governments are owned and operate the transportation infrastructure within each state, such as highways, transit systems, and local airports. So, they implement regulations for different sectors of the transportation system and provide security services in their area of transport. The federal governments include the ministry of transport responsible for setting standards, issuing regulations, establishing policies, and managing financial targets, such as taxes and budgets for the different modes of transportation (United States General Accounting Office, GAO, 2003). Therefore, to ensure an integrated security system through national territory, cooperation must take place between the government and the private industry to continually re-evaluate security measures.

The ministry of transport is the national government's agency, which is concerned with all intermodal transport problems including security issues for various reasons. Ministries are among those first responding authorities to the crises; they are the authorized entity for the transport regulatory oversight and licensing of transport companies, operators, and vehicles. They also govern the carries´ rules of transport fright and passenger, and they play an important role in improving information technology, which is the key of transparency and communication of information among different modes and different actors in the transportation chain (OECD, 2005, p.21).

The government regulations are the key issue that could affect the efficiency of the domestic and international transportation system. These regulations may affect the requirements for tightening security measures, distribution and expanding of populations, improving the industry, enlarging urban centres, and changing capacities and requesting of various modes of transportation. However, recently some unavoidable factors may affect the role of governments to set or deregulate their system, such as the current terrorist attacks by using transportation facilities which requires all the nation's authorities to continue accurate assessment of the threats (Sweet, 2005, p.9).

1.4. Structure and organization

This discussion will begin with vulnerability of intermodal transportation in terms of the container industry using risk management assessment and relevant scenario to identify the gaps through the various modes of transportation. The assessment will include the effect of the decision makers to cover the gaps, weaknesses identification on the outer edges (land & inland waterway), and the maritime sector including port area, ships, and shipping actors. Examination of the effectiveness of the ISPS Code to cover these gaps will be carried out.

Then, the current initiatives and responses, which have already been taken over the last few years will be introduced and their approach to the overall solution from the

technological point of view, will be described. Examination of the effectiveness of the new security measures to cover the gaps in the container transportation and the possibility to emerge these initiatives in the international regime will be introduced.

Finally, there will be a study of economic consideration to implement the different security measures including ISPS Code and container initiatives. A cost benefit analysis and a possible answer to the question, “Who will pay for this security?” will be introduced. The study will include the economic impacts for certain countries such as the developing countries and shipping actors due to these new measures.

Chapter 2

Shipping transportation across modes

2.1. Introduction

The study through this chapter provides an inclusive examination of the intermodal security framework for different types of transportation with emphasis on the container transportation chain through risk assessment of each mode to identify where the vulnerabilities estimated along the supply chain including the effectiveness of the only current international regime, the ISPS Code, to cover the security of maritime sector.

The most tangible chain from a security point of view is the substantial movement of freight from point to point and from one mode to another. Intermodal Transportation Network is a logistically linked system using two or more transport modes with a single rate. Modes are having common handling characteristics, permitting freight (or people) to be transferred between modes during a movement between an origin and a destination. In other words and according to the Merriam Webster Dictionary the system is defined as “Being or involving transportation by more than one form of carriers during the single journey” (Merriam Webster Dictionary, 2005). The essence of efficient intermodal transport is to choose the most suitable modes to achieve operational and cost effective delivery of cargo, putting into consideration the frequently of the service, availability of facilities, presence of other alternatives, speed of delivery and security consideration (Lowe, 2005, p 1).

The container transport system is a typically intermodal system, which is carried by maritime and inland waterway, road and rail operators. This system could provide high safety and efficient delivery of global goods transport through different modes. The significance of the containerization basis on that small steel box could carry all different types of cargo including gas, liquid, chemical, reefer, and dangerous goods in package form and bulk cargo. The containers are not limited to use inside the

transportation modes but can also be found anywhere from major ports and cities to small side streets. However, it is very difficult to address security of the container transport chain because a single transport framework does not cover the system. The different interests of industrial operators, which affect the security level from one node to another, affect the system infrastructure.

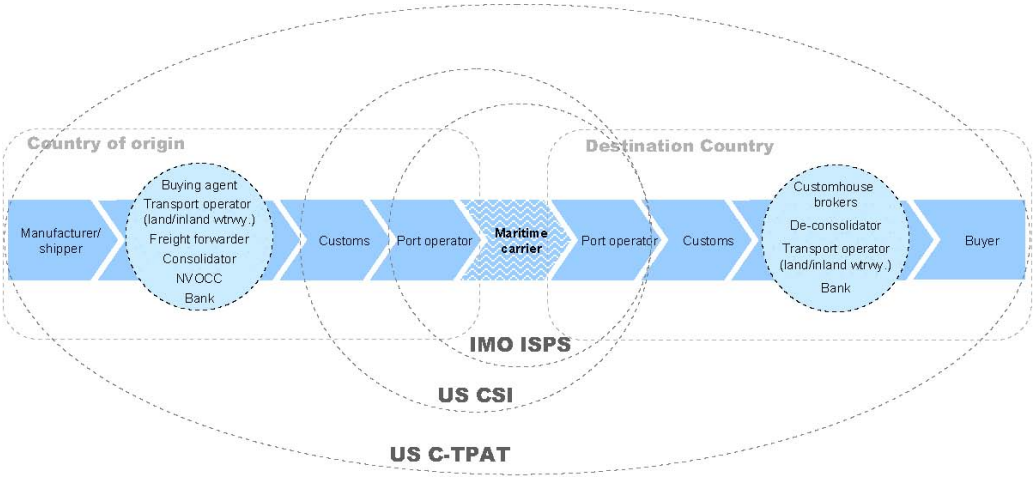

Figure 1: security coverage for intermodal transportation chain. (Source OECD, 2003, p. 50)

A comprehensive security intermodal framework is required to secure the container transport chain from the point of origin to the point of destination. Whereas the central part of the system is covered in ports and the maritime transport sector by an international security framework which exists through the International Ship and Port Facility Security Code (ISPS) which entered into force on 1 July 2004 as Chapter XI-2 of the SOLAS Convention, the outer edges of the chain such as land and inland waterways are not yet covered by an equivalent framework except some individual efforts from some countries to conclude cooperation agreements to cover some elements of the security breaches in those areas such as the Container Security Initiatives (CSI) by the USA, container stuffing and seal management guidelines by World Custom Organization (WCO), EU Freight Security Directive and some other initiatives which will be covered in details in the next chapter of this study (Organization for Economic Co-operation and Development(OECD), 2005, p. 12).

The risk of security breaches at any point of the transportation links will affect all the other links of the intermodal transportation chain. The level of security varies from point to point and from one mode to another, and also from country to country. One should estimate the risks associated with all cargo types, especially cargo which is vulnerable by nature such as the container, which is being used to deliver Chemical, Biological, Radiological and Nuclear (CBRN) weapons. International action to strengthen the security of the container transport chain is actually needed. It is also important to increase awareness of how to identify the weaknesses and cover the gaps in and between the transportation modes where terrorists may act (OECD, 2003).

2.2. General Background of Container Intermodalism

Containerization permits the mechanized handling of cargoes of varied types and dimensions that are placed into boxes of standard dimensions. The International Standards Organization (ISO) in reference sizes standardizes the dimensions of the containers. One of the major sizes is Twenty-foot Equivalent Unit (TEU) with dimensions of 20 feet long, 8 feet high and 8 feet wide, and with a permissible load of 22 tons. The other major size is the Forty-foot Equivalent unit with dimensions of 40 feet long, 8 feet high and 8 feet wide, and with a permissible load of 32 tons. In this way goods that might have taken days to be loaded or unloaded from a ship or other transportation mode can now be handled in a matter of minutes. The maritime fleet are now exceeding the number of 2700 modular container ships and the emergence of a global network of several hundred highly automated port handling facilities (OECD, 2005, p. 24).

Each year about 2 million TEUs worth of containers are manufactured that may make the number of the global containers 21 million TEUs in 2005. The use of containers shows the integration between freight transportation modes by offering a higher fluidity to cargo movements and standardization of loads (Rodrigue, et.al, 2004). The Bureau International des Containers (BIC) indicates that about 15 million TEUs were circulated world wide in 2002. The world shipping council indicates that 17 million TEUs were circulated in 2003. These figures indicate the huge volume of

container movements around the world and it is expected to increase in the coming years as world trade increases (OECD, 2005, p.24). The security of the container transportation chain is a matter of importance due to its popularity and its great importance to the world trade system.

2.3. Capability of the Global Container Supply Chain

The ability of the supply chain to successful deliver cargo depends on its efficiency and security level, which is represented by five capabilities:

- **Efficiency**. The container intermodal system has the exclusive advantage of its ability to deliver goods faster and cheaper than any other types of transportation, taking into consideration the value of the cargo in terms of its weight and volume.
- **Shipment reliability**. The system should provide the minimum amount of cargo loss by theft or accidents due to the high level of protection inside this steel box.
- **Shipment transparency**. The goods transported through the system should be legitimately represented to authorities and pass through a legal and authorized regime which prevents any kind of illegal transportation.
- **Fault tolerance**. The system should be able to react to disturbance and failures by isolating the damaged part without any further fatigue in the entire system.
- **Resilience**. The system should be able and designed to go back quickly to normal operating conditions after any loss or damage to one or more of its mechanisms.

The first three of these capabilities are functions of the container shipping system. The final two, resilience and tolerance, are system properties which react with normal or international turbulence.

While all these capabilities are interconnected together, they need to be evaluated through different metric measures. Gains or losses in any one capability must be assessed against the result of gains or losses in the others. The efficiency,

capability and security of the system may be achieved under normal circumstances and normal operation conditions, but this will be in conflict with the emergency situation, especially with such kind of loss of life or unprepared emergency responding plan for the different modes. For instance, security and investment will be against each other in terms of increasing inspection, which may improve security, level but increases time delay in ports. This requires the decision maker to design the security policy and technology with respect to those capabilities to avoid conflict (Willis & Ortiz, 2004, p. 16).

2.4. The Transport Security Risks

The efficient assessment of the transport security risks is based on the identification and assessment of a full range of foreseen possible terrorist intervention scenarios. The security risk is based on the possibility of a transportation crime including terrorism compared to its level of protection and the consequences of a successful attack including the level of fatalities and economic impact. The transport security risks may be categorized into two main types.

- Infrastructure risks, which are one aim of the terrorists to disturb and destroy, e.g., the transportation supplies chain risks. Many areas are considered as high risks and are directly linked to a transport element which the terrorists may target such as rail/road tunnels or bridges, rail/ road/ ports terminals, waterways and ships locks.
- Supply chain risks. The other aim of terrorist is to use the supply chain to transport their illegal weapons or use it as a weapon of mass destruction to create fatigue in the entire country infrastructure. The cargo on the transport units will pass through key areas such as industrial locations and heavily populated areas. During this trip, it is an easy task for the terrorists to locate any kind of destruction weapon adjusted by timer to destroy the transport unit, create losses in human lives and affect the country's economy. Further damage will be tremendously high if the cargo is dangerous such as toxic chemicals and any flammable gases or liquids (Mackenbach & Coolen, 2005, p. 2).

More specific, these types of risk analysis have limitations when dealing with terrorism. A common approach to dealing with this type of uncertainty problem is to seek out situations of vulnerability and develop scenarios that can reduce this vulnerability or that may provide flexibility if there are attacks on vulnerable points. Containers, for example, would seem to be a vulnerable link in the security network because of their number, nature and continual movement, although they have not yet been used as a means of attack. Reducing this vulnerability is a matter of expectation and a significant degree of subjectivity and 'expert opinion' is certainly involved to create possible scenarios to the threat, which may help the transportation authority to adapt security measures (Brooks & Button, 2006, p. 100).

2.5. Fundamental Container Risk Measures

According to the opinion of the experts of the European Conference of Ministers and Transport in an OECD report in 2005, there are two approaches to specify security measures for the container transport chain. The first is “hijack scenario” which shows the possibility of terrorists to intercept a legitimate consignment and tamper with it. The second is “Trojan horse scenario” which assumes and/or develops a legal trading identity to load an illegal and dangerous shipment.

These techniques were earlier used by criminals to smuggle drugs, illegal imports and for criminal purposes while they can now also be used as potential “modus operandi” of terrorists with more organized methods whereby they can access the container without leaving visible traces as expert criminals. Their first priority is to ensure that their illegal consignment gets to the final consignee unnoticed and untouched while they are interested in removing the contents of the container in such way to avoid, or at least delay, discovery of their action.

2.5.1 Container Hijack

Hijacking the container is insertion or placement of an illegal consignment within a container by targeting a legitimate container and accessing its contents at any security weak step during its voyage and hides the illegal consignment inside, and

then they re-seal and re-insert it back into the legitimate trade flow. This way is used without the knowledge of all the responsible parties in the container transport chain.

When the freight is placed on trucks or trains, for various periods of time and moves to ports to be shipped on board vessels, it will pass through different traffic conditions in which it is within the capacity of terrorist organizations to insert a mass of smaller explosives in the supply chain or in the cargo itself. For example, if a container is loaded with some kind of bagged cargo, it will be stowed inside the container on pallets, so breaking the seal and hiding the explosives between the bags and returning the seal again to the original condition could access the contents of the container. This will be easy when the cargo is not moving at the transfer points such as loading and storage facilities. Randomly, the explosions may occur at industrial areas, population areas, dense traffic, critical infrastructures, transfer points, and distribution centres. Furthermore, the supply chain will grind to a halt to allow inspection of all cargo (Mackenbach & Coolen, 2005, p. 34).

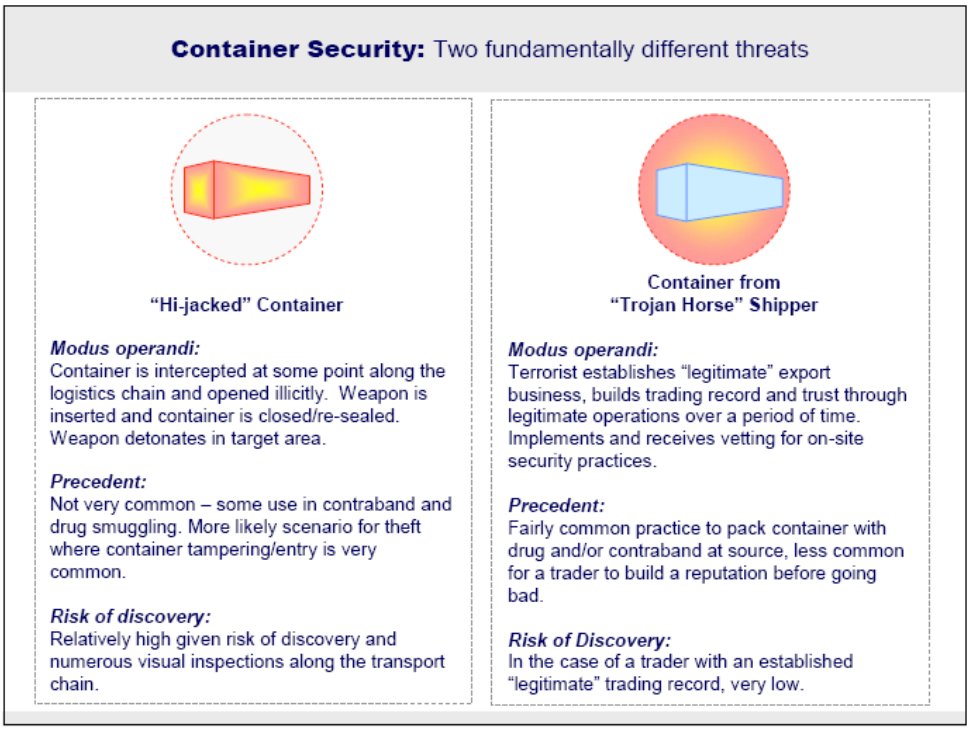

Figure 2: The two fundamentally possible scenarios to use container in terrorist threat. (Source: OECD, 2005 (container transport security across modes)

2.5.2 “Trojan Horse Scenario”

The Trojan horse is the second technique used by terrorist organizations, which depend on setting up or purchasing staffing inside the legitimate trading companies that allow the criminals to achieve their illegal purpose through the normal trade patterns. Those stuffing may belong to cargo warehouses, managers, forwarders and even Customs. The buyer may also involve this scenario as a part of a hiding terrorist organization or work belonging to “Trojan horse” shippers. The expert terrorists consider this way as more effective than “hijacking container” perhaps because it is easier and more-cost effective to use the knowledgeable staff involved the transportation chain than to use their skills (OECD, 2005).

Generally, it is very difficult to know whether the targeted container is “hijacked” or “Trojan horse”, but after September 11 when the world started to take additional security measures especially in the supply chain the most possible method to use by terrorists is “Trojan horse”. For example, the Chief Security Officer at Hutchison Port in the USA, which is considered one of the largest container terminals in the world (it handled 42 million containers from 35 ports in 2003) said, “Each of the 42 million containers that went through our facilities around the globe was a Trojan Horse. We don’t have the ability to truly know if the containers have been tampered with”. He stated that the modern society is greatly dependent on the efficient, reliable and cost-effective movement of goods through this supply chain, and it’s clear that the risks involved in securing the goods are huge (Gilbert, 2005, p. 3).

2.6. Stowaways and the Effectiveness of the ISPS Code

Illegal immigration or stowaways are a major international problem, which represents the security breaches and fatigues in the implementation of the ISPS code in many countries, especially those countries suffering from political or economic problems. With the significant awareness of international port security after the terrorist attacks of September 11, 2001. IMO defined a stowaway as, “a person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the ship owner or the master or by any other

responsible person and who is detected on board after the ship has sailed, and is declared as a stowaway by the master to the appropriate authorities" (Ref, IMO DOC. FAL 29/4) The problem is that some of those stowaways pose criminal elements such as trading in illegal drugs or supporting other criminals to facilitate the movement of illegal materials related to terrorist organizations.

Table 1: Stowaways cases reports, ships involved in stowaways' incident. (Source: www.intertanko.com)

	2003	2004
Flag	Number of cases	Number of cases
Algeria	1	0
Antigua and Barbuda	7	0
Bahamas	31	19
China	0	1
Croada	1	0
Cypois	25	20
Denmark	22	2
Egypl	1	1
Estonia	1	0
France	2	1
Germany	4	1
Greece	4	3
Hong Kong, China	5	3
llaly	7	4
Liberta	25	15
Luxembourg	1	0
Malla	3	3
Marshall Islands	1	0
Morocco	2	0
Netherlands	2	2
Netheriands, Antilles	10	2
Norway	5	3
Panamá	10	11
Portugal	1	0
Saint Vincent and the Grenadines	2	2
Singapore	1	0
Spain	0	1
Sweden	2	1
Switzerland	1	
Turkey	3	1
United Kingdom	2	0
United Kingdom (Bemnuda)	0	1
United Kingdom (Isle of Man)	1	1
Total	183	98

Regarding the volume of stowaways problem, the statistics prepared by INTERTANKO according to IMO reports show that the incidents during 2003 and 2004 related to the total number of the stowaways decreased from 183 cases in 2003 to 98 cases in 2004, which represents the starting point of the effective additional security measures taken directly after the ISPS Code came into force owing to strict accessibility into the port area and the proper implementation of measures on board vessels. For example, table 1 shows the number of stowaways on board vessels flying Denmark flag decreased tremendously from 22 cases in 2003 to only 2 cases in 2004, while the number of stowaways remained the same or increased in percentage on board the vessels flying Panama, Liberia, Cyprus and Bahamas flags. Most of the embarkation into vessels in 2004 was in West Africa: 56%, also the Mediterranean, black sea and North Sea: 34%. Most of these cases are reported in container, general cargo and RORO vessels, but the number is decreasing in container and general cargo while it is increasing in RORO vessels (INTERTANKO, 2005).

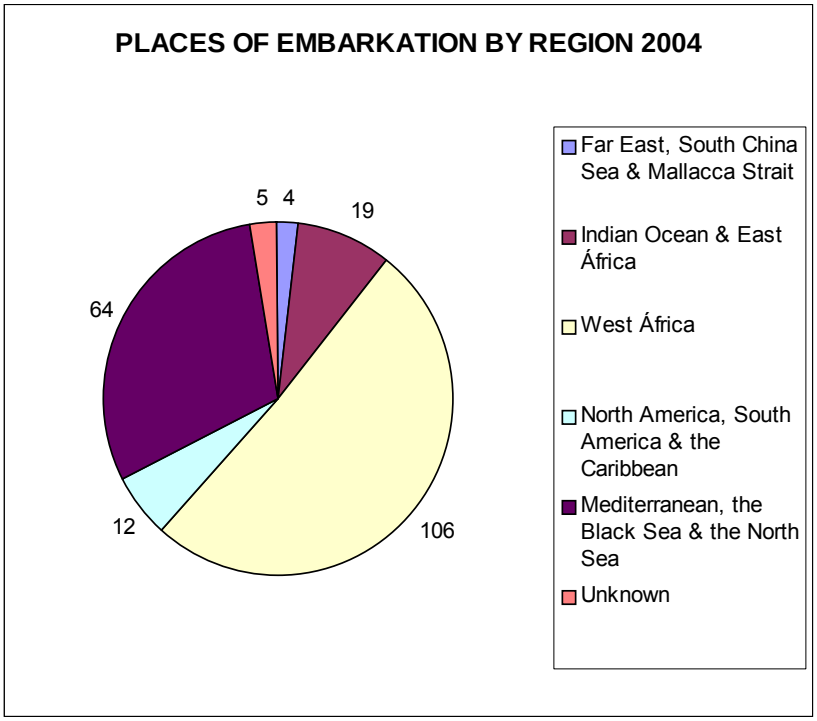

Figure 3: places of stowaways' embarkation vessels by region in 2004.

(Source: www.intertanko.com)

Another example comes to the screen when the Associated Press news agency in USA announced on the fifth of April, 2006, that twenty two persons including four women expected to be Chinese were taken in custody after they apparently let themselves out of a 40-foot container that had been used to smuggle them from China on board container vessel *Rotterdam*. The container was loaded in Shanghai and stayed on board for 15 days before it was discharged in Seattle Port in the USA and stowed in the storage terminal area where the security guards found some of the stowaways out of the container. The spokesman for U.S Customs and Border Protection, Michael Milne, said that "this container had been flagged for special examination, but the examination had not been conducted before the group was caught" (KUTV, News, 2006).

Recognition of the stowaways' problem gives great awareness of the terrorist problem due to the accessibility to the port area and weak implementation of the ISPS Code. The stowaways have a great impact on the ship-owner once they are discovered on board and the master announces that. The vessel will face a lot of problems when entering any port, which may delay the vessel and have an adverse economic impact on the ship-owner or the charterer. Additionally this vessel will be considered not compiling with the requirements of the ISPS Code and will be subjected to further inspection and further security control measures. However, the ship-owner blames the port authority that his vessels are not safe while berthing and that those illegal immigrant persons were able to access the port through the port borders.

"Regardless of the efforts made by ship-owners to control access to their vessels in port, the task of securing port facilities is a much more complex operation and one which many ports will find difficult to achieve", says risk-management executive Tony Baker in North of England P&I. He also added that "North of England points out that despite the introduction of IMO guidelines on prevention of stowaways in the 2002 amendments to the Convention on Facilitation of Maritime Traffic (FAL Convention), port security in many parts of the world remains extremely lax. 'It remains to be seen whether the ISPS Code will improve the situation". More security measures and more effective implementation of the ISPS Code, cooperation and communication between governments, ports and the shipping

industry are important. Strict access to port facilities, containers and ships is essential (North of England P&I Club, 2004).

2.7. Transportation Authority assessment

The national governments normally hold the overall security policy for the transportation chain. At the same time, regional and local authorities promote a significant responsibility of the transport infrastructure such as railroad, inland waterways, motorways and ports. Clear definition of the role and responsibilities at all levels in the government is essential to avoid any conflict and to respond effectively and efficiently to crisis situations and ensure maximum protection from terrorist activity across transportation modes (OECD, 2004, P. 51).

The intermodal transport system is integrated. Danger occurs when the transport unit moves from one place to another, which makes security complicated because any weaknesses of the security level in one mode will affect all the other links and the risk may transfer from the weak node to the other nodes. Therefore, if there is any security concern relating to the use of maritime shipping, they should also be common to all other modes and any authorized persons will take the decision in each responsible organization. Many of the breaches in the security level will start from the top manager and they are common for all the modes.

The main feature of intermodal land and maritime transportation is that the system is open to the users. Any person can access the system to know some information about passenger trip schedules and places to go to or get information about schedules of vessels' arrivals at ports; one may also get information about the type of cargo on board those vessels, discharging sequence, and storage area position located in port. The documentation system, such as bill of lading or cargo manifest or passenger list, should be secure. The Internet and announced media as well make it easy to help the costumers know every thing about their cargo or passengers' relatives. However, this is also against the security measures because the terrorist groups could use this information also to plan for attacking this infrastructure. Meanwhile, the additional security measures to restrict the flow of this

information or passenger and cargo movement may create commercial impact on the operators and bad consequences for the customers (United States General Accounting Office (GAO), 2003).

The transportation chain is interconnected through various means of transportation facilities including railways, trucking, buses, barges and seagoing ships. All modes work in harmony to facilitate the movement of billions of passengers and million tons of freight beyond the countries borders. This kind of complex connection and size makes this intermodal system difficult to be adequately secured. At the same time, the meeting of all modes in one place, such as ports, makes ports potential targets for terrorist attacks due to the presence of passengers, employers, equipment and cargo which may contain some kind of hazardous materials such as biological, nuclear, and radioactive substances (GAO, 2003).

Additionally, the difficulty to secure the system may increase in terms of the decision maker level when the system is divided into public and private transportation operators. The tremendous difference of the stakeholders' interests will affect the security decision, where some operators carry passengers only, others carry freight only and others carry both. There are stakeholders who represent the government and others who are individuals. A number of operators invest millions of dollars, and others invest limited sums but their deficiencies will affect the security of the system (GAO, 2003).

The conflict of the stakeholders' interests may create some kind of security weaknesses when some parties try to implement the safety standards and others try to implement the security measures. For example, the International Maritime Dangerous Goods (IMDG) Code requires shippers to fasten placards on every side of the container to show the nature of danger inside this container during the transportation period. This will be against the security measures, which may make this container an attractive target for the terrorists.

Since the transportation modes depend on one other, the deficiency of the security system in one mode will affect the other modes. For example, if a box or container

containing weapons of mass destruction is discharged from one vessel in port to a train or truck, and this train or truck moves outside the port area, then explosion will happen. This will affect all the railway or highway systems as a result of a deficiency in the maritime mode (GAO, 2003).

Other points of weakness could arise when an accident occurs in the train or truck within the port area where the security regulations will be under the supervision of two or more of the government departments such as coastguard, land transportation authorities and port authority. Confusion may affect the law enforcement bodies where every party moves forward to enforce security measures.

2.8. Outer Edges Assessment through Intermodal Network

The outer edges of the intermodal system lie in two different countries where there are different security regulations to control the movement of goods. At the first point, millions of shippers introduce the service for thousands of intermediaries to organize and ship their cargoes to hundreds of ports through maritime carriers. At the other end, the system works in the opposite way gradually moving towards great messy networks where millions of receivers deliver their cargoes. With every step the flow of cargo, especially containers, becomes denser and the overall visibility of the system becomes greater (OECD, 2005, p. 25).

In addition, the international regime will be applied by all the country members of the IMO and who implement the ISPS Code. The weaknesses here come from those countries, which did not ratify the Code or did not implement the system into their national legislation in a good manner. The transportation unit passing from the land or inland waterway area which has security breaches to the port area will decrease the effectiveness of the ISPS Code to secure the port and ships, especially with the container that is normally loaded and sealed in the land sector before it reaches the port area.

The supply chain is a potential target to terrorist attacks while the railroads and trucking system become the principal means of domestic and international

transportation to many nations. They have great commercial importance to the landlocked countries, which are the main connection between them, and maritime countries to transfer their cargoes by sea. The high-speed trains provide transportation time equal to flight time, particularly in Europe and Japan. Railroads and trucks must participate with maritime shipping which is considered the effective means of land transportation to bulk cargo such as coal and grain, ore, and chemical in bulk form such as sulphur and phosphate; and some cargoes which are sensitive to the rain water such as hazardous materials which become dangerous when wet and most of the steel products (Sweet, 2006, pp. 23 - 24).

The container point of origin is a shipper premises where the container will be stuffed and sealed. The cargo after stuffed inside the container become only information on the paper prepared by the shipper and transmitted to all concerning parties. Consequently, the other parties such as land or ocean carriers have there knowledge about the container contents only from this paper which called cargo manifest. Accordingly, if there is possibility to interfere the container contents, as *Trojan horse,* it will be during packaging time and then the container will continue its legitimate journey without discovery to what are its real contents. Security of the container will also start from shipper point through sealing and tracking system, which it will discuss far and wide in the next chapter. Therefore, shippers or other parties packing a container are the most important link in the container security chain.

2.9. Maritime sector assessment

2.9.1. Why Is the Maritime Sector a Target for the Terrorist Attacks?

Shipping remains the main mode of transportation. The port facilities and maritime infrastructure play an important role in trade and economy for each country by providing profits from the maritime investment, tax revenues, jobs, and providing supplies to the other industries. The maritime industry is a rich area in nature for several criminal acts starting from the old piracy and cargo theft in the seventeenth century up to the currently probable use of maritime shipping for smuggling illegal cargo or using the ship itself as a weapon of mass destruction.

The maritime industry infrastructure depends on the construction, maintenance, and use of ports and canals worldwide. Ports are a vital part of the industry which consists of two main components: port facilities including cargo handling equipment, reception facilities, warehousing and terminals and harbour work including pilot activities and vessel reception / departure procedures. All commodities, including petroleum, chemical, biological and raw materials, which are necessary for medicines, technology and heavy industry, pass through this gate (Sweet, 2006, pp. 30-32).

The canals are also vital to the world economy, for example the Suez Canal connecting the trade between the east and west part of the world. The world countries faced economic crises from 1976 to 1973 when the Suez Canal was closed to navigation for about sex years due to the war between Egypt and Israel. Nowadays a vessel of 150,000 displacements and a draft up to 16 meters could transit the canal. The maintenance operations carried out every day will allow vessels of draft up 22 meters to transit the Canal in 2010. The Suez Canal authority reported that 17,224 vessels passed the Canal during 2003, which is more than 8% of the world shipping fleet (Suez Canal authority, 2006). Another vital canal is the Panama Canal, which connects the Pacific Ocean with the Atlantic Ocean. The size of the vessels, which pass the canal, is called Panamax, which is around 65,000 tons displacements and with a maximum draft of 12 meters. The passage time is about 9 hours and 14,011 vessels passed the canal during 2005 (Panama Canal Authority, 2006).

2.9.2. Port Assessment

Ports are sea gates and vital to the economic health of each maritime country that is considered one of the main parts in the intermodal transportation system. World ports vary in size and complexity and use a mixture of modes of transportation. The port area is an attractive target for terrorist attacks. The estimated economic consequences of a successful attack and the resulting shutdown of this system cost billions of dollars. In April 2004, a fast boat filled with explosives attacked the Iraqi oil terminal at Basra despite the forceful U.S. security presence. Another example, in

May 2004, terrorists fired on workers at the Saudi petrochemical terminal on the Red Sea. Other attacks against maritime infrastructure occurred in Nigeria, Colombia and Yemen (Poulin, 2005, p.3).

In the port area, there are different types of cargo and passenger terminals, chemical factories, oil refineries, power plants; dangerous cargo stowage areas and other important facilities often located in port areas which add another set of possible targets. The port is a central part in the intermodal transportation system where concentrations of cargo and passengers flow and meet at different types of transportation points such as container terminals, where containers are transferred between ships and railroad cars or trucks to move inside and outside the port area as fast as possible. Roads and railroads crisscross many ports, allowing access by land as well as by water. The number of people working in or travelling through ports is in the billions. Port facilities are also used to ship military cargo to support nations during wartime. Different types of vessels sail in and out ranging from oil tankers and freighters to tugboats, pilot boats and passenger ferries. This huge investment in, and structure of, the ports may increase vulnerability of the risk factors based on terrorist attacks against any maritime countries (GAO, 2005, p. 22).

Sometimes the container area in the port is classified as a special area due to its sensitivity for handling operations, which depends on fast movement of the container to minimize its time in port. At the same time, international minimum standards for containers terminal security should be established. Ensuring proper sealing of the container is important to protect the container from unauthorized access while in port or in a storage facility and ensure that access is restricted only to authorized personnel and vehicles. In areas where containers are stored temporarily, waiting for shipment or transit, attention must be given to adequate fencing, lighting, and access control points. Sufficient numbers of well-trained security personnel are needed to carry out routine monitoring and inspections of container shipment (Binnendijk, et. al, 2002).

The effectiveness of implementing the International Ship and Port Facilities Security (ISPS) Code will affect the level of protection in the ports and on board vessels,

which may prevent the transfer of risk from one country to another by sea. The ISPS Code introduces to the authorities the basic ways of protecting the port area such as implementing the security plans for each port recognizing the nature of the operation inside the ports because the risks in one port are different from the risks in another. For example, ports that support passenger ferries and container cargo may be exposed to different risks than ports that primarily support bulk cargo. The plan must also be able to control access to areas containing dangerous goods or hazardous substances and restrict access to terminal areas to control access onboard as well such as bridges or other control stations critical to the vessels' operation (GAO, 2005, p. 22).

However, there is a strong argument whether the ISPS Code is enough to protect the maritime sector or not and if it is so, is everything running well to ensure effective results from the system? The answer to the first question is already valid because the ISPS is not a "cure-all" for the security aliments of the maritime sector, but it is a starting point to show the right way and put the entire industry in the same direction. The benefit of the international regulations, which control any system, is that the entire world will be able to understand the requirements for each country and it is easy to find from where the deficiencies started. The answer to the second question is considered the principle of the security aim through the ISPS Code. The facts indicate that up till now the system is not able to achieve the security for the maritime industry. This is because many countries do not comply with the regulations inside the port area or on board ships, which makes a weak point in the system as is clear from the practices of stowaways, pirates and cargo thieves up till now (Billings, 2006, p. 32).

In the USA, the national security strategy takes action through the Department of Homeland Security to undertake foreign port assessments and the U.S. Coast Guard will be responsible for this function according to its "International Port Security Program" objective. This objective is to open discussion with trading nations around the world to exchange information and share the best practices to align a port security program through the implementation of the ISPS code and other international security standards. The aim of the USA of improving the security in the

foreign port is to ensure early alarm as soon as possible in the origin ports to any danger which may threaten its ports from the visiting ships (Goulielmos & Anastasakos, 2005). The plan is to assess the ports of 135 countries that have commercial interests with the USA. The Coast Guards began conducting assessments in 2004 to review about 35 ports a year. The vessels coming from non-complying ports will not be accepted to visit any of the U.S ports or approach its territorial waters (Subcommittee on Coast Guard and Maritime Transportation, 2005).

2.9.3. Ship assessment

Ships are the most important point for maritime transportation security system. The vessels may be used to transfer dangers to any country through cargo or to be used as a weapon in a terrorist strike just as the scenario of aircrafts in September 11, 2001 against the world trade centre in the USA. For instance, the vessels may be used against the population by creating chemical or poisoning pollution near the beaches or create explosions in the population centres adjacent to the port area or damage the port facilities themselves. The terrorists may also sink the vessels to block the harbour entrance and/or shipping channels. The existence of piracy and armed robbery against ships, phantom ships, illegal migrants and stowaways indicates the existence of security weakness due to improper implementation of the ISPS Code on board the vessels.

The studies made by the International Transport Workers' Federation (ITF) show that although the code increased the level of security on board vessels and in port areas, the number of armed attacks had not been reduced after the code came into force in 2004 and most of the attacks were on the vessels in ports or at anchorage areas, which means that some vessels and ports still do not comply with the security requirements. For example, the reporting of attacks rose approximately by 8% in the first quarter of 2006 (61 attacks) when compared with the same period in 2005 (56 attacks) (International Maritime Bureau (IMB), Piracy reporting centre, 2006).

The economic consideration for the ship owners to decrease operations costs is an important barrier in security implementation. Decreased number of crew and

increased fraudulent certificates between officers indicates improper training and substandard of security measures as well. That substandard crew are not being able to cover the requirements of the ISPS Code. Another barrier is that some Flag States are clearly failing in their responsibility to maintain safe manning on board their vessels as required by the International Convention on Standards of Training, Certificates and Watch-keeping (STCW). The ITF survey for the 165,000 seafarers' from Turkish, Greek, Ukrainian, Indonesian, Chinese, Filipino, Latin America, Polish and Croatia results indicate that 96% said "there had been no increase in crew levels to cope with additional workload required by the code", especially with the vessels operating in short voyage, "it has become impossible to perform the requested clerical duties together with the normal duties diligently, efficiently and consciously" (Jump, 2006, p. 13).

The control mechanism for ships to ensure the effective implementation of the ISPS Code is a subject for Port State Control (PSC). Control is the process of monitoring activities to ensure that they are being accomplished as planned, and correcting any significant deviations. The basic aim of PSC is to identify sub-standard ships and sub-standard flag states as well and promote strict regulations to access the international ports as a defensive line against any danger that may affect the security and the safety of the shipping industry.

The port state control database of the major regional maritime administrations and MOUs such as the Paris MOU, Tokyo MOU, Black Sea MOU and the United State Coast Guard (USCG) analyses the successful level of the ISPS implementation, has been sharing information and industry co-operation since July 1, 2004, when the ISPS entered into force. However, the statistics also give common awareness of errors and lapses, which should be identified and avoided to develop a security culture in the shipping industry.

The statistical analysis of security deficiency and non-complying ships of the first year after the ISPS Code entered into force shows that 2511 ships were detained by PSC worldwide for various reasons, of which 259 ships (10.3%) were detained on security grounds. The detention rates for each individual region are: the Tokyo MOU

4.4%, the Black Sea MOU 6.6%, the Paris MOU 8.7% and the highest rate was the USCG 45.7% where most of the detentions were due to security grounds. The statistics also show that the security deficiency increases with older ships where 77.3% of detentions were for ships 15 years old and over. Another important remark is that all the security ground detentions were related to the Flags of Convenience ships (FOCs) except the Russian Federation and 45% of the overall detentions are attributed to 5 flags only where the Panama Flag is the highest among them by 20.1% (Yilmazel & Asyali, 2005).

Table 2: ISPS non-compliant ships classified by type of ship.
(Source: http://www.iamu-edu.org/generalassembly/aga6/pdf/s2-yilmazel.pdf)

Ship's Type	Black Sea MOU		Paris MOU		Tokyo MOU		USCG		TOTAL	
	Det. No	Rate %	Det. No	Rate %	Det. No	Rate %	Det. No	Rate %	Det. No	Rate %
General Dry Cargo Ships	15	88.2	57	67.9	26	65.5	19	17	117	45.2
Bulk Carrier	0	0.0	2	2.4	5	10.9	53	47.3	60	23.2
Refrigerated Cargo Carrier	0	0.0	6	7.1	9	19.6	6	5.4	21	8.1
Passenger Ships	1	5.9	1	1.2	0	0.0	9	8	11	4.2
Ro-Ro ships	0	0.0	8	9.5	1	2.2	2	1.8	11	4.2
Oil Tanker	0	0.0	3	3.6	0	0.0	6	5.4	9	3.5
Container ship	0	0.0	1	1.2	0	0.0	7	6.2	8	3.1
Chemical Tanker	0	0.0	0	0.0	1	2.2	7	6.2	8	3.1
Other	1	5.9	6	7.1	4	8.7	3	2.7	14	5.4

Table 2: Indicates that the highest detention rate was for general cargo ships (45.2%) and the low detention rates were for containers ships, tankers and passenger ships,

which reflect the proper implementation of the code on board vessels where the high-risk cargoes are transported. Also, it should be noted that most of the detentions related to USCG compared to other MOUs, reflecting more strict security regulation in this region.

The provision of regulation XI-2/9 of SOLAS and part A of the ISPS Code make the vessels inside the foreign port or intending to enter foreign port subject to control and need to be able to show valid International Ship Security Certificate (ISS) as well as relevant security records. The vessels which fail to demonstrate compliance with the ISPS Code will be denied entry and they will be subject to "additional enforcement measures", which may be stricter For example, the USCG has indicated that its port state control program reflects the compliance history of all vessels, flag state administrations, and recognizes security organizations. This history is stored in electronic and documentary form to use when making P.S.C decisions regarding the enforcement action to take for vessels has commercial interests with U.S.A ports (Yilmazel & Asyali, 2005).

This statistics indicate satisfactory level of implementation of the ISPS Code in a relatively short period. However, most of the main problems in the implementation process seems to be related to the personnel performance such as access control procedures, inadequate Master/Ship Security Officer familiarity with overall Ship Security Plans, inadequate crew familiarity with the ISPS roles and responsibilities, inadequate monitoring of ship's security reliability, sub-standard attitude and awareness, and lack of enough experience and training of ships' crew about the ISPS code (Yilmazel & Asyali, 2005).

2.10. ISPS Code and container security

The ISPS Code is an international agreement providing methodology of addressing security threats and managing potential risks that ships and ports may face in the international trade. IMO has provided the matter by introducing global minimum standards and procedures to prevent acts of terrorism. Individual governments can use these as a basis for expansion as appropriate to increase the level of security

according to the recent threat. In addition, the co-operation among world wide countries will have meaningful impact in reducing and preventing maritime criminals. For example, container security is a complex system and exchange of real time intelligence and updating information among all countries will have prevention measures against container criminals including terrorist attacks.

Meanwhile, security is not a static issue as threats changes from time to time. Governments need to monitor changes and offset them, as they occur, by communicating proper information and guidance to ships and port facilities to increase awareness and prompt response. Security of the containers needs the fastest, effective and efficient security systems especially when the container is passing to the port area where the ISPS Code is implemented. Using the technology and global cooperation will introduce the best solution to obtain this aim by inspecting, tracking and securing the containers without disturbance to the containerization trade pattern.

2.11. Conclusion

Maritime security can only be achieved with the commitment of all stakeholders to implement the ISPS Code in a uniform way. In situations where not every nation implements this Code effectively, there is bound to be lapses in security. But the ISPS Code should not be considered as an end to security problems. Vigilance is required of all.

Security should start by awareness on the dangers of terrorist acts and port authorities should take appropriate measures to reduce opportunities of any containers to be hijacked or becoming Trojan horses. Often these opportunities are so far “provided” with the help of port authorities due to lack of vigilance or negligence.

Just as technology can be said to be advancing, maritime terrorism is advancing as well considering the changes in forms of terrorist acts and the sophisticated nature of their acts. The advent of internet has led to most terrorist organizations to easily gain advanced information that helps them perpetrate their acts.

Chapter 3

Container security and technology

3.1. Introduction

The study through the previous chapter shows the gaps and weaknesses in the intermodal transportation system, which maybe used by terrorists. Meanwhile, considering the importance of using the technology to secure the container transportation system and since it is expected that this strategy will become the international security strategy for ships and port facilities. Therefore, it is of great importance to study the aspects of the various types of technology that could be used to secure the container movement and cover the gaps in the transportation chain from its origin point to its final destination.

In order to get fastest, most effective and efficient way to secure the containers in the intermodal transportation system, technology is the solution to integrate the security system together with the ISPS Code. Container security has improved gradually in the last few years, in reaction to the event of September 11. The world now establishes a risk management system to identify potential high-risk containers, and automate that system. This system should introduce the smoothing of the container movement in all steps and allow inspection of all containers as early as possible in the ports of origin.

All countries towards this issue are now making a great effort especially from the United States. Many proposals were introduced to the International Maritime Organization (IMO) to take action in order to increase not only the container security but also the entire containerization system such as port security in terms of container terminals, container vessels and container companies. But, the problem in the container security as an intermodal system is that some areas are beyond the scope of IMO such as the security measures to be applied for shippers and container packers to secure the real content of the container. Therefore, other organization such as World Custom Organization (WCO), and International Labour Organization (ILO) should take an important part in the container security.

3.2. Cargo security at the point of origin

The point of origin is the point where the container starts being stuffed by the cargo in the exporter's factory passing through land transportation mode then the port area till shipment on board the vessel in the country of origin. Security during these steps is necessary because inspecting cargo on board vessels on the high seas is almost impossible and inspecting cargo upon its arrival at destination port could be too late to prevent a terrorist event. Containerized cargo is a relevant example to that issue because the containers are stuffed and sealed at the exporter's factory. Ensuring that the container was not stuffed with illegitimate cargo, not tampered while trucked to the port of loading, and ensuring that the cargo details reported is not fraudulent, is all critical challenges in supply-chain security. Therefore, confirmation of security of each transport facility and the reliability of every company involved in the intermodal shipping process are important (Congressional Research service (CRS), 2004).

3.2.1 Security at originating shipper premises

Shippers and carriers play a fundamental role in justifying the potential illegal cargo from entering the containers within the supply chain. Once the container is stuffed on the shippers' premises, it will be immediately sealed to prevent any tampering with the container contents after its complete loading. The shipper will start to issue his documents to indicate the description of the container contents including the container and seal number and identification code. Then it will be loaded on trucks or railroad bounding to the port area for shipment. However, sometimes the warehouse facilities may have weak controls and personnel practices. For instance, access to shipping areas may not be secure and warehouse personnel practices may lack sufficient background or identity checks. Also, the seals types which are used to lock the container doors may provide minimum security tampering. Therefore, many proposals and new technology are now intended to push the shipper performance towards more efficient and effective security at this stage of the container inermodal transportation chain (OECD, 2004).

3.2.2 Custom Trade Partnership Against Terrorism (C-TPAT)

The C-TPAT is a voluntary government business initiative proposed by the U.S, intended at building “co-operative relationships that strengthen overall supply chain and border security”. The basic concept of that agreement is to making supply-chain participants, such as shipper and carriers, responsible for putting the best security performance of cargo transportation through implementing processes for the packing, tracking and distribution of all containers and goods in the intermodal layers (Customs and Border Protection (CBP), 2006).

The program includes recommendations and guidelines to be followed by the parties after signing cooperation agreement. For instant, the recommendations will require the shipper to provide basic physical security for all building and transportation access areas and it may also required this building to be constructed of materials that are resistant to unlawful entry. The carriers are also required to make visual inspection inside the empty containers before being loaded, and ensure that high security electronic seals are fixed on all containers. Moreover, all companies work in the system should have documentary procedure for their employees to screen their identification and background of each one according to his work type and the sensitivity of the position (Sweet, 2006, p. 176).

Once the agreement has been confirmed between parties, they are expected to show their ability to comply with the C-TPAT recommendations and guidelines. However, no more liability for non compliance party but the U.S. customs may remove this party from the C-TPAT membership which means stop all its commercial interest with the USA which may cause damage to his business (CBP, 2006).

Concerning the effects of C-TPAT on the intermodal supply chain, the program improves efficiency through implementation practices and standards of parties in containers transportation layers. It is also may make it more difficult for smugglers and terrorist organizations to use the container shipment for their illegal purposes. However, it does not make any clear prevention measures through the supply chain

security and does not help reduce the probability of successful attack or any compensation measures when theft or terrorism occurs (Willis & Ortiz, 2004).

3.2.3. The technology of the container seals

Most present container seals are mechanical devices that are categorized into indicative, security, and high security seals. Those types of seals are generally providing evidence or indication to the authorities if there is illegal entry or tampering with the container contents through the transportation chain. But, mechanical seals are easy to defeat while the expert thief or terrorists could cut the seal and replace it by a similar unit after they complete their crime. However, security seals could overcome this weakness by having unique identification number and being marked by the seal owner's stamp. For example, the U.S coast guard has changed the shipper seal to new one that should mark with an "alphanumeric identifier, which consists of five digits related to the port code, followed by a sequential number, (BALMS 00064)" (USCG, 2005).

The mechanical seals are only useful when joining cargo documents such as bill of lading or manifest, which indicates what was inside the container when it was sealed. Therefore, the seals should be fixed on the container on jointly attendance of direct responsible persons such as shipper and customs representative to verify visually the container contents before it is sealed. For more effectiveness, farther information about the seal should be kept by authorities in a special log book such as date and time of each visual inspection, ID number of the container and transportation unit, name and rank of inspector and name/ title of witnesses. This information will be useful to identify where the container was breached on the transportation chain and who is responsible (USCG, 2005).

The electronic seal is a new technology device that has physical security and information management capability. The electronic seal is similar to the mechanical seal with an additional smart chip to be able to record all the information data related to the container and its contents as an "electronic cargo manifest". The seal is also able to send its recorded message using Radio Frequency (RF) or infrared (IR).

Some advanced types transmit data through the Global Positioning System (GPS). This message will be sent automatically in time of any illegal tampering with the container that makes the authorities be able to identify the risky container location (OECD /ECMT, 2005, p. 53).

From a financial point of view, the use of the electronic seals today as part of the global container chain is difficult; this is mostly because of economic considerations. The effective system for e-seals should consists of an enormous number of reading devices/scanners, computer hardware and an outfit of fundamental information management software systems capable of accurately processing the seal data. These requirements may be deployed and effectively managed by some large ports or some big companies, but it is quite difficult for the small individual companies and small ports especially in some developing countries (OECD / ECMT, 2005, p. 54).

However, the advanced technologies of Radio Frequency Identification Tag (RFID) have several advantages, including relatively low price and proven operational capability. RFIDs are classified as passive or active. The passive type is cheaper and its power supply comes from a reader or scanner that make its use limited to relatively short distance, but it is read only and affixed by the party stuffing the container to track its movement through various transportation modes. An active seal has independent power supply that makes it able to record more events and transmit through greater distance. This tag is read/written that would provide the supply chain by more data of the container contents. In both types (passive or active) the tags can be read by RFID readers through the transportation chain and provide information on the exact location of the container. These readers could also identify the ID of the container being transported. Communication to the office through a wireless LAN, the location of any vehicle or container can be automatically recorded and displayed (Lukas, 2004, p. 18).

Standards for RFID tags used with container seals are also being discussed by institutions, such as the International Organization for Standardization (ISO), and International Telecommunication Union – Radio-communication (ITU-R), as the aim is to agree upon radio frequency that can be used internationally for that purpose. At

the present time, standards exist only for mechanical container seals and passive RFID tags which are considered mandatory for all containers imported to the USA. The ISO codes for electronic container seals using RFID tags currently being developed is (ISO/DIS 18185) (OECD / ECMT, 2005, p. 56).

Concerning the effects of container security seals on the transaction of the intermodal system, it might increase detection capabilities at the port of origin of transport of any illegal cargo, which reduces the potential damage as well (Willis & Ortiz, 2004). However, the system does not increase the supply chain efficiency in case of “Trojan horse scenario” where illegal cargo is stuffed on the container before the sealing process. That may occurs by any person working in a legitimate position such as stuffing persons at the shipper premises and being involve at the same time with illegitimate organizations such terrorists or smugglers.

3.3. Tracking the container

As mentioned before, the e-seals improve the security of the intermodal containers through alerting the authorities in case of any illegal interference to the container or its contents. Another advantage is the tracking and tracing function to identify the location of the container or the transport unit within the transportation chain. Once the containers stuffed and leave the shipper premises to start the transportation journey, its route should be previously planned. If the control centre of the tracking system is reported of any such deviation in the container routes or opening of the container door without previous permission and before reaching its final destination, it will be sequentially notified to local authorities to take security action. Cargo-tracking systems could be particularly well suitable for ensuring that in-transit cargoes do not fall into the wrong hands and are not diverted from their legitimate route, whether through simple theft or territories such as in case of “Container Hijack” or swap of an illegal imports cargo for a legal one through the legitimate trade pattern such as the case of “Trojan horse” (James & Robert, 2002).

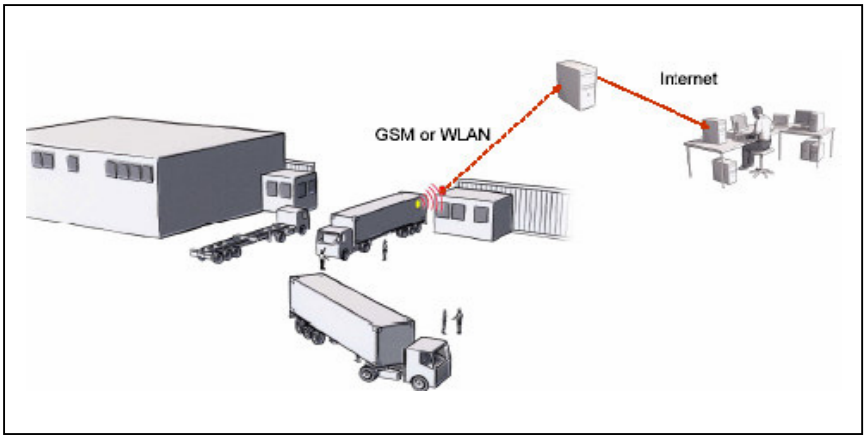

Figure 4: Tracking on shippers premises through WLAN or GSM and internet

Several varieties of technology are available to track containers. To decide which technology is suitable for such transportation mode will depend on the geographic scope for the tracking. In the case of the relatively limited area such as land transportation rail/road and port area, and in container terminals, the best technology will be the RFID tags with bar codes for each container or its seal, and set of readers and scanners in many different positions to cover all the container movement. Scanners can read codes from almost any direction and the portable scanners allow workers to read bar codes anywhere. In the case of long distance movement such as maritime transportation and some kind of land transportation through the borders between countries, the best way of tracking is satellites through the Global Positioning System (GPS). The technology of the GPS is available to be used for civilian purposes and have worldwide coverage. This system need satellite transponder to be fixed on the container to communicate with GPS to generate the updated position of the container to the ground station, which is consequently connected with the GPS satellite (Balog, 2005).

Concerning the effect of the RFID technology on security of the intermodal system, it has significantly increased the supply chain efficiency while the shipper and carriers are able to see where the weaknesses occur in their supply chain and could potentially optimize coverage of the gaps in the shipping process. Early detection of

misrouted or illegal goods will reduce the costs of theft and lost goods. Detection of any tampering with container contents at the port of origin will reduce damage of terrorist crimes. While, RFID is not able to identify the causes of the effects, it will improve the supply chain resilience if quick response is taken to reroute shipments in case of any disaster (Willis and Ortiz, 2004).

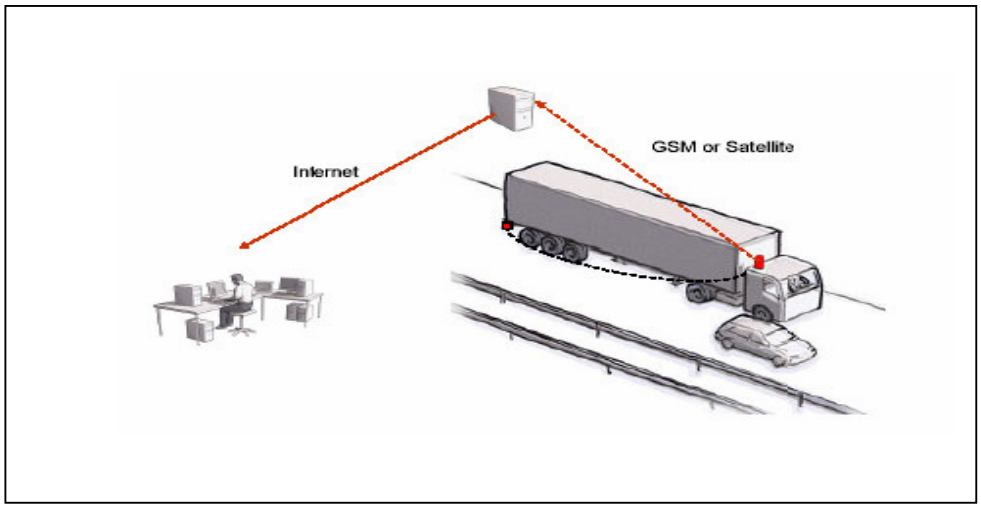

Figure 5: Tracking through land transportation mode

Tracking the containers on board vessels is considerable secured that is because the maritime mode is the only the mode that has an international security regime presented by the ISPS code. IMO has done a great effort to secure the ships cargo on board as well through navigation overseas. Regulation (19), paragraph 2.4, chapter V, 74 as amended and MSC 76 requires carriage of Automatic Identification system (AIS) on all ships of over 300 gross tonnages engaged on international voyages. The AIS is a navigation system installed on ships that automatically sends the ship's identity, position, course, speed, navigation status, and other safety related information to other ships and shore-based agencies, to allow for ship tracking and monitoring by the Vessel Traffic System (VTS) located in each port.

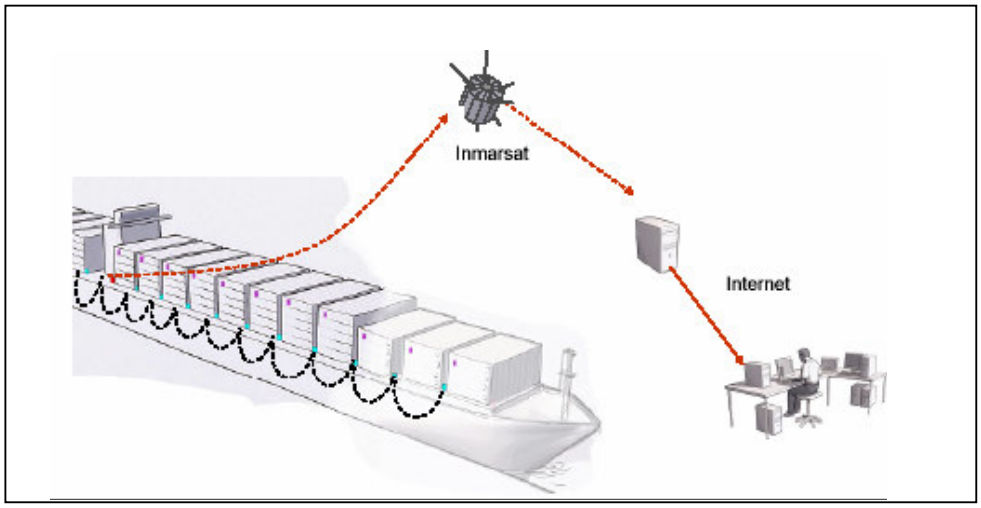

Figure 6: Tracking at maritime sector transportation using INMARSAT system

Concerning a Ship Security Alert System, IMO has adopted regulation (6) chapter XI-2 of SOLAS, 74 as amended during the diplomatic conference in December 2002. This regulation that came into force in July 2004 requires ships of over 500 gross tonnages to be equipped with an alarm system in order to strengthen ship security. This system allows the crew, in case of danger, to activate an alarm button that automatically sends a message to the ship owner and to competent authorities. The message is sent without being detected by someone on-board or by other ships in the area. These requirements with the addition security measure have been taken by the shippers or carriers to track the container itself while boarding on such vessels at sea. The GPS transponder has the ability to send its message to the authorities through satellite communication in case of any illegal tampering with the container at sea travel. Consequently, the authorities will take additional inspections for such containers in the port of arrival.

3.4. Security at port area

Once the container arrives to the port gate, it is time to leave the national security regime and lies under the international security regime of the ISPS Code and other

additional measures taken by some countries through cooperation agreement to maximize the security for the intermodal transportation. As an extension of the tracking system, the technology of Optical Character Recognition (OCR) will be applied starting from the terminal gate. Also the technology of scanning, screening and 24 hour rules will be implemented. This technology is part of the U.S. proposal named Container Security Initiative (CSI) in January 2002 to extend its security border to the foreign ports of origin including transit ports.

3.4.1. ISPS Code in action

The ISPS Code requires ships to provide pre-arrival information before arrival to the port approach area. This information to be supplied should at least include: ISPS identification certificate; operating security level statement; a statement of any additional security measures required; a statement of any previous security action taken against the ship or any other special measures and history of at least last 10 ports of call. Any delay to submit such information to the Port Security Officer (PSO) on such mentioned time may delay or prevent the vessel to be allowed to enter this port. Once the vessel is inside the port, port security guidance should be announced to all persons concerned such as crew on board. This information includes access control, restricted areas, cargo handling operations, monitoring of ship security and interaction with port facilities. Therefore, the one big consequence of not complying with the ISPS Code for ships is that a ship can be denied access to a port, which in turn means that it interrupts the carriers' schedule and causes delays in the cargo deliveries. This delay may maintain major costs to the carrier and the risk of lost business (SOLAS, CH. XI-2, regulation 9, 2004, p. 448-451).

3.4.2 Optical Character Recognition (OCR)

The system consists of a group of cameras positioned on the gates of the container terminal, which is divided into lanes. Each lane allows for one truck only to pass through; other groups of cameras are spread inside the area of the terminal including the rail and yard operations, and others are fixed on the loading cranes. Those groups of cameras have different criteria to take images for the container, as

a video, and connected to the software to make all systems available at any time from any place. The system has many benefits, which are: based on tracking the container to provide quick classification of the object, the system eliminates false-identification resulting from other tracking device, computerized tracking and screening system eliminates manual interference of traffic at gates. In addition, the OCR gives more benefits such as calculating the real-time for computerized operations and improved security response, makes more facility in order to have smooth flow of containers, ensures that the container does not pass any security check point, and makes files for the images which may be used for security confirmation. In other words, the OCR system will make it easy to make container tracking management in the terminals in terms of more accuracy tracking, increase the terminal capacity, reduce terminal staffing requirements, and the images files will assist for any further inspection (Elovic, 2003).

3.4.3 Container Security Initiative (CSI)

The driving force behind the CSI is to “push the border back” in an effort to secure containers at the point of origin before shipment in order to identify the high-risk container as early as possible to prevent containerized cargo from being an easy terrorist target. The U.S. has addressed their security concerns to have agreement with countries, which have a direct or indirect trade relation with them. In the beginning, the U.S. custom office focuses on 20 major ports around the world, where more than 70% of U.S. trade passes through. At the present time the number of contracted ports is 44 around the world (CBP, 2006).

The following data states that 44 CSI ports are currently operational from the date of contract. They include: “Halifax, Montreal, and Vancouver, Canada (03/02); Rotterdam, The Netherlands (09/02/02); Le Havre, France (12/02/02); Marseille, France (01/07/05); Bremerhaven, Germany (02/02/03); Hamburg, Germany (02/09/03); Antwerp, Belgium (02/23/03); Zeebrugge, Belgium (10/29/04); Singapore (03/10/03); Yokohama, Japan (03/24/03); Tokyo, Japan (05/21/04); Hong Kong (05/05/03); Gothenburg, Sweden (05/23/03); Felixstowe, United Kingdom (U.K.)

(05/24/03); Liverpool, Thamesport, Tilbury, and Southampton, U.K. (11/01/04); Genoa, Italy (06/16/03); La Spezia, Italy (06/23/03); Livorno, Italy (12/30/04); Naples, Italy (09/30/04); Gioia Tauro, Italy (10/31/04); Pusan, Korea (08/04/03); Durban, South Africa (12/01/03); Port Klang, Malaysia (03/08/04); Tanjung Pelepas, Malaysia (8/16/04); Piraeus, Greece (07/27/04), Algeciras, Spain (07/30/04), Nagoya and Kobe, Japan (08/06/04), Laem Chabang, Thailand (8/13/04), Dubai; United Arab Emirates (UAE) (03/26/05); Shanghai (04/28/05), Shenzhen (06/24/05); Kaohsiung (07/25/05); and Santos, Brazil (09/22/05), Colombo, Sri Lanka (09/29/05), Buenos Aires, Argentina (11/17/05), Lisbon, Portugal (12/14/05), Port Salalah, Oman (03/08/06), and Puerto Cortes, Honduras (03/25/06)" *(CBP, fact sheet, 2006).*

The container security initiative (CSI) consists of the following four elements:

- The system depends on the use of the automated information to identify and target the high-risk containers through use of advanced information.
- Pre-screening those containers to identify which are high-risk at the foreign CSI port before arriving to the U.S. ports.
- Using detection technology to quickly pre-screen high-risk containers including radiation detectors and large scale x-ray imaging equipment to carry out inspection as quickly as possible and without any delay of legitimate cargo.
- Using smarter, tamper-proof containers. The elements explain if the container has been tampered with after security screening (CBP, 2006).

3.4.3.1. 24 hours rules

First, using automation information to identify and target high-risk containers or what is known as the "24-Hours Rule". The system, which started on December 2, 2002, requires carriers to provide the ship cargo manifests by submitted electronically to U.S. Customs before cargo to load on board by 24 hours destined for the U.S. ports. The rule is also valid for the empty containers and transit containers which are called "Foreign Cargo Remaining on Board (FROB)"; however, bulk shipments are exempted from this requirements and break bulk cargo exceptions may be made on a case-by-case basis (UNCTAD, 2004).

Manifests vary by transportation mode but they generally contain information about the shipper, consignee, carrier, country/port of origin, and description of cargo. This will make the Custom and Border Protection authorities very closely linked to the shipment contents including timing of each cargo movement from one mode to another. It also, establishes new policy for the container shipments: adding new criteria to U.S. customs service automated system, which indicates the latest information about any terrorist action, to be sure that the manifest is reviewed by experts. Finally, it tracks the container in case the system identifies any risk or dangerous container. This electronic cargo information is used for the importation into or exportation from the United States (CBP, 2005).

The system of 24 hours makes the carrier responsible for any failure to provide manifest information or failure to present or transmit accurate and complete manifest data in the required time or transmission of any false, forged or altered document. He may be liable for civil penalties. Moreover and for security reasons, the U.S. custom office has decided not to release information from cargo declarations until the complete manifest is filed with them and the information may be published after the vessel has completed loading and leaving the foreign port. The efficiency of the 24 hour rule requires the carrier to be accurate, fast and efficient to sending the required information without any delay. It also depends on the efficiency of the Customs Office experts to quickly analyze the received information in order to be able as quickly as possible to assign the high risk cargo and send the message “not to load” to the carrier without any further delay for the legitimate cargo (UNCTAD, 2004).

3.4.3.2. Screening and scanning technology

Second, the pre-screening system uses a combination of large-scale x-ray, gamma rays machines and a global positioning transponder. The manual process of opening, discharging, and physically inspecting a container takes approximately 8 hours and may be more, which depends on each individual case, while the manual inspection can cause significant delays of cargo flows. This technology will help to

make quick inspection for the containers without any delay of the normal flow of the trade. The system has different capabilities to identify specific materials such as explosives, radioactive material, drugs and any kind of weapons. Different kinds of equipment may be used for that purpose such as crane mounted, hand-held, and mobile. The pre-screening will be in the port of origin and before 24 hour at least of the container shipment on board the vessel (CBP, 2005).

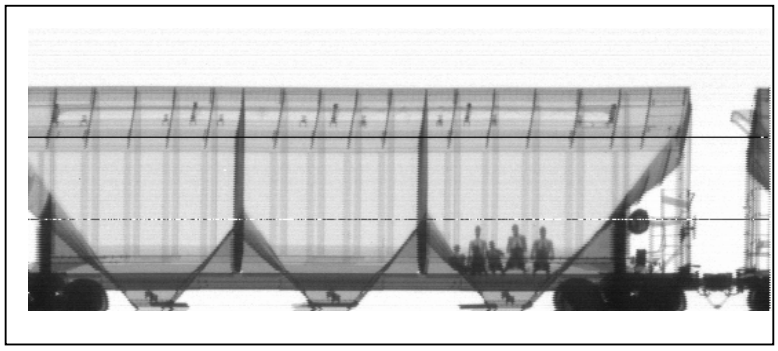

Figure 7: Scanning the container before shipment and screening picture. (Source: Bureau International des Containers)

The ability of the inspection equipment, even with the latest updated technology, is limited and detection of materials relies on the experience of the operators. An X-ray machine could detect the material by examining its density and give alert through a sound alarm (see figure 7), but the final decision about what kind of material it is exactly will depend on the screen operator's judgment while viewing the image and sometimes physical inspection is needed. Therefore, inspectors need to be well trained to understand the x-ray images. However, table 3 will summarize the inspection technology which is used for the security functions (OECD/ECMT, 2005).

3.4.3.3 Technology to identify high risk container

Third, the US custom service takes more steps to identify and target the high-risk containers; this system applies to both countries using CSI and non-CSI ports. The system introduced a new form of vessel manifest to be used in the system called Sea Cargo Targeting Initiative, which is a computerized system to identify high-risk containers, and it establishes a new policy for shipment toward US ports. The Initiative has three main components: to add new technology to the US service computerised system to have the updated information about possible terrorist actions; to be sure that all the available information will be passed to expert persons to review it and make standard system for US customs in all the ports and trained for how to handle the action when the system indicates high-risk shipment (Jagc, 2003).

3.4.3.4 Improvement in electronic seals

Finally, the US customs service has also taken advanced steps to improve the electronic seals as an alerting system for any tampering of containers after they have been screened. The alerting system is a motion detection or light detection used to warn of anybody trying to go through the container contents by bypassing the seals. Some containers today already have this system for example; refrigerated containers in use today contain a smarter device to maintain the temperature to avoid the melting of the meat. US custom service has taken more steps to inspect

the containers by using gamma rays in some kind of machines in order to allow the inspectors to inspect the containers within 90 second whether they are empty or loaded with cargo. This machine will be used for in- bound and outbound containers in US ports and also in other partner ports where the CSI system is applied (Jagc, 2003).

3.4.4 Underwater surveillance

Using technology for securing port infrastructure is extended to the under water area to combat any possible attacks by terrorist divers. The system is designed to track and observe underwater threats in order to give alarms for authorities to act on. The way is to use Remotely Operated Vehicle (ROV), which is normally used to inspect the underwater hull of the vessels or protect navy vessels. ROV is a robotic system for underwater operations, which differs in size and configuration. Different types and a number of cameras, mechanical tools, sonar and sensors support the robot. Some harbors in the USA and Europe have implemented this system for security issues in commercial harbor areas, either by using the same kind of hull inspection robot or by using fixed underwater installations. Benefits include increased protection of ports, critical waterside infrastructures and other fixed shoreline sites and prevention of attacks affecting large areas of local populations such as those near dangerous cargo areas such as gas and oil terminals. The advantage of this system is to discover any risk of terrorists without negatively impacting a port's capability to operate and free movement of the vessels (Ferriere, 2005).

Table 3: Technology features. (Source: European Conference of Ministry and Transport (ECMT) report, 2005, p.50).

	Description	Indicates potential presence of threat	Provides material Discriminate--ion	Time for inspection	Installation	Cost
Active systems						
Acoustic	An ultrasonic transducer is put into the container and a sensor detects the reflection and forms an image	Yes, in liquids	No	2-5 minutes/ object	Portable/desktop equipment, which can be operated by battery or wall plug power	$$
Gamma ray	The gamma rays interact with the object and are displayed as an image	Yes	No		Mobile, fixed or relocatable sites. Fixed and relocatable sites require local infrastructure of power, road access, personnel facilities and attention to radiation safety	$$$
Pulsed Fast Neutron Analyses (PFNA)	Pulsed neutrons are directed at the object and create gamma rays with energies characteristic of its elemental composition	Yes	yes	90+ minutes/ object		$$$$
Thermal Neutron Activation (TNA)	Sophisticated sensors detect the energy of the gamma ray photon emitted when the thermal neutron is absorbed by material within the object	Yes	Yes			$$$
X-ray						
Standard transmiss--ion	The transmission of x-rays is directed through the cargo to a detector and presents one "shadowgram" image to that overlays all items in the beam path	Yes	No	2-5 minutes/ object		$$$/$$$
Dual energy transmiss--ion	Two different x-ray energy spectra are used. Generally ineffective for large cargoes	n.a.	Not in high density cargoes			n.a.
Dual view transmiss--ion	Two views of the object are displayed	Yes	No			$$$$$
Backscatter with transmiss--ion	Two or more views are displayed. Backscatter images highlight items in the object that contain low atomic number elements	Yes	Yes			$$$$
Passive system						
Canine use	Dogs are trained to alert the presence of explosives and other threat objects	Yes	Yes	0.5-1 minute/ object	Requires care, feeding and shelter, together with trained handlers	$
Radiation detection	A detector measures the ionizing radiation or other characteristic radiation emitted from a radioactive substances	Yes	Yes		Portable/ desktop equipment, which can be operated by battery or wall plug power	$
Trace detection/ vapour detection	A "sniffer" types sensor collects and analyses air samples	Yes	Yes			$

Cost key: $ ≤ $ 50, K;$$≤ 100

3.5. Conclusion

Technology is available to secure the intermodal transportation chain in term of container transport. Using this technology could cover many gaps and weaknesses in the container transportation system. The cooperation agreement among most of the industrial countries gives validity for emerging the system in the international security regime. The system could also take further steps to improve the management procedure and identify the responsibilities among shipping actors.

However, this technology alone cannot achieve effective security. The people works on the field, especially in land mode, is another important factor could affect the level of protection such as the availability to interfere the container contents at shipper premises and before the container start its legitimate journey.

Moreover, the efficiency of the system mostly depends on its effective implementation on the country of origin where there is different customs and practices varied from one country to another. This technology will not be effective without international agreement and harmonization for the system together with the ISPS Code.

Decision makers should be aware of the benefits and impacts of their decision to implement this technology such as:

- How this technology will be used?
- Who will pay for its cost?
- The impacts for their country if such implementation take place,
- Detailed cost benefit analysis for tightness security measures and its impacts to the other industries,
- The international market situation in term of the demand and supply theory,
- The effect of this implementation, especially these initiatives which depends on bilateral agreement on their countries sovereignty.

Most of these analyses are subject for economic consideration and the discussion through the next chapter may help to better understand some of these factors.

Chapter 4

Security control and economic impact

4.1. Introduction

The aim of this chapter is to donate to a better understanding of the impact of the new security measures on the maritime community. The chapter will introduce the cost analysis for implementation of mandatory IMO security measures related to ships and port facilities. The cost analysis will also include the cost of American Initiatives, its effect on the shipping industry and try to answer the question of “who will pay for the security”. The chapter will bring in the cost of terrorist attacks take into consideration some real examples and opinion of industrial experts. The cost benefit analysis will be discussed to give attention to the benefits and impacts of tight security measures on industrial actors.

Shipping plays a vital role in the economy of world trade and maritime transport is an economic activity. The United Nations Conference on Trade and Development (UNCTAD) estimates that the operation of merchant ships contributes about US$380 billion in freight rates within the global economy, equivalent to about 5% of the total world trade (IMO, 2005). The concept of the shipping business that every player on the field need to gain, but sometimes-unavoidable factors may affect this environment. The September 11 event gives attention to the world of possibility of using transportation facilities in the terrorist act. Quick action has been taken to increase security, which appears in mandatory implementation of the International Ship and Port Facility Security (ISPS) Code as chapter XI-2 in SOLAS convention. Additionally, the United States and European countries proposed tighter security initiatives considering the intermodal transportation system includes various modes of transportation.

New security improvement will require expensive infrastructure and technology. The costs arising from terrorist attack are huge including loss of lives. A decision should be taken by the maritime community and industrial actors to save the international

trade and world economy. Cost analysis is the way from an economic point of view for such decision.

4.2. Cost analysis in intermodal security

4.2.1. Direct and indirect costs

Cost of intermodal transportation security can be classified as either direct or indirect. Direct costs are the capital costs, which are needed to build security framework such as:

- costs of purchasing new security equipments to prevent any terrorist activities and protect the fixed physical infrastructure (e.g., terminals, warehouses, supply chain),
- cost of implementing new security regulations,
- cost of employing new security staff and increase their awareness through sustaining education and training procedures.

Indirect costs are the operational costs that need to update the system to cover any security gaps, which may arise during the work such as:

- maintenance of the equipment,
- increase efficiency of the supply chain through increased management density,
- cost of responding to a terrorist event (communication, collect information, central distribution system),
- cost related to consequences of management recovery including recovering from interrupted operations and re-constructing.

4.2.2. Cost of implementing security measures

The cost affecting ship-operators to enhance maritime security will be in two areas, namely shore side and on board vessels. In general the cost will include documentation transaction to and from other involved parties, such as port authorities, increased communication, personnel training shore side / on board vessels, increase labour, using standard devices and security-related technology.

Some other factors will affect the cost level depending on the types of vessels they operate. For example, the costs will increase for vessels entitled to flag of countries involved in additional security agreements, such as container vessels proceeding to US ports require additional devices for the ship and its cargo. The vessels that do not apply to these requirements will not be able to enter any U.S ports, which mean great economic losses for the ship operators.

For security concerns, all ships involved in international trade are required to be equipped with Automatic Identification System (AIS), ships identification number, and ship security alert system. These requirements were agreed by the Maritime Safety Committee 76, and become mandatory for all vessels from July, 2004 as SOLAS requirements in Chapter XI-2. However, AIS requirements were already in place in chapter V of SOLAS for the purpose of safety of navigation. Concerning container vessels, U.S Container Security Initiative (CSI) requires additional equipment for tracking and anti-tampering devices such as Radio Frequency Identification (RFID), Global Positioning System (GPS) with special characteristics, 96 hours notification of arrival and 24 hour advanced manifest rules.

For the purpose of this study, the number of world fleet vessels will be needed to estimate the cost of security implementation on board sea going vessels. According to IMO statistics in its international day meeting for carriers of world trade 2005,

> The current world trading fleet was made up of 46,222 ships, with a combined tonnage of 597,709,000 GT. The vast bulk of the fleet was made up of: general cargo ships (18,150), tankers (11,356), bulk carriers (6,139), passenger ships (5,679) and containerships (3,165). Other ship types accounted for 1,733 vessels.

Table 4 summarizes the estimated cost calculations for both international requirements (SOLAS / ISPS code) and United States maritime security measures. The contents of table 4 were obtained from IMO data, industrial sources, United States Coast Guard (USCG), and Organization of Economic Co-operation and

Development (OECD) report 2003. Calculations were based on the average price of each device up to the current market price. The actual number of world fleet vessels used in the calculation was based on vessels more than 500 G.T and involved in international trade, 43 291 vessels as corresponds to Lloyd's Register estimation.

Table 4: Summary cost of maritime security and non Anti-terrorism Benefits. (Source: OCED report, 2003, P.55)

Measures	Initial cost approximate (million USD)	Yearly Cost approximately (million USD)	Indirect cost	Confidence level	Non terrorism benefits
IMO SOLAS/ISPS Code					
Government Security Alert Levels	(Low)	N/a	Potentially large	Low	+
Automatic Identification Systems	649.3	(Undetermined)	Undetermined	High	+++
Ship Security Alert System	86.5	4.3	0	High	
Ship Identification Number	216	n/a	0	Medium	+
Company Security Officer (large companies)	514.6	514.6	Undetermined	Medium	+
Company Security Officer (small companies)	150	150	Undetermined	Low	+
Ship Security Assessment	103.9	(Low)	0	Medium	
Ship Security Plan	51.9	(Low)	0	Medium	
Ship Security Officer	29	29	0	Medium	+
Ship Security Training/drills	16.8	16.8	0	Medium	
Vessel Security Equipment	304.4	15.2	0	High	+
Record-keeping	(Low)	(Low)	0	High	
Port facility Security Assessment	27.9	8	0	Low	++
Port facility Security Plan	27.9	8	0	Low	++
Port facility Security Officer	Undetermined	Undetermined	Undetermined		++
Port facility Training/drills	Undetermined	Undetermined	Undetermined		+
Port facility Security Equipment/staff	Undetermined	Undetermined	Undetermined		+++
United States Maritime Security measures					
Maritime Transportation Safety Act of 2002 (non- IMO provisions)	(Undetermined)	(Potentially large)	(Undetermined)		
96-hour Advance	6.7	6.7	(Undetermined)	High	
INS Crew Seafarer Requirements (proposed)	95 (at least)	(Undetermined)	High	Low	
24-Hour Advance Manifest Rule	281.7 To 10 000	281.7 To 10 000	(Undetermined)	Low	++
Container Security Initiative	(Undetermined)	(Undetermined)	(Undetermined)		+
Customs-Trade Partnership against Terrorism	(Undetermined)	(Undetermined)	(Undetermined)		+++

4.2.2.1. Cost of IMO, SOLAS/ISPS Code, mandatory regulation

As it shown in table 4 above, the initial cost estimated to be spent by ship operators to comply with the ISPS Code is at least USD1.3 billion and USD730 million per year thereafter. However, the cost related ISPS code implementation for port facilities seems to be larger. The OECD confidence level in their judgment of some costs varied, especially with costs related to many US initiatives. That is basically because these initiatives have fewer technical elements and have a potentially border and more disperse effect. The confidence level is higher in the IMO measures targeting companies and ships than other IMO measures targeting ports and many of the US initiatives. Some undetermined data will be observed because it depends on how each country will handle the case or otherwise there will be lack of experience on future maintenance price to some systems (OECD, 2003, P.54).

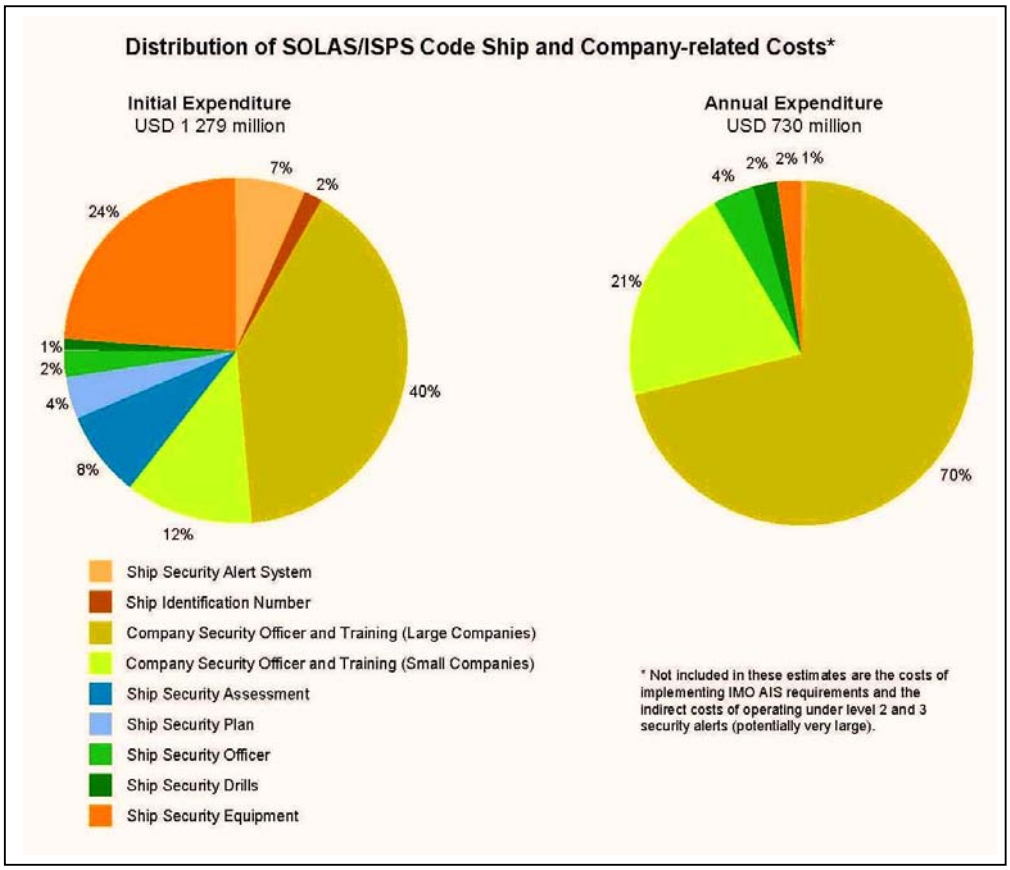

Figure 8: ISPS Code implementation costs. (Source : OECD, 2003, p.38).

4.2.2.2. Estimated cost of United States maritime security measures

Concerning the cost of the American proposals, the Department of Homeland Security has an appropriate budget of USD4.2 billion for port, container and cargo security. However, this budget is not enough in the opinion of the American port safety advocates, such as Sen. Patty Murray, D-Wash., and Port of Seattle Chief Executive Mic Dinsmore. Murray said, “Those funds are not enough and that is why we ask for more”. He also added that “ports need the kind of hardened security now present at the airports, and that the cost of doing so far exceeds the bill's budget for it”. The estimation budget should include USD2.1 billion for Coast Guard port security operations, USD1.7 billion for Customs and Border Protection cargo inspection and trade operations, USD139 million for a Container Security Initiative, USD178 million for radiation portal monitors, USD70.1 million for a Customs Trade Partnership Against Terrorism, and USD200 million in port security grants (Bolt, 2006, p.1).

4.3. The economic impact due to successful terrorist attack

In the maritime sector, the volume of world trade conducted by sea was estimated by the United Nations Conference on Trade and Development (UNCTAD) to be 5.8 billion tons traded by sea. This account for over 90% of the world trade by volume and contributes about USD380 billion in freight rates within the global economy, 5% of total world trade (World Maritime Day, 2005). The impact of any coordinated terrorists attack will have significant effect start from industrial users; extending to individual country economy and the entire world economy as well.

A coordinated terrorist attack against a port could result in shutting down the entire system and disturb the government organization. This may also extend to disturb all transportation modes serving this port. The economic impact of such incident will be huge and will affect the country economy. For example, in the United States one of the Government Senators called Levin Coleman made a study to estimate the economic consequences of an attack on the Port of Los Angeles and Long Beach. This study found that the United States’ Gross Domestic Product (GDP) would

decline by about USD150 million per day for each day that the ports were closed and that the annual cost would be approximately USD70 billion (Coleman, 2006).

Another real example, when a group of terrorists attacked *Limberg* tanker on October 2002 while at anchorage at Yemen Port. This incident increased the insurance premium three times more for the vessels calling Yemen ports as much as USD0.3 million and the premium for the 20-foot container reached USD250. Terminal operations dropped from 43 000 TEUs to 3 000 TEUs in three months only. Many shipping lines changed their routes and schedules to Yemen, which had a negative impact on the country's industry. About 3000 jobs were lost on Yemen port. Governments estimated losses of USD15 million per month, which negatively affected the Yemeni 2001 GDP by 1% if this situation continued for complete year (Jain, 2004).

The attacks on the World Trade Centre resulted in massive economic losses on the United States. The consequences were huge in the entire transportation industry, especially airlines due to the closing of the American air space for four days. Approximately 200 000 jobs were destroyed or transferred out of New York, another reason is that lower Manhattan lost approximately 30% of its office space and scores of businesses disappeared. The damage on the physical infrastructure suffered losses of USD14 billion for private businesses, USD15 billion for state and local government enterprises and USD0.7 billion for the federal government. Additionally, the great losses for world wide insurance companies due to the terrorist attacks were estimated up to USD58 billion to pay liability insurance (OECD, 2003).

Another study shows the impact on Japanese economy based on scenario of terrorist incident affecting the waterway around Japan. The experts estimated the losses for the Japanese economy in case disturbance or prevention of shipments of crude oil from the Middle East to Japan by USD88 million if the Malacca / Singapore Strait were blocked, USD200 million if the South China Sea were closed, and 1.2 billion if the Indonesian Archipelagic Waters become impassable. The estimation of these losses was not only for Japan but also for many other countries in the area. This is because the blocking of these waterways will make freight bound for them

detour around south coast of Australia. The European countries and the US will also suffer from economic losses from such estimation due the disturbance of container trade with Southeast Asia's countries and Japan. In other words, the disturbance of container shipment will impose serious losses on the world economy. The delay of transportation of raw materials and industrial elements transported by container will inflict stoppage of many factories and projects, which will affect the entire world economy (Akimoto, 2001, p. 8-9).

4.4. Cost benefit analysis

While implementation of security measures is costly, consequences of terrorist attacks are more costly and while some measures may slow trade, many others can in fact lower trade cost. The benefits of tight security measures mainly have economic aspect for countries and for the entire world trade. Apart from economic gains, the major benefit that should be considered is tighter security measures will prevent or at least decrease losses of life resulting from any successful terrorist attack. Loss of life could be by direct killing with weapon of mass destruction or with long run killing affecting people's health by chemical, biological or nuclear weapon.

The benefit express the revenue from invested the money in such previous control option per each unit to avoid or minimize the risk. Stakeholder is vital element in this step, which they can affect the decision because they have more commercial interests therefore the decision should be equitable and fair to all stakeholders. To obtain the objective, the risk balance is developed to calculate the gain of the new implementation. In other words, they should found that return benefits and effective risk reducing it more than cost investment and the present situation of risks. For example, how much the investment costs to allow the port authority to check the condition of the container before loading on board in term of time cost in the operation schedule of the vessel to avoid the crises results from terrorist action. Also, the investment costs for education and training of the crew on board in front of the results to increase security awareness. The decision maker should consider the capital cost for implementing the new regulations, communication costs, operation costs, labour and training costs, maintenance, inspection and certification costs. On

the other hand they evaluate the benefits in term of prevent the implication of terrorist attack and its further consequences such as reduce damage for human and environments.

Additionally, the economic benefits for tighter security are tremendous and will increase in long run operations some of which them may appear with the following examples:

- All the industrial actors will gain benefits from decreasing cargo theft and pilferage, lowered insurance premium, reduced delays, and faster processing times, improve inventory control and decreased documentation routine due to improved information technology. For example, the cost benefit analysis of a new automated cargo manifest estimates direct saving to American importers only by USD22.2 billion over 20 years and saving USD 4.4 billion for the American government over the same period (OECD, 2003, p.56).
- Increased security would have an impact on reducing stowaways and illegal cargo trafficking such as drug smuggling that kills more people and has bad effects on society over time.
- The government will be able to identify cargo which had previously counterfeit or misidentify with gaining exceed USD2 billion.
- The government will be able to gain USD16 billion from tobacco tax alone that had previously traded by illegal way.
- Protect the marine environment from damages through detecting undeclared, improperly described and improperly load of dangerous cargo and nuclear materials (Trelawny, 2006).

4.5. Various economic considerations

4.5.1. Who will pay security costs?

The American initiatives to improve container security request all foreign countries that have commercial interest with United State to implement the CSI program in their ports. U.S Customs intend to pay to arrange their officers and computers in the foreign ports, but other costs related technological equipment such as screening and

detection equipment will be paid by the host port. Most of the countries recognized the importance of trade with U.S started to addressing question of (who will pay for this expensive technology?). Many of the decision makers are still confused that the cost will be covered by relevant host ports or by way of public funding (i.e. exporter, importer, shipper, carriers or any other party) (UNCTAD, 2004).

The trend of maritime communities indicates that the consumer will pay the cost of security. The cost for the container will increase about USD7 for screening and implementing other container security measures (U.S. Subcommittee on Coast Guard and Maritime Transportation, 2005). The government will primarily pay for security implementation and then this cost would be passed to the users such as shippers and carriers, and finally this cost would be passed to consumers of goods or in other words to the public community. This concept is clear in the speech of Mr. Tim Blood, manger director of P & O ports in Australia and New Zealand, who said "the Federal Government expected the shipping industry to bear the security cost but the community did not realize this would inevitably mean higher prices for consumer goods". He added, "Importers and exporters would be hit with increased costs that would be passed on to consumers" (Russell, 2004).

In the 2nd Annual U.S Maritime security Expo and Conference, October 2003, many speakers gave their opinion about how security costs should be covered. Mr. Thomas Thune Andersen, Maersk representative, enhanced the importance of co-operation between governments and the industry partnerships to identify measures that would be effective in this matter. He also stated addressing security," Progress has been made, but much work still lies ahead and no single entity can do it alone". Another speaker at the same conference was Mr. Michael Connors, of Booz, Allen, Hamilton, said that the solution is to seed money for technology development in maritime security and the only way for that is increased costs to consumers because in one way or another they will pay for it (Babul, 2004).

However, The American Association of Port Authorities (AAPA) announced the importance of the ports in the nation's economy and declared that additional fees and taxes upon ports are unacceptable. They said that the maritime community

already pays billions of dollars in user fees and taxes to the federal government. This money is considered as federal revenues, which include USD17.5 billion from customs duties and should be used as a source of security funds (American Association of Port Authorities (AAPA), 2006).

4.5.2. Impact on developing countries

While the costs of security implementation are expensive and the level of technology and equipments required to comply with the new security measures is not easy to establish, developing countries may suffer some implication to cover either the direct or the indirect costs of security. The huge competition in the shipping market and the limited ability of small entities, such as ports, carriers, shippers, and intermediaries comparing with the same parties in the developed countries will make participation of the developing countries in international trade is difficult. Potentially, the legitimate trade may be negatively affected, due to the incapacity of principally small and medium size enterprises within these countries, to effectively comply with the new requirements. For example, the CSI program proposed by the US will be difficult to implement by some small developing countries because the cost per port for that program varied from USD1-5 billion (UNCTAD, 2004, p.20).

In the developing countries most of the industry businesses are related to government operations such as ports and fleet operations. Private sectors are very limited for specific types of jobs such as shippers, forwarders and agency. These private sectors are also related to the government in their final job procedures like documentation and customs process. Therefore, most of the load to cover the security implementation will lie on the government, which should get part from the nation economy. These deductions from the national economy will be the strategy in the exports and imports and increase the price of goods for the public consumers as well.

On the other hand if some countries take medium solution by implementing only the mandatory (IMO – SOLAS/ISPS Code) part of the security measures and decline the other optional part which lies under U.S. initiatives, as an option to save some of

these costs, they will face a problem of limited international trade because most of the exporter and importer will prefer to transport their cargo through ports and shippers which they apply to the US initiatives to avoid any stoppage or delay for their trade. These will show up the problem of bilateral agreements which may divide nations into favoured and less favoured trading partners and may lead to competitive disadvantages and failure to participate of developing countries in the international trade market.

Decision makers should be aware of the opportunity cost theory, which is one of the most suitable economic theories that should apply to developing countries and problems of security implementation costs. This theory simply explains `Who needs the others and there must be decisions on what will be done and what is left undone, what service will be provided and what not provided? `. In other words, the shipping market is a competitive market and if one country did not accept any rules, which generally apply to other countries, this country will be only the looser because it will be out of the market. There fleet will suffer many stoppages by the port state control detention or decline allowing to enter some ports. Shippers and exporters will suffer great losses due cargo delay in pay of huge demurrages to compensate cargo owners and finally they will loss the existing in the market.

Moreover, technological devices which are required by the container security system, such as electronic seals and smart container system will need the availability of suitable equipments, electricity supply, technical assistance, maintenance schedules, and experts' operators. These requirements are a problem of many developing countries at this time to apply with the rules and will increase the risk on the exporters to participate on the competitive international trade (UNCTAD, 2004, p. 25).

4.5.3. Impact on shippers

Shippers have a responsible role in implementation of security measures as mentioned before, as they are considered the major actors in security of the point of origin through intermodal transportation, such as installing tracking and anti-

tampering devices in the containers. The European Commission gives priority to create transport security in depth through the logistic supply chain and it is apparent that very soon it will be reality. The European Shipper Council (ESC) paper on “The Impact of Security Regulation and other Requirements on Shippers” has analysed and estimated the effects of the additional security requirements on shippers that will be discussed below.

Generally, shippers consider the cost of compliance with security regulations like any other business and this cost will simply be recovered from their customers. However, the ESC registered many cases where shippers were suffering more cost than they were expected to due to long delays to their cargo movements caused by U.S. customs authorities. These delays some times recorded two weeks and they were mainly caused by carrying out stricter screening and other security procedures. The shippers announced that they had to pay the cost of demurrage in addition to the liability consequences of some cargo damage and loos of some customers because they were unable to deliver the cargo on time (ESC, 2004).

On the other hand, shippers are also suffering from fluctuating costs of the market, especially in the liner market, such as container shipping being more competitive than the other markets. The demand is (e.g. container vessels, shipper offices) present in the market more than the supply (e.g. export and import cargo). Then the rule of price elasticity will apply in this case particularly for the demand sector (Shou, 2005).

This means that the shipper should decrease transportation freight to continue combating on the market or otherwise if the customers find another cheaper way, they will take it. In that sense, shippers will suffer two opposite directions of the market completion:

- Shippers should increase freight rates to cover the cost of new security measures, especially U.S. requirements in intermodal transportation.
- At the same time shippers should decrease the freight as the liner market is a competitive market and supply is more than demand in the recent time.

Table 5: Fluctuations in container freight rates in the major East-West trades. (Source: Containerization International, various issues).

Qtr/Year	Asia/US Eastbound	US/Asia Westbound	Europe/Asia Eastbound	Asia/Europe Westbound	US/Europe Eastbound	Europe/US Westbound
Q2 2003	100	100	100	100	100	100
Q3	116.19	101.16	104.33	106.50	98.59	103.14
Q4	110.19	94.08	98.95	105.86	90.26	104.93
Q1 2004	107.75	93.15	96.19	107.39	84.20	102.64

Table 5 shows fluctuation of the market freight price and it also shows the difference in of the freight price for the same cargo coming from the US and bound for the US. For example, in the first quarter of 2004 the freight price for the cargo bound east from U.S to Europe will cost 84.2 while the same cargo bound west from Europe to the US cost 102.6 which means extra fees in the US bound cargo including the fees and taxes of the security measures and expected delay of cargo in security procedures (shipping Australia limited, 2004).

The 24-hour rules required by American customs expressed extra cost on shippers stemming from the early manifest requirements. While the security rules stated that only shipment data is required 24-hours before loading, some ports did not accept this data without existence of the cargo in front of port inspectors themselves. Therefore, shippers are paying extra cost for port space for containers shipped in advance one or two days before loading on board the vessel. Additionally, some carriers require shippers to send this data for them even earlier so that they should also transmit this data to the American customs as part of the carrier requirements (OECD, 2003, p.48).

4.6. Conclusion

While the security implementation is costly, the economic losses due to any successful terrorist attack will be badly. The cost of implementing container security stay under two categories: the first is the cost related to IMO-ISPS Code implementation which is estimated to be around USD 1.3 billion as a direct cost and 730 million as indirect or operational cost. The second is cost related to implement

the new container initiatives which is undetermined for many port because it is depends on the level of technology will be used. However, the American studies shows that this cost may arise up to USD 4.5 billion for port.

The cost of successful terrorist attack is tremendous due to its further implication on human lives physically and psychologically. The attack may cause losses of lives and keep its impact to the environment for long period. It is also affect the nations and international economy and keep them suffering to recover over long term period.

The cost benefits analysis resulting that the cost which nation will spend on increase security over the transportation chain will consider finally gain of money to all the industrial actors. Gains will include protect the trade from thief, illegal trade, fraudulent cargo, illegal immigration, and improve communication technology in term of saving time in the normal documentation procedure that had been used before.

Developing countries may suffer some implication to cover either the direct or the indirect costs of security. The huge competition in the shipping market and the limit ability of small entities, such as ports, carriers, shippers, and intermediaries comparing with the same parties in the developed countries will make participate of the developing countries in international trade is difficult. Potentially, the legitimate trade may be negatively affected, due to the incapacity of principally small and medium size enterprises within these countries, to effectively comply with the new requirements. The bilateral agreements may divide nations into favoured and less favoured trading partners and may lead to competitive disadvantages and failure to participate of developing countries in the international trade market.

Chapter 5

Conclusions and Recommendation

5.1. Conclusions

The research through the security framework of the international transport chain and intermodal container system provided theoretical and analytical viewpoints on the estimated weaknesses in the different modes of transportation, the most promising solution to enhancing security, and the economic consideration for the new security measures. The solutions presented for improving security are encouraging for the purposes of protecting the national and international interests including protection of human lives and provide a safe economic environment for the world.

Transport authorities face great challenges to cover the weaknesses of the intermodal system under their jurisdiction. One the most difficult challenge is that there is no single system governing the international movement of the container from its point of origin to the final destination. While, the international security framework exists at the centre of the chain covering ports and maritime transport, under supervision of SOLAS and the International Ship and Port Facility Security Code (ISPS), there is not yet an equivalent framework to cover the outer edges of the system, such as land and inland waterway transport.

Many of the security breaches in the container transport chain may be established at the land mode where there are possibilities of tampering with the container contents. Two possibilities may be addressed:

- The first is the *Trojan horse* scenario, which depends on setting up or purchasing staffing inside the legitimate trading companies that allow the criminals to achieve their illegal purpose through the normal trade patterns.

This may happen at the shippers' premises when stuffing the container contents.

- The second is *hijacking the containers* when the terrorist are targeting a legitimate container and tampering with its contents at any security weak step during its voyage.

Once the container is at the port, there is another challenge for the port authorities to namely identify whether this container is previously hijacked or Trojan horse. Port authorities applied only the requirements of the ISPS Code, which is not able to cover the security weaknesses at the land mode. The real example for that is the continual existence of piracy, ships hijack, and stowaways' problems. . Recognizing stowaways' problem, where the most cases are reported in containers, also gives great awareness of the terrorist problem due to the possible accessibility to the port area by unauthorized persons, indicating the weak implementation of the ISPS Code in some maritime countries and its inability to cover the breaches in the intermodal container system.

However, the statistics from the port state control in 2005 related to the ISPS Code, non- compliance ships classified by ships types indicate that the container ships have the lowest detention rates among other ship types. This may point to the proper implementation of the code on board these vessels after the code come into force, but it also signifies that most breaches come from the shore side area whether it is in land mode or at the port area.

The intermodal container industry requires a solution, which does not delay the flow of commerce but significantly improves the security of the system. Many initiatives are in place as a first step for the overall solution. These initiatives try to employ the advanced technology to cover the gaps in the container chain. The system proposed provides further steps to improve the management procedure and identify the responsibilities among shipping actors.

The initiatives introduced devices to track and trace the container from the point of origin by introducing the electronic seal and RFID tags which they activate automatically and send signals to the authorities in case of any try to tampering with

the container content through the entire transportation chain. These devices are working with radio frequency to cover the land area and with satellite frequency as well to cover the maritime sector. But, in land mode it needs many readers to support the system. On the gate of the ports scanning and screening for the container will be carried out to check the container contents and identify the high risk containers. Anti- tampering devices will continue their function at the transit time at the port storage area.

Concerning improvement of the security management system, shippers are requested to be held fully responsibility for the container contents and send this information automatically through the automatic cargo manifest to the customs authorities 24 hours before the cargo is loaded on board. The carriers are also requested to hold the responsibilities of any unknown deviation from the normal trade route and send notification of arrival by enough time to the port of arrival 96 hours requested by the US ports.

The technology is available to cover the gaps. However, this technology alone can not achieve effective security. The people working in the field, especially in land mode is another important factor that could affect the level of protection, such as the availability to tamper with the container contents at shipper premises and before the container starts its legitimate journey.

Moreover, the efficiency of the system mostly depends in its effective implementation on the country of origin where there is different customs and practices varying from one country to another. This technology will not be effective without international agreement and harmonization for the system together with the ISPS Code.

In that sense, the security of intermodal transportation system cannot depend on the ISPS Code only because the code is not “Cure-all” and it is a starting point to show the right way to the entire industry in the same direction. The Intermodal transportation chain needs an international regime to cover the system from its point

of origin to the final destination because it will be easy to find form where the deficiencies start to understand the requirements of each country.

Decision makers should be aware of the benefits and impacts of their decisions to implement this technology such as:

- How will this technology be used?
- Who will pay for its cost?
- The impacts for their country if such implementation take place,
- Detailed cost benefit analysis for tightness of security measures and its impacts to other industries,
- The international market situation in terms of the demand and supply theory,
- The effect of this implementation, especially the initiatives that depend on bilateral agreement under their countries sovereignty.

The United Nations Conference on Trade and Development (UNTCAD) and the International Maritime Organization (IMO) estimate that the operation of merchant ships contributes about USD380 billion in freight rate within the global economy. More than 90% of the world trade in volume transported by sea moves by containers. The world fleet made up 46 222 ships, including 3165 container vessels, transfer nearly 250 million containers annually between countries. Most of the dangerous cargo, such as chemical, nuclear, biological, and radioactive material moves in containers. These figures give an indication of the great importance of the intermodal container shipping to the world trade.

Container security is essential to protect this industry and the world economy. While the implementation of security measures is costly, consequences of terrorist attacks are more costly and while some measures may slow trade, many others can in fact lower trade costs. Additionally, there are more cost benefits resulting from increased security in the transportation chain, namely gain of money to all the industrial actors. Gains will include protecting the trade from theft, illegal trade, fraudulent cargo, illegal immigration, and improved communication technology in terms of saving time in the normal documentation procedure that was used before.

However various impacts may face the industrial actors and the country of origin to implement the new security measures. The most affected actor will be the shipper and the most affected countries will be the developing countries. The international market is a competitive market, particularly in the liner shipping such as the container shipping. The theory of demand and supply will control the market, which means that the actors, who will able to provide cheaper services, will be able to continue in the competition. Therefore, the shipper will face two opposite problems: first to contribute to the security requirements interim of the additional cost and second to try to maintain the freight charges within the normal limit of the market.

All the industrial experts estimate that the governments will pay the security costs and additional taxes will be collected from the actors such as carriers and shippers. Consequently, the actors will increase the freight rate on the exporters and importers, and finally the normal costumers, or in other words the public citizens in each country, will bear these costs in terms of more expensive commodities in the domestic market.

Developing countries may face some implications to apply with the new security measures. This is mostly because the small number of the industrial enterprises that are able to cover the security costs and the huge competition in the international trade market. The new security measures proposed by the US depend on the bilateral agreements that may some countries sign and others not sign. These may divide nations into favoured and less favoured trading partners and may lead to competitive disadvantages and failure to participate of developing countries in the international trade market.

Shippers and carriers will also face some difficulty in the flow of their trade due to the expected delay to deliver the cargo in case of tightness security procedure at some CSI Ports. Identification of high-risk container by scanning systems may delay the flow of the trade and make the shippers bay compensation for the cargo owners due to time delay. In some developing countries shippers also suffering problems of implementing the CSI, which lead the exporters to choose another port, comply with the rules to load their freight to avoid any further problems on the ports of arrivals.

The ocean carriers may also suffer the problem of time delay if they are comply with the requirement by refuse their entry to the ports or facing further unfavoured delay, which may lead to loss chartering contracts and lost trust of the users .

5.2. Recommendations

The stakeholders and transportation authorities must co-operate to address the various issues correlated to improve intermodal security and reduce the vulnerability to a terrorist attack using the cargo container and transportation chain. The role of responsibilities among the transportation authorities must be defined. This will be appropriate with using the risk management plane to organize the work and avoid the duplicating or overlapping of responsibilities. Stakeholders should increase the co-operation between the private and public sectors of transportation facilities, as any weakness in system, either private or public, will affect the level of protection for the entire system. These plans should be under continuous supervision by the national governments to ensure updated response according to the international criminal situation in the transportation system.

The transportation authorities should carefully identify the efficiency of the supply chain under their domestic legislation and focus on removing the weaknesses, particularly on the outer edges of the intermodal transportation system. This will lead to improving the entire security system and prevent risk transfer from one mode to another, which will give positive results in the effective implementation of the ISPS Code in the maritime sector. Referring to what was mentioned earlier in chapter 2 of this study, the container may become a Trojan horse or hijacked during any gaps in the land transportation mode. So, providing more security awareness in the shippers' premises, and within land transportation carriers, will decrease the risk factors through the entire intermodal transportation. It is recommended to establish a strict employment system to know the history of each worker, establish security education and training programs, increase security awareness among the workers, monitor the work done by more than one supervisor, and update the workers´ knowledge according to the current international threat.

In the port area transportation authorities should ensure effective implementation of the ISPS Code in terms of establishing strict controlling access to the port area, monitoring port employees, monitoring stevedoring companies and their employees, and establishing stricter security measures around the vessels in their terminals.

The national governments should also supervise the level of the ISPS Code implementation on the national ports and fleet. The voluntary flag state audit enhanced by the IMO is a good opportunity for each country to ensure its compliance with the international regulations including the security measures. Increasing the national fleet compliance will decrease the time stoppage for their vessels due to the detention by the foreign Port States Control which will encourage the ship-owners to register their vessels under this flag and will lead to more economic gains to this flag.

Increasing the security funds is one successful solution considering that security is normal business in the shipping industry. Using the technology to secure the system may use these funds to increase the level of protection. For example, the existing cameras in and around the working area will introduce more protection levels and make it easier to discover any unauthorised persons or illegal action by the authorized workers. Intermodal transportation stockholders should also consider the cost benefits that will be gained from security improvement in terms of lower insurance premiums, cargo loss prevention, increased tax revenues, and improved supply chain management system. It is recommended to the decision makers that technology should take place in the container security system and that it is not necessary to provide a very high level of technology, which is expensive, but it is important to use the budget available to cover all the gaps that are determined through the transportation system.

International action is required in terms of working group operation among IMO, International Labour Organization (ILO), and World Custom Organization (WCO) to establish a security form for the intermodal transportation system. International standards on transparency and identify responsibilities for the parties involved with or having commercial interests in the ships or ports. There should be some measures to evaluate the security performance on the shippers, agencies, and

stevedoring companies. In this sense, IMO should be an active contributor in developing a container security system in terms of tracking, screening, and identifying the high risk containers. The system should be under an international forum to create a form, which is suitable for all member states. This new international regime may be based on:

- Identifying the technology required to cover the gaps of container security from the point of origin to the point of destination with minimum costs to be available for each country to contribute to the system.
- The system could identify the availability of the technological security devices in the international market to ensure coverage of the existing worldwide containers and existing entire world container vessels fleet.
- The system could also include guidelines for the users in terms of its technical establishment, regular maintenance, training courses, availability of the spare parts, and experts' opinions.

International security agreements between the shipping countries that outline ways that these countries will assist each other on advancing information on vessels, crews, cargo and indicators of which cargo items have already been inspected in various ways. These agreements should have an international forum under the supervision of a United Nations agency, such as IMO. The working example on the horizon is the piracy problems, where IMO requires all flag states to report the current incidents and then reporting back the cases to the world fleets. These gives progressing in handling this problem by identifying the dangerous areas at sea and advising the vessels how to navigate through these areas to avoid pirate dangers. In this sense, the shipping countries could co-operate to inform each other of the probability to stowaways; high-risk containers or any terrorist threat. This fast communication and co-operation will enhance the quickly preparation and response to this risk, which may prevent or at least minimize the danger that may exist.

References

American Association of Port Authorities, (2006, March 12). *Seaport Security*. Retrieved July 28, 2006 from World Wide Web: http://www.aapa-ports.org/govrelations/aapa_security_position.pdf

Akimoto, K. (2001, December 11). *The current state of maritime security: Structure weaknesses and threats in the sea lanes*. Tokyo: Institute for international policy studies.

Babul, M. (2004, May 3). *No silver bullet managing the ways and means of container security*. Washington: Army war College.

Brooks, M., & Button, K. (2006). Market structures and shipping security. *Maritime Economic & Logistics Journal, 8 (1), 100-120.*

Billings, B. (2006, January). Thinking outside the Box: Laying security myths to rest. *Official Journal of the International Association of Ports and Harbours, 51(1), 32-34.*

Binnendijk, H. (2002, August). *The virtual border: Countering seaborne container terrorism*. Washington, DC: Defence Horizons, Centre for Technology and National Security Policy: National Defence University.

Bolt, K. (2006, June 8). *Congress Report: Congress drops financing for increased port security*. Washington, USA. Retrieved July 25, 2006 from World Wide Web: http://seattlepi.nwsource.com/local/273184_containers08.html

Balog, A. (2005, June 3). *Riding the wave on ship container seal and tracking System*. Washington. Retrieved June 20, 2005 from World Wide Web:http://depts.washington.edu/poeweb/gradprograms/envmgt/2005symposium/ContainerProjectReport.pdf

Congressional Research Service (CRS), the library of congress. (2004, October 19). *CRS issue brief for Congress: Transportation Issues in the 108th Congress.* Washington: Congress Publication.

Coleman, L. (2006, March 30). *Coleman- Levin caution that US still vulnerable to smuggling threat: Congressional hearing highlight*. Carl Levin, United States Senator, Michigan. Retrieved July 27, 2006 from World Wide Web: http://www.senate.gov/~levin/newsroom/release.cfm?id=253321

European Shippers Council (ESC). (2004, November 4-5). *The impact of security*

regulation other requirements on shippers. Paris: OECD publications.

Elovic, P. (2003, February 26). *Implementation of Gate and Crane OCR system for Container Terminal Automation and security*. Retrieved May 10, 2006. From World Wide Web: http://www.htsol.com

Ferriere, D. (2005, September). *Using technology to bridge maritime security gaps.* Portsmouth: National infrastructure Institute center for infrastructure expertise.

Gilbert, G. (2005, January). *Securing the Supply Chain: Container security and sea trial demonstration results*. Retrieved May 6, 2006 from the World Wide Web: http://www.raesystems.com/~raedocs/Securing_the_Supply_Chain_011205.pdf

Goulielmos, A., & Anastasakos, A. (2005, November 14). *Worldwide Security Measures for Shipping, Seafarers and Ports: An Impact Assessment of ISPS Code*. Piraeus, Greece: Department of maritime studies, University of Piraeus.

International Ship and Port Facility Security (ISPS) Code and SOLAS Amendments International Maritime Organization (IMO) 2003. London: IMO publications.

INTERTANKO - Latin American Panel (LAP). (2005, October 22). *International Maritime Organization (IMO) Reports on Stowaways Incidents: Annual Statistics for the years 2003 and 2004*. Miami Beach: Trade Wind Tankers.

International Maritime Bureau, IMB: Piracy reporting centre. (2006, May 3). *IMB Release Latest Piracy Statistics*. London: International Chamber of Commerce (ICC).

Jain, R. (2004, September). *Security the port of New York and New Jersey: Network-centric Operations applied to the campaign against terrorism.* Hoboken, USA: Stevens Institute of Technology.

Jagc, A. (2003, September 3). Container and Port Security. *The International Journal of Marine and Coastal Law, 18(3), pp. 341-361.*

Jump, J. (2006, April 23). Right of Passage: Access Denied. *Journal of International Transport Workers´ Federation (ITF)*. London: ITF Publications.

James, M., & Robert, G. (2002, February). Global Trade: America's Achilles heel. *Defence Horizons (volume 7)*. Washington: National Defence University, Centre for Technology and National Security Policy.

KUTV, News. (2006, April 5). *Stowaways from China found in Cargo Container*. Retrieved May 14, 2006 from World Wide Web:

http://kutv.com/topstories/local_story_095131306.html

Lowe, D. (2005). *Intermodal freight transport*. Oxford; Burlington: Elsevier Butterworth Heinemann.

Lukas, A. (2004, April 8). *Protection without Protectionism: Reconciling trade and Homeland Security*. Washington: Cato Institute's Centre for Trade Policy Studies.

Mejia, M.Q. (2002). Defining maritime violence and maritime Security. In P.K Mukherjee, Q.M. Mejia & G.M. Gauci (Eds.), Proceedings of the International symposium on 26 – 30 August 2002 (pp.27-38) on Maritime violence and other security issues at sea. Malmo, Sweden: WMU Publications.

Mukherjee, P. & Mejia, M. (2003). The ISPS Code: legal and ergonomic consideration. In Q.M. Mejia (Eds.), Proceedings of international symposium on 11 -15 August 2003 (33 -51) on Contemporary Issues in Maritime Security. Malmo: Sweden: World Maritime University publication

Mackenbach, P., & Coolen, M. (2005, October). *DNV Consulting, Study on the Impact of Possible European Legislation to Improve Transport Security: Managing Risk.* Brussels, European Commission DG TREN, DNV Consulting.

North of England, P&I Club. (May 25, 2004). *ISPS will make Stowaways a Bigger Problem. Newcastle: North of England P&I Club*. Retrieved May 14, 2006 From World Wide Web: http://www.nepia.com/news/press_releases_article.php?offset=2&id=44

Organization for Economic Co-operation and Development (OECD) report. (2005). Container transport security across modes. *European Conference of Ministries of Transport (ECMT).* Paris: OECD publications.

Organization for Economic Co-operation and Development (OECD) report. (2004, June 02). OECD urges integrated approach to container security. *European Conference of Ministries of Transport*. Paris: OECD publications.

Organization for Economic Co-operation and Development (OECD) Annual Report. (2004). The role of transport authorities. *European Conference of Ministry of Transport*. Paris: OECD publications.

Organization for Economic Co-operation and Development (OECD) report in Maritime transport Committee. (2003). *Security in maritime transport: Risk factors and economic impact*. Paris: OECD publications.

Organization for Economic Co-operation and Development (OECD) report. (2003). *Security in Maritime Transport: Risk Factors and Economic Impact.* Paris: Maritime Transport Committee

Panama Canal Authority. (2006). *Description of Panama Canal*. Retrieved April 17, 2006From World Wide Web: http://en.wikipedia.org/wiki/Panama_Canal

Poulin, S. D. (2005, May 18). *Realigning Coast Guard Enhanced Maritime Capabilities: A Lesson Learned from the U.S. Special Operation Command*. Philadelphia, U.S: Army War College.

Rodrigue, J., & Slack, B., & Comtois, C. (2004). *Intermodal transportation:* Containerization and intermodalism. Retrieved May 30, 2006 from the World Wide Web: http://people.hofstra.edu/geotrans/eng/ch3en/conc3en/ch3c5en.html

Russell, M. (2004, April 11). *Port moves on container terror checks: Security at Australia's Busiest Port, Melbourne, is being upgraded to prevent a terrorist* attack. Retrieved July 29, 2006 from World Wide Web: http://www.theage.com.au/articles/2004/04/10/1081326985037.html

Safety of Life at Sea convention (SOLAS, 74). London: International Maritime Organization (IMO) publications 2004.

Scotland Yard announced on B.B.C. news. (2006, August 10). "*Airlines terror plot Disrupted*". Retrieved August 10, 2006 from World Wide Web: http://news.bbc.co.uk/2/hi/uk_news/4778575.stm

Sweet, K. M. (2006). *Transportation and Cargo Security: Threats and solutions. (pp.174-177)*. New Jersey: Pearson Education LTD.

Suez Canal Authority. (2006). The modern Suez Canal. Retrieved April 16, 2006 from World Wide Web: http://en.wikipedia.org/wiki/Suez_Canal

Shou, M. (2005). Maritime economics. Unpublished lecture handout, World Maritime University, Malmö, Sweden.

Shipping Australia Limited (2004, August 18). *Submission to the Productively Commission's: Review of part X of the trade practice act*, 2004. Retrieved July 30, 2006 from World Wide Web: http://www.pc.gov.au/inquiry/partx/subs/sub016.pdf

Standards of Training, Certification & Watch-keeping (STCW) Convention (1995). ' London: IMO publications

The subcommittee on Coast Guard and Maritime Transportation. (2005, June 29). *Hearing on implementation of the maritime transportation security Act*. Retrieved April 15, 2006 from World Wide Web: http://www.house.gov/transportation/cgmt/06-29-05/06-29-05memo.html

Trelawny, C. (2006, May). Filling the gaps. *Containerization International magazine Pp.76-77*

United Nations Conference on Trade and Development (UNCTAD). (2004). *Container Security: Major initiatives and related international developments*. Geneva: United Nations.

U.S. Customs and Border Protection (CBP). (2006, March 29). *Container Security: Fact sheet*. Washington: CBP publication.

United States General Accounting Office (GAO). (2003, September 09). *Transportation security: Federal action needed to enhance security efforts*. Washington, DC: US. General Accounting Office.

United States General Accounting Office (GAO). (2005, December). *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*. Washington, DC: U.S. General Accounting Office.

United States Coast Guard (USCG). (2005). *Container Inspection Program*. Washington. Retrieved June 20, 2005 from World Wide Web: http://www.uscg.mil/hq/g-m/nmc/pubs/msm/v6/c9.pdf

U.S. Subcommittee on Coast Guard and Maritime Transportation. (2005, June 29). *Hearing on Implementation of the Maritime transportation Security Act*. Retrieved July 29, 2006 from World Wide Web: http://www.house.gov/transportation/cgmt/06-29-05/06-29-05memo.html

Willis, H., & Ortiz, D. (2004). *Technical Report of Evaluation the Security of the* Global Containerized Supply Chain. Santa Monica: RAND Europe.

World Maritime Day of the International Maritime Organization (IMO). (2005). International Shipping – Carrier of World Trade. London: J/9015, IMO publications.

Yilmazel, M. & Asyali, E. (2005). An Analysis of Port State Inspection Related to the ISPS code. Malmo, Sweden: Annual General Assembly, International Association of Maritime Universities (IAMU).